Universiteit Leiden

ICT in Business

The development of an information security governance maturity model for Dutch hospitals

Name: Fynn Loeffen
Student-no: s2097605
Date: 06/08/2019

1st supervisor: Tino de Rijk

2nd supervisor: Bas Kruiswijk

Leiden Institute of Advanced Computer Science (LIACS)

Abstract

In 2017, the hospital industry around the globe was the victim of a large set of cyber-attacks which posed a real threat to the hospitals' ability to provide (immediate) care to their patients (Schellevis, 2017). These cyber-attacks were relatively easy to prevent, and this raised the question of how it could be possible that organisations like hospitals, which are so dependent on their complex information systems, can be so vulnerable. Research showed that a possible explanation for the effectiveness of these unsophisticated cyber-attacks could be the lack of basic IT security hygiene, as well as the lack of a good foundation of an information security program (Morse, 2017).

Information security is about people, processes and infrastructure, where security governance is the overarching layer that fits everything together and establishes the foundation of an effective information security program (ISACA, 2006).

In this research, an information security governance maturity model specific for hospitals has been created to measure the current maturity of information security governance within hospitals in The Netherlands. The maturity model consists of five capability domains, namely: *Organisation, Strategic Alignment, Risk Management, Validation, Value Capturing & Delivery* – and 36 attributes; the maturity levels have been developed based on the governance processes defined by the ISO 27014 standard. The maturity model has been improved in two iteration rounds, using the feedback of a diverse set of strategic information security experts – both within and outside the hospital industry. To make the maturity model industry specific, the attributes have been geared towards the hospital industry and hospital-specific governance challenges have been considered. The two hospital-specific governance challenges which have been identified are: *Workability*[1] and *Connected Medical devices*[2].

What can be concluded from the case studies (limited to n =3) is that all the investigated hospitals are on a similar information maturity governance level. The hospitals are, at best, trying to create an information security management system in order to be compliant, but none of the hospitals had a single capability domain which scored on average a maturity level of 4 (managed). In regards to the hospital-specific governance challenges, it can be concluded that all hospitals had a maturity level 2 regarding *Workability*. With regards to *Medical Devices* only one hospital excelled and scored a maturity level 4 (managed), where the other two hospitals were scoring a level 2 maturity.

Creating a foundation for an information security program is the minimum requirement for hospitals, but a lot of improvements can and have to be made in regards to information security governance to become resilient against current cyber threats. Furthermore, the maturity model can help hospitals identify their current information security governance maturity level and constitutes as a starting point for their future improvements.

[1] Workability focuses on the integration of security with business processes and on determining how the end-user experiences the usability and user-friendliness of a security control.
[2] Connected medical devices are currently (implemented) insecure within the IT landscape of hospitals.

Table of contents

Abstract 2
1 Introduction 5
2 Research Design 6
2.1 Research Problem 6
2.2 Research Objective 7
2.3 Research Question 7
3 Methods 9
3.1 Methodology 9
3.2 Overview 9
3.3 Literature Review 10
3.4 Building the maturity model 10
3.4.1 Iterative process 11
3.4.2 Criteria 11
3.5 Case studies 11
4 Literature Review 13
4.1 The role of governance within information security 13
4.1.1 Holistic overview 14
4.1.2 Structure 14
4.1.3 Relationship with Information Security Management 16
4.2 Information Security Governance as a metric 19
4.2.1 Strategic Alignment 20
4.2.2 Risk Management 22
4.2.3 Value Delivery 26
4.2.4 Resource Management 29
4.2.5 Performance Measurement 29
4.3 Information Security Governance challenges in the hospital environment 31
4.3.1 Connected medical devices 32
4.3.2 Workability 33
4.3.3 Zero Trust as a solution 34
5 Measuring Information Security Governance 37
5.1 Structure 37
5.2 Maturity model definitions 39
5.3 Presentation of results 39

5.4 Scoring Scheme 40
5.5 Construction of capability domains 42
5.6 Construction of attributes 44
5.7 Validation and improvement of the maturity model 46
5.7.1 Iteration 1 46
5.7.2 Iteration 2 50
6 Results 53
6.1 Case study 1 53
6.2 Case study 2 55
6.3 Case study 3 57
6.4 Overall results 59
7 Discussion 61
7.1 Phase 1 61
7.2 Phase 2 61
7.3 Phase 3 62
7.4 Internal Validity 62
7.5 External Validity 62
8 Conclusions 63
8.1 Future work 64
References 65
Appendix A – Maturity Model 71
Appendix B – Maturity Model Assessment Tool 85
Appendix C – Structured Interview Form 86
Appendix D – Interviews With Experts 88

1 Introduction

With the rapid adoption of technological applications in our daily life, we have made human life vulnerable to cyber risks by implication (von Solms & van Niekerk, 2013).

In 2017, the hospital industry around the globe was the victim of a large set of cyber-attacks which posed a real threat to the hospitals' ability to provide (immediate) care to their patients. In some cases, hospitals had to cancel medical procedures because of unavailable systems (Schellevis, 2017). Even though the impact of the attack was high, the complexity of the attack itself was relatively low and could have been prevented with basic IT security practices - as stated by the British National Audit Office (Morse, 2017). How is it possible that within an industry where cyber-attacks pose a threat to patients' health, the ability to execute basic IT security hygiene is missing? Choi et al. (2019) have calculated that the current responses to cyber-attacks significantly influence the 30-day mortality rate for specific medical emergencies like a heart attack and can set back the 30-day mortality rate by more than a decade.

In the hospital industry, business processes have been converted into ICT-enabled activities and are a crucial component in providing (immediate) care. ICT-enabled activities are not purely technical activities, but also consist of socio-technical activities[3] like van der Berg (2018) proposes in his *conceptualization of cyberspace*. To create an effective defence while managing this complex ecosystem of people, processes and systems, it is required to look at how information security governance is implemented within the hospital environment.

Information security is about people, processes and infrastructure, where security governance is the overarching layer that fits everything together and establishes the foundation of an effective information security program. The goal of information security governance is to deliver strategic alignment, execute proper risk management, maximize value delivery & capturing, and validate, maintain and improve the information security management program (ISACA, 2006).

Currently there are no tools available for the measurement and improvement of information security governance. Governance is barely touched upon in information security best practices like the ISO 27001 or used as a metric when assessing an organisation's information security maturity.

The goal of this research is to establish how information security governance can be measured in the hospital environment through an information security governance maturity model. The information security governance maturity model will provide strategic information security leaders within hospitals with a tool to measure and improve their information security governance program.

[3] *Socio-technical activities are defined as activities where interaction between people and a technology occurs. (van den Berg, 2018)*

2 Research Design

The aim of this chapter is to identify an existing problem - which this research will tackle, as well as the gap that exists in literature in addressing the problem itself. The research objective will define what the goal of this research is and what will be developed to reach this goal. To achieve the research goal, various research questions have been defined.

2.1 Research Problem

Hospitals are being transformed into ICT-enabled enterprises and want to leverage the digital transformation to improve the quality and efficiency of the caregiving process. The issue that arises with the digital transformation is the rising need and dependency on information security as a business enabler. Hospitals are interesting targets for malicious criminal actors, since they work with large amounts of sensitive (medical) data which has to be reliable, kept confidential, and has to be available at all times. Even though the stakes are high, it is worrying to conclude that hospitals still seem to fail at executing basic IT security hygiene.

Literature gap

Information security governance's importance in this context is derived from being one of the main requirements and predictors of an effective information security program. Yet the amount of research into information security governance and how to measure it is missing in literature. A way of filling the literature gap would be to research whether it is possible to develop a measurement tool which can measure information security governance (within hospitals). The measurement tool should define *what* good information security governance is, and *how* it should be executed – information which is currently missing in literature and best practices.

Information security governance maturity could be a good predictor of information security resilience because it doesn't solely look at one specific facet of information security, but considers its people, processes and infrastructure - and their alignment, as a whole. The organisation can have the latest and greatest security products and tools; however, these will not work if security policies and procedures are not implemented correctly (CGI, 2016).

Information security governance in Dutch hospitals is specifically interesting because of the following problems:

I. Dutch hospitals have to work according to the NEN7510 standard by law; they don't have to be certified, but do have to be audited regularly (NEN, 2019) (Overheid.nl, 2017). A normative standard like NEN7510 (or ISO 27001) is a good way to start with technical and operations measures, however it doesn't consider the governance side of information security. The lack of an assessment of information security governance can result in a poor evaluation of the information security maturity (during a compliance audit) (Da Veiga & Eloff, 2007) (Siponen, 2003) (CGI, 2016). *From this problem we can derive the question: What is the current maturity of information security governance in Dutch hospitals?*

II. The number of medical devices attached to the (IP) network constitutes one of the bigger challenges for current information security governance bodies within hospitals. There have been reports of large amounts of medical equipment being infected with malware – however medical equipment suppliers still refuse to constantly update their equipment because 'the risk of malfunctioning equipment' is too high (Deloitte, 2015) (Schellevis, 2017).
From this problem we can derive the question: How does information security governance within hospitals deal with the challenge of connected medical devices?

III. The act of balancing out security and workability constitutes a challenge in any sector. Implementing too many security measures might result in people finding an insecure way to bypass them. This question is from even greater importance in the medical field because of the high stakes involved in emergency, life-and-death situations.
From this problem we can derive the question: How does information security governance within hospitals deal with the challenge of balancing out security versus workability?

2.2 Research Objective

The objective of this research is to define what information security governance in hospitals is, and how it can be measured objectively. Since the research's focus is on the Dutch hospital environment, it is important to look into the specific challenges that the governance body of Dutch hospitals has to deal with.

The deliverable of the research will be an information security governance maturity model which can be used to carry out an information security governance assessment for hospitals. The maturity model will be based on literature review but will be reviewed, validated and improved with expert knowledge both within and outside Dutch hospitals.

The final objective of the research is to validate the model and to get an overview of the information security governance maturity in various Dutch hospitals, by applying the model to real case studies.

2.3 Research Question

Main research question:

How can the maturity of information security governance in Dutch hospitals be measured objectively?

Sub questions:

I. What is the role of governance within information security?
II. What are the information security governance challenges within the hospital environment?
III. Is it possible to develop a valid maturity model to effectively measure information security governance within hospitals?

IV. *If so*: what is the current maturity level of information security governance within Dutch hospitals, using the developed maturity model?

3 Methods

In the current chapter the researcher will describe the process through which the research will be executed. This chapter will provide the reader with guidance and the tools to examine the repeatability and reproducibility of the research.

3.1 Methodology

The used methodology for this research is *Design Science Research (DSR)*, since one of the main fundamental drivers behind DSR is *learning through building.* The DSR methodology provides the research with a structured process and iterative process, which makes the DSR methodology a good choice for the creation of a maturity model.

The DSR methodology consists of the following five process steps:

1. Awareness of problem
2. Suggestion
3. Development
4. Evaluation
5. Conclusion

The *awareness of problem* has been described in the chapter *Research Problem.* The *Suggestion* process defines a possible solution to the identified problem, which has been described in the chapter *Research Objective*. In the development phase it is important to determine an *artefact* which will help to achieve the research goal. For this research, various challenges regarding information security within the Dutch hospitals - related to information security governance, have been identified. In order to measure information security governance within Dutch hospitals, it is required to build an information security governance maturity model, which is the artefact of this research. The *development* and *evaluation* phases are iterative processes which will provide the necessary feedback and validation, until the artefact reaches a quality level which is usable for the research (Vaishnavi & Kuechler, 2012).

3.2 Overview

The DSR methodology provides a structure with process steps which will be followed throughout the research. Based on the DSR methodology, the *development* and *evaluation* phases will lead to the construction of the artefact. Various tools can be used within the development and evaluation phases to achieve the desired results. The tools which will be used to create the artefact are a literature review and structured interviews. In order to illustrate which tools are used and for which objective, a research overview has been created:

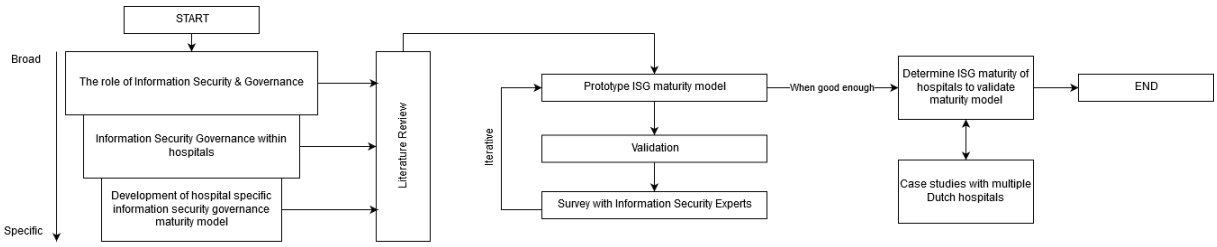


Figure 1. Research Overview

3.3 Literature Review

The literature review has been executed according to the funnel model as described by Hofstee (2006). The funnel model proposes to start researching the main topic from a broad perspective - resulting in the creation of a broad theory base, before focusing on its specifics. This process begins with a broad research into information security and information security governance in general, and continues specializing on information security governance in Dutch hospitals through an investigation of hospital-specific challenges in the later stage of the literature review.

At the beginning of the research process, a literature review has been executed to provide a knowledge foundation which serves as a starting point for the first prototype of the information security governance maturity model. Information security is a very broad field that consists of many differentiations, which all have to work together and individually contribute to the information security defence of an organisation.

The goal of the first research question is to get a clear view of information security as an overarching function within an organisation. This stage of the literature review has served to define what information security, in general, is, as well as to understand how information security governance works, how it correlates to information security and which areas of expertise are relevant for the study of information security governance - and thus for the creation of the information security governance maturity model. This information served to build the 'skeleton' of the maturity model; furthermore, it also supports the creation of the 'attributes' within the to-be-developed information security governance maturity model.

The goal of the second research question is to make the information security governance maturity model complete and suitable for the Dutch hospital environment; to achieve this, recent and relevant challenges that people responsible for information security governance have to cope with have been researched. This not only made the information security governance maturity model more relevant, but it also helped to create and support knowledge sharing, since these challenges are probably shared among all Dutch hospitals.

This preliminary literature review constitutes a starting point for the building of the hospital-specific maturity model. The supporting activities for the model construction will be described in the following paragraph (3.4).

3.4 Building the maturity model

Since the literature review is only able to consider the theoretical side of the possible solution, it is also necessary to collect additional feedback and validation using information security experts who have knowledge and experience in the fields of strategic information security.

For the validation of the developed information security governance maturity model, an iterative improvement process according to the DSR methodology has been executed to refine the model.

3.4.1 Iterative process

The validation of the information security governance maturity model has been achieved by creating a semi-structured interview - using a standardized assessment list - aimed for expert review, as proposed by Salah et al. (2014). The standardized assessment list measures the expert opinion on 14 quality attributes such as *accuracy*, *sufficiency* and *comprehensiveness* etc. on different elements of the maturity model, like the *attributes*, *maturity levels* and *ease of use*. The measurement is taken according to a five-point scale going from *Strongly Disagree* up and until *Strongly Agree*. Next to the quantitative measurement of the 14 quality elements, there 10 open questions aim to collect extra information that can be used for further improvements of the information security governance model (Salah, Paige, & Cairns, 2014).

The iterative process consists of multiple rounds where the same structured approach is used. An iteration round is finished when no new feedback is collected. The collected feedback is then analysed, and the proposed changes are applied to the model. In a next iteration round the improved maturity model is validated through the same semi-structured process, by different interviewees. The iterative process stops when no more significant feedback for improvements is collected.

3.4.2 Criteria

The researcher has chosen to validate the information security governance maturity model using semi-structured interviews. The researcher chose to use at least 2 experts on strategic information security who are currently working in a Dutch hospital and a minimum of 1 expert of strategic information security who is not working in the Dutch hospital industry.

In iteration one, the first version of the maturity model has been investigated by 6 experts (n =6). Out of the 6 experts, 5 are currently working in a hospital and are responsible for information security at the strategic level. The other expert has >20 years of experience within the information security industry.
In iteration two, the second version of the maturity model has been investigated by 6 experts (n = 6). 2 experts are currently working in a hospital, 4 other experts are included because of their extended amount of experience in the field of strategic information security within different large industries. The combination of both “hospital-experts” and “non-hospital-experts” was used to get as much of a diverse feedback as possible.

3.5 Case studies

To verify and test whether the model is able to produce reliable results, the researcher has applied the model in several case studies within Dutch hospitals. The maturity model aims to measure the current state of information security governance within a hospital, and the researcher used the developed maturity model as such assessment tool.

The goal of the case studies is to verify and test whether the information security governance model is able to produce reliable results. The results have also been used to gain insights on the average maturity of information security governance in Dutch hospitals. In total, 3 Dutch hospitals have participated in the case study, through which the maturity model was used to assess their current maturity level. Even though 3 hospitals are not

representative enough for the whole of the Netherlands, the case studies did provide the opportunity to test the maturity model in practice. The 3 hospitals were all general hospitals and were a mix of large and smaller sized hospitals which are geographically spread across the Netherlands.

For the execution of the case studies, for each selected hospital a strategic information security specialist within that hospital has been asked to fill out the developed maturity model for their current situation and to share these results with the researcher. The researcher did not intervene in the case study, in order to limit any influencing external factors.

The names of the participating hospitals have been kept anonymous because the information collected and produced by the maturity model is private/confidential.

4 Literature Review

The objective of information security is "protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity." (Williams, 2001)

Since information is everywhere, possible security solutions cannot exist in isolation. There is not a single solution towards a secure organisation: a solution requires various differentiations within the information security domain to work together, ranging from policy creation to networking. Information security management tries to protect an organisation by constantly applying risk management and implementing the correct controls (in the form of network security, policies and computer security, as identified by Whitman et al. (2012)). The three pillars of information security management are *people*, *processes* and *technology*, which have to be protected but can also be leveraged to provide protection (Dutton, 2017).

The "*Business Model for Information Security*" shows the relationship between the three pillars and how governance plays an important role in the alignment between these pillars.

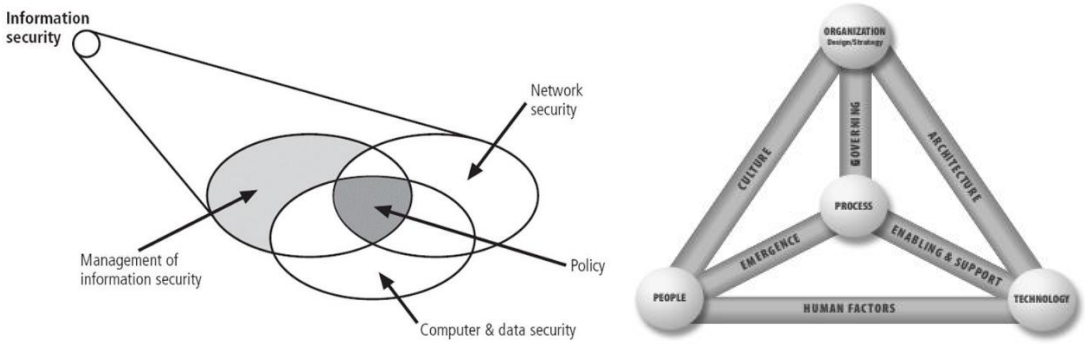


Figure 2. Business Model for Information Security (Whitman & Mattord, 2012) (ISACA, 2009)

With the increasing reliance on information security as a business enabler, the need for alignment between people, processes and technology increases, and taking a closer look into what drives this alignment becomes more important. One of the main drivers of information security within an enterprise is governance.

4.1 The role of governance within information security

The goal of corporate governance is to provide a business strategy to achieve the company's mission, vision and goals, while minimizing risks, using the least amount of resources. In other words, strategic management has to develop a plan to reach its desired destination while minimizing the risks, and while spending the least amount of resources to maximize profit. (Ula, Ismail, & Sidek, 2011)(Moulton & Coles, 2003)

To achieve this goal, governance uses rules, policies, standards and procedures to direct and control the organisations activities. Information security governance provides the organisation with, but not limited to, policy compliance, increased predictability of business processes, a structure for security resource allocation, rational decision making, improved

risk management, assurance, accountability and organisational reputation safeguarding. (ISACA, 2016) (Ula, Ismail, & Sidek, 2011)

4.1.1 Holistic overview

Corporate governance and information security governance are interrelated. Information security is only effective when it is embedded within the organisation as a property of a person, process or technical component.

Information security governance is the process by which the organisation's information security activities are directed and controlled to preserve the availability, integrity and confidentiality of its people, processes, information and infrastructure. (CGI, 2016) (von Solms & van Niekerk, 2013) (Posthumus & von Solms, 2004) (NEN, 2013)

We can conclude that risk management plays an important role within the governance-domain. This statement is confirmed by the wide variety of risk management approaches which are included in corporate governance frameworks. Those risks need to be managed accordingly so the company is compliant with external and internal rules. The audit department is there to assess and assure the situation and conclude if a company is actually compliant or not. (von Solms B. , 2005) (Moulton & Coles, 2003)

The first step when developing an information security governance program is to determine a strategy, which is what the organisation wants to achieve with regards to information security. An information security manager should translate the needs of the organisation into security program requirements. From these requirements, a set of objectives will be created, which fulfil the security programs requirements. The security program aims to bring the current state of information security into a desired state.

To execute and achieve these objectives, the organisation has to specifically determine how these objectives will be met. When analysing the objectives, it could be beneficial to make business cases: when creating business cases for security improvements it is important to consider time, skills, funding, laws and regulations. Lastly, to achieve said objectives various solutions can be created in the form of technology, standards and processes, which are being supported by people. (ISACA, 2016)

4.1.2 Structure

All basic governance frameworks are based on a *Direct-Control Cycle* structure.

The main three actions of the direct-control cycle are *direct*, *execute* and *control*. The focus for information security governance is primarily on *direct* and *control*.

For information security governance the results that this Direct-Control Cycle produces constitutes an important feedback for the management program. The strategic layer can use this feedback to make changes in their

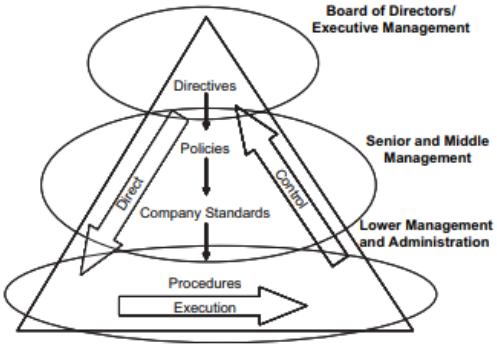


Figure 3. Governance framework (von Solms & von Solms, 2006)

strategy to get the desired result. (von Solms & von Solms, 2006)

A more specific governance model for information security is based on the ISO 27014, which includes extra processes. The ISO 27014 consists of the five following main processes: *Direct*, *Monitor*, *Evaluate*, *Communicate* and *Assure*. These activities have to be executed by the governing body of information security within the organisation (Mahncke, 2013).

DIRECT

On a strategic level, the general direction of the organisation is defined together with the security strategy. On the tactical level, management translates these goals into measurable key performance indicators (KPI's) according to best practices for information security management and policies. These policies are being translated from policies into procedures by lower level management.

The direction on the strategic level is generic and is set for a longer period of time. The KPI's and policies on the tactical level are more specific and allow room for interpretation from every operational department. The operational department interprets the tactical policies and creates very detailed procedures which fit within their departments.

The goal of *directing* is to give a direction about the information security goals and implement a fitting strategy. Changes in directing can be applied to risk management plans, policies, resource allocation, and much more.

MONITOR

Monitor (or control) is the phase where feedback is collected. The operational departments report to their tactical managers to check if the procedures were effective. Tactical management uses this feedback, together with their measurable KPI's, as input for the strategic layer to make changes (if required).

The goal of *monitoring* is to check the effectiveness of the *directing* process.

EVALUATE

With the information gathered in the monitor phase, the information security governance body is able to evaluate the progress of the information security management system. If required, adjustments can be made and the cycle (direct-monitor-evaluate) starts again.

COMMUNICATE

The results of the evaluation phase need to be reported to the stakeholders. The stakeholders can be anyone from suppliers, customers, regulatory authorities and governments. Each stakeholder (depending on the *power/interest* rate) should be managed appropriately. Feedback from the stockholders can constitute new requirements for the evaluation phase. A good example of an important stakeholder is a regulator, who has high power and low interest and introduces new directives with regards to security of data.

ASSURE

Assure is the phase where an independent audit gets executed and recommendations are given to the information security governance body.

(NEN, 2013)

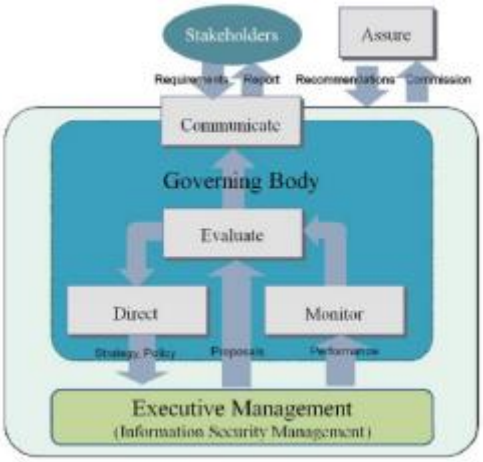


Figure 4. Information Security Governance processes according to the ISO 27014. (NEN, 2013)

4.1.3 Relationship with Information Security Management

Under the information security governing body, the actual execution of information security happens. The implementation of information security within an organisation can be managed using an Information Security Management System (ISMS). To implement a proper Direct-Control Cycle structure, certain frameworks can be used. A popular ISMS best practice is the ISO 27001 standard, which describes the steps required to implement an ISMS within an enterprise. An ISMS itself is not information security governance, however an ISMS is a tool which can help provide a continuous feedback loop for proper information security governance (Disterer, 2013). There are various ISMS frameworks available, most of which are generic and have to be specifically tailored for the organisation in order to be effective. Which ISMS framework best suits a specific organisation depends on which geographical location they are (mainly) doing business in and whether their operating industry has any industry specific compliance requirements. In the United States the ISMS framework NIST 800-53 is common practice and is usually a requirement when dealing with the United States government. In the Netherlands the NEN7510 standard is the preferred ISMS framework for the Dutch hospital environment.

An ISMS provides implementors with guidance on how to implement a general ISMS within an organisation, however it is applicable to any enterprise from any size, thus meaning that the standard itself and its controls are very general. The ISO 27001 standard is the management instrument of the ISMS: within this structure, security controls – which can be found in the ISO 27002 – are implemented. The ISO 27002 describes how a security control could be implemented and what criteria the organisation should follow at minimum; standards like these provide a baseline of security requirements, which can be extended with more security controls depending on the organisation's own requirements. Different ISMS management frameworks have different 'addons' for security controls. (Disterer, 2013)

The goal of compliance is to provide assurance about all the individual controls and the functioning of the management system. This assurance is important for the internal information security governance program (because it confirms or denies that the information security strategy is effective) but is also becoming increasingly important for (future) business partners. More companies are outsourcing bigger parts of their supply chain to focus on their core business meaning that their supply chain is not completely in their own control anymore: in this context, (external) information security assessments are becoming more important for the business continuity of the enterprise.

In practice, some professionals assume that the results of an ISMS audit reflect the maturity of information security within an enterprise, however this is not entirely true (Siponen, 2003). The goal of an ISMS is to support organisations in achieving compliance with laws and regulations. There are a few challenges when assessing information security maturity based on *just* compliance. Compliance isn't necessary security, and neither is the other way around. (Da Veiga & Eloff, 2007)

The ISO 27001 standard can check 11 security domains (consisting of 130 security controls) in total. Compliance is checked in a normative way (checklists), which checks each individual component separately instead of the alignment between controls (Disterer, 2013). However, this mentality is slowly changing into a risk-based approach instead of rule-based, looking at the NEN 7510:2011 standard in comparison with the NEN7510:2017 standard (Zijlstra, 2016). Where in the NEN7510:2011 version there was no attention to the process and alignment of information security management at all, the NEN7510:2017 version is closely related to the ISO 27001 standard.

The general controls also allow for open interpretation, meaning that the same control implemented in two different companies can be completely different in practice. This could be a good thing, because it means that companies are tailoring the controls to their own needs, however it makes comparing and assessing the controls (for an external party) much harder.

Besides the fact that one control isn't the same in other organisations, neither is the scope of the ISMS. Information security governance sets a goal, which indirectly sets a scope for the ISMS. If the goal for example is to have a completely secure *HR department*, then the scope of the ISMS shouldn't be any bigger than that (cost-benefit conclusion). The company could get a certification for that specific scope and can call itself *ISO 27001* certified at that point in time. However, the statement of applicability (the scope - in ISO terms) is only valid for the HR department, meaning a lot is still unknown about the security maturity of that whole organisation. When an organisation is assessing information security (of their suppliers), it is important to assess an ISO 27001 certification on a proper statement of applicability and check if the scope fits in the departments you are dealing with (within that company).

Another issue with information security compliance (especially within large corporations) is the separation of duties. In other industries it is common practice to have a clear separation of duties to reduce risk of malicious activity, like financial transactions which always have to

be checked by an independent party. Legislative changes created by the GDPR (within the European Union) dictate that a data protection officer (DPO) cannot be working within the information security department within that company. However, a DPO is only required if a corporation meets a certain set of requirements. Hospitals do fit these requirements since they employ a large number of employees. A general best practice would be to have a separate internal security audit department from information security management. (von Solms B. , 2005) (ICO, 2019)

Standards like the ISO 27001 are a good baseline and provide a good foundation to build a secure organisation upon. Compliance provides valuable information up to a certain extent: however, the need for compliance has changed. In a fast-paced society, especially with security threats rising so quickly, the need for continuous compliance feedback is higher than ever before. However, compliance auditing is resource intensive, takes time and only provides a snapshot of a selected amount of controls, about a specific moment in time. (Moulton & Coles, 2003) (George, 2013)

To summarize, the need for continuous security assessments has increased by suppliers, customers, regulatory authorities and legislation from (foreign) governments. A large amount of technical controls can be audited automatically using a technical solution; however, information security is also about people, processes and organisational structure. To get a better (futureproof) assessment about the true information security maturity within a company, it could be beneficial to include information security governance as a metric.

4.2 Information Security Governance as a metric

In the previous chapter the role and processes of governance within information security has been established: this helps in determining what the goal of ISG is. In this chapter what is required to implement proper ISG is researched: this information will in turn be used as a foundation for the construction of an ISG maturity model.

When defining the foundation of the ISG maturity model, the first step is to understand the core principles of ISG. What are the main outcomes that ISG should deliver to an organisation? To answer this question the *IT Governance Institute* defined five basic outcomes which will help to create an understanding of what ISG should realize.

Outcome	Description
Strategic Alignment	"*Strategic alignment of information security with business strategy to support organisational objectives.*" (ISACA, 2006)
Risk Management	"*Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.*" (ISACA, 2006)
Resource Management	"*Resource management by utilizing information security knowledge and infrastructure efficiently and effectively.*" (ISACA, 2006)
Performance Measurement	"*Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved.*" (ISACA, 2006)
Value Delivery	"*Value delivery by optimizing information security investments in support of organisational objectives.*" (ISACA, 2006)

These outcomes provide a very generic definition and direction and are not specific enough to be measurable. Gashgari et al. (2017) introduced various principles which should provide guidance when implementing ISG. Gashgari et al. (2017) proposes to combine both *COBIT 4 Information Security* and *ISO 27014 principles* together into guiding principles for ISG. These guiding principles were made more specific by assigning critical success factors to each principle (Gashgari, Walters, & Wills, 2017)(ISO, 2015) (NEN, 2013) (Tu & Yuan, 2014).

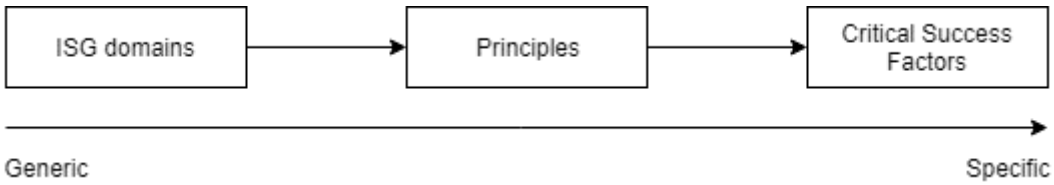


Figure 5. Explanation of proposed model by Gashgari et al. (2017)

The issue with Gashgari's proposed model remains that it does not provide any measurable statements and doesn't define what the criteria are for each *critical success factor*. This means that the proposed model cannot be used as a measuring tool, since it does not provide any details on *how* certain activities *should* be executed.

In order to measure ISG, the researcher has to create an ISG maturity model which specifies the criteria that determine a good level of ISG. The criteria will be the factor that will allow the maturity model to be used as an assessment tool for ISG.

In the following sub-chapters the researcher will go into detail about the identified ISG domains and gain knowledge to identify conditions for good ISG, which later on can be used to develop an ISG maturity model.

4.2.1 Strategic Alignment

The main goals of strategic alignment are to consider information security as an organisation-wide issue, to have visible involvement & leadership, and to operate according to internal and external information security requirements (ISACA, 2016).

The first step into creating strategic alignment is accepting the fact that information security is an organisation-wide issue: people work with applications according to processes, which run on systems, which are being served by supporting infrastructure. If one of the elements in the chain doesn't run well, the whole business process stops. Even though this seems very obvious, the strategic layer has to actively carry out their concern for this issue, since organisational wide support starts at the strategic layer. Top management support for information security is in fact seen as a critical success factor to make any information security program effective: it is required to integrate information security with the business activities (since information security should be seen as a business enabler) (Posthumus & von Solms, 2004).

To achieve proper communication of information security, a compatible organisational structure has to be realized. Various types of generic organisational structures for information security are widely used:

Responsible	CFO
Description	Risks usually have a (in)direct negative financial impact and are therefore commonly combined into a Finance and Risk department. The problem with information security risks is that they are difficult to assess using just monetary values.

Responsible	CTO
Description	Information is usually seen as purely digital and is therefore seen as an IT problem. In practice, the view of a CTO is limited to technical security and is therefore not representative for the whole of information security.

Responsible	CIO
Description	The information department is the bridge between IT and business and focuses on achieving alignment between the two. When alignment is achieved, the business decides and IT supports: the possibility, however, exists that business dictates the way information security will be governed. This is

	not recommended since security can have negative impact on efficiency (which is one of the objectives for a CIO). This structure leads to violation of segregation of duties (Whitman & Mattord, 2014).

Responsible	CISO
Description	Having an information security department is already acknowledging that information security is not part of one specific department but is a shared problem. However, it still sees itself as a separate entity instead of a property of all the other departments.

Responsible	CRO
Description	A Chief Risk Officer is a role existing in mostly large organisations where risk management has been part of the organisations core business for a long period of time already (such as banks). Risks are too important and too difficult to just assess on monetary values for these organisations. The difference between a CRO and CISO is that the CRO focuses on other kinds of risks besides information risks. The CRO focuses on the overall risk program of the organisation and does not therefore focus on one specific type of risk. The CRO seeks integration of a risk program within the organisation (Burgess, 2014).

What the best organisational structure is, depends on the specific organisation considered. These common structures can have positives and negatives depending on the organisation. For example, a very technical organisation could benefit largely from security under a CTO since technical security plays an important role in their core business. (Sinnett, 2015)

Independently of the chosen structure is the need for a CISO, since information security is a decentralized process spread out over different organisational layers. Information Security requires a central entity to coordinate, organize, execute, implement, monitor and respond to information security activities. For security to be part of the strategic part of the organisation, it is essential to have a CISO in the board room. Boards of directors and executives have acknowledged the fact that information security has been one of their priorities for a longer period of time now, however the Chief Information Security Officer (CISO) role is still not widely accepted as a strategic function, even though 60% of the board members understands that a security breach is inevitable. (Nominet, 2019)

The problem with holding just the CISO responsible is a conflict of interest, since security has to be applied in different departments: this means that a CISO has to cope with other board members and managers, who have different KPI's and objectives than the CISO. These conflicting interests cannot work together and will result in a CISO being held responsible for security, without him/her having the authority to make the required changes. A clear

example could be between a CISO and CIO, where the CIO's main objective is to create efficiency: the fact that security is usually defined as waste creates a conflict of interest between the two figures. The conflict of interest is not a new phenomenon and has been observed before: an example of this is the conflict of interest between *operations* and *development* departments, which has been solved with the DevOps mindset (Leffingwell, 2010). What we can learn from the DevOps mindset is that it is required from all parties to have awareness about each other's goals, create mutual awareness, support each other and understand that all parties are working to achieve the organisations mission. In terms of information security, it is important (for other board members) to realize that security is a business enabler and a safeguard to business continuity, opposed to a business disabler. The ideal situation in the board room would be to make multiple board members responsible for information security, especially when there is a conflict of interest, which forces the CISO and other board members to work together and understand each other's point of view. (Curry, 2017)

To guard over the process of responsibility, a helpful tool could be to implement the RACI methodology. RACI maps all the activities and stakeholders against who is responsible, accountable, should be consulted and who to keep informed.

Roles, responsibilities and policies have to be clearly defined and enforced to achieve strategic alignment. Strategic management can show their support by officially approving IS policies and by communicating their existence. To check the enforcement of these roles, responsibilities and policies, compliance should be checked regularly to make sure that policies are still effective and that significant changes haven't occurred.

In summary, it is important to have a c-level role to oversee the whole information security process, however the responsibility should be shared equally among the whole organisation: this will create strategic alignment and help creating a shared goal. Getting people to all be responsible starts with proper policies and procedures: these not only have to be created, but also have to be properly implemented. To implement the policies and procedures means that people know that the policies exist, what their role in those policies is, and what the ultimate objective of those policies is. Leadership and the creation of organisational support starts at the strategic layer and is essential for any organisation which aims to improve its security. Security should be integrated within business activities and to ensure proper strategic alignment it is required to work conform the set rules, requirements and policies.

4.2.2 Risk Management

Blakley et al. (2001) defined risk as "*the possibility of an event which would reduce the value of the business were it to occur*". How a business deals with unexpected events is defined in its risk management processes. It is important to make a strong distinction between the types of risks because risk management can focus on different things. In the context of hospitals, risks usually refer to patients' safety risks, whereas banks usually talk about financial risk. A large implementation of a risk management process, which continuously provides information, is essential for strategic management to make any rational decision. A company's attitude towards risk management is largely defined by its strategy, culture, risk

appetite and ability to change (George, 2013). Risk management is the main driver behind governance and helps to seize opportunities and minimize loss.

When talking about risk management it is important to know what a risk consists of, because in practice the terms risks and vulnerability are being used interchangeably, while they should not be. A risk can be formulated using the following formula (Ghazouani et al., 2014):

Risk = Vulnerability x Threat x Impact

Risk management can be explained using a practical example:

The **asset** is a house. The **threat** is the (rising) sea. We can't remove or relocate the sea: the threat is always there. If the sea would overflow, the house would become completely unusable (**impact**). To still be able to use the asset, we implemented a **security control** (mitigation) called a dyke. The dyke separates the danger from the assets. However, after a certain time a crack could endanger the effectiveness of the dyke: this is called a **vulnerability**. This vulnerability could be prevented by performing maintenance to the dyke. However, it is not possible to always be around the dyke to check if somebody complied with the regular maintenance schedule: this is where compliance and audit come into play.

Concept	**Definition**
Asset	An asset is something owned by an entity, which can be in any form: this can be information but could also be people.
Threat	This can be anything that can potentially endanger an owned asset or cause harm, like a criminal hacker or a natural disaster etc.
Vulnerability	A vulnerability is a weakness which can be exploited (by a threat) to cause an owned asset harm.
Impact	The impact is the effect of an exploited vulnerability by a threat on an owned asset. The impact is usually measured against the confidentiality, availability and integrity in information security context; however, this could also be measured, for example, by reputational damage.
Security Control	A security control is a measure which is implemented to deal with the risk. This can be executed by minimizing the impact or solving the vulnerability. A security control can be avoided, accepted, reduced or transferred.

(Coertze, 2012)

Risk management is the main driver behind information security in general, and analysing risks according to the formula helps to create a strategy on how to address each individual risk, since aiming to mitigate every risk completely is not a viable option. Neither is every risk a significant danger to the organisation: this however largely depends on the context.
A vulnerability with a big impact but without a threat is not necessarily a big risk, neither is a big threat without vulnerabilities. The aim is not to be completely risk free, but to be in control and be able to adapt quickly to (un)known risks. For an organisation it is important to assess which assets are important and execute regular risk and threat assessments according

to a formalized process, since risk management is a reoccurring event which has to be repeatable to be effective.

The ISO 31000 risk framework can be used to introduce risk management within the organisation: it helps to create a mutual understanding about risk management (within different contexts), create a shared terminology and implement a continuous process. The ISO 31000 is a good tool when executing Enterprise Risk Management (ERM). A standard that can be used to focus more on applying information security risk management and the process around information risk management, is the ISO 27005. The ISO 27005 is more of an implementation standard and advices about risk assessments and treatments. The ISO 31000 and ISO 27005 can be used together for the total coverage of the risk management process (Kosutic, 2014). There are other standards which can be used to implement risk management, such as COSO, NIST or OCTAVE; however, for most organisations it is important that the standard fits with the same methodology their ISMS is supposed to be compliant with.

In general, every risk management process starts with the establishment of the context. This means that criteria, scope, boundaries, roles and responsibilities have to be established for the information security risk management process. After the context has been established, the risk assessment process starts. The basic steps of risk a risk assessment are: risk identification, risk analysis and risk evaluation. It is important to involve the required people in the risk assessment phase because this has benefits for the whole enterprise. Instead of using a traditional top down approach for risk management, it could be beneficial to take a collaborative approach towards risk assessment. This way the risk assessment will give results about every organisational level and therefore provide a complete and accurate view of the organisational risks (Marosin, van der Linden, & Sousa, 2014).

After the identification and classification of the organisation's assets, the next step is to collect information about vulnerabilities and threats regarding the assets. Together with the assets' classification, it is now possible to calculate the risk. Once the risk is known, the risk has to be analysed in order to then determine which actions to undertake to make the risk fit in the organisation's risk strategy.

The strategy determines how (un)identified risks are handled. The goal is to be in control, meaning that the aim is to have a balanced approach towards risk depending on the risk appetite of the organisation. Once a risk has been identified, it is possible to either avoid, transfer, mitigate or accept the risk.

There are three types of approaches towards risk management:

1. Reactive

The reactive approach is when security has a negative reputation within the organisation and is seen as a business encumber. Other characteristics of a reactive approach is the lack of management support, lack of resources (people, money and time), no reporting and at best, security issues are solved at the tactical level. The goal of the reactive approach is to

block every threat that arises at that point in time. Preventive measures are mainly missing (*curing when occurring*) (George, 2013).

2. Compliance-Driven

This approach uses the same threat defence as the reactive approach, extended with control-based security which leads to a check-box mentality. In this approach security is seen as a liability and the organisation does not pursue risk management with a clear strategy in mind; rather, they only make sure to tick the boxes – by being compliant to the standards – because they are afraid of the consequences resulting from not doing it. The goal is to be compliant with laws, regulations and (industry specific) standards: the motive behind the goal is, however, not to be secure but to be compliant, since being non-compliant can be a danger to the business continuity in some sectors. When the compliance-driven approach is used, the goal is to pass an audit and get certified: this causes the organisation to aim for the minimum requirements of the audit (George, 2013).

3. Risk-Based

A risk-based approach is pro-active and interconnected. In this case, a risk-based information security program, which is continuously monitored and improved, is implemented. The motive is to be secure and prevent bad things from happening. Compliance is the baseline, but the whole organisation wants to improve in both technical and organisational layers and security is seen as a business enabler and essential for business continuity.

In today's society the need for a risk-based approach is essential since the reactive-approach is not fulfilling anymore since security threats are always present. Security must be dealt with in a pro-active way, for business continuity, law and regulations since damage from security threats can be permanent, for example the damage from a data leak is not reversible. The compliance-driven approach is still very common in organisations since stakeholders want assurance. However, compliance is not the same as security. The compliance-driven approach is therefore an indicator that information security is still seen as a necessity, and security requirements are kept at a minimum.

The risk-based approach mainly consists of a positive attitude towards security, which is seen as a business enabler. A risk-based approach consists of continuous compliance, continuous monitoring and a risk based-remediation. With a risk-based approach the focus is on preventing and minimizing risks, and therefore on reducing cost. The extent to which a company minimizes risks depends on its risk strategy. Various risk postures can be adopted, such as a risk avoiding, accepting or a natural strategy. Experts from different departments are working together with their domain and expert knowledge to identify risk and create fitting and effective security controls. (George, 2013) (Lazarikos, 2015)

There are risks we know, we know we don't know and risks we don't know, we don't know (Donald Rumsfeld, 2002).

Because not every risk can be known and planned for, risk management should always consider a general strategy to deal with the unknown. These kinds of scenarios are managed by business continuity management (BCM).

Since business continuity is primary focused at preserving the availability of the organisation, it has some overlap with information security; however, the description of business continuity is limited within the ISO 27001 standard. In practice, the ISO 27001 standard only recommends the writing of a *disaster recovery plan* (DRP), though business continuity is much more than that. The ISO 22301 is the standard for *business* continuity, which provides the implementor with the tools to write a *business continuity policy*, *impact analysis*, *continuity strategy*, *continuity plan* and describes how the plans should be *tested*. Both the ISO 27001 standard and ISO 22301 standard are using the same management system and could therefore be implemented together instead as a separate management system for business continuity. This would reduce cost since business continuity management can be seen as a part of risk management with a different approach. BCM is not be that different from the ISO 27001 standard and can even been seen as part of it, however it should be extended beyond the minimal requirements stated by the ISO 27001 standard (Zijlstra, 2013) (Kosutic, 2015). It should be mentioned that BCM doesn't only focus on IT or information, since it is about the organisation's core business - where IT is becoming an increasingly important part of. For large organisations like a hospital the scope of BCM is enormous, therefore such organisations have to be prepared for an enormous amount of disaster scenarios. Because of the size of this scope, it could be beneficial to have a separate business continuity team; however, the collaboration between the risk management department and the business continuity team should be seen as priority number one, since this will lead to better BC plans and less duplication of efforts.

Business continuity focuses primary on the core business processes of the organisation, but it is also important for businesses to look at third party processes that their core business is dependent on. It is important to assess the security of third-party vendors thoroughly, in order for one own's organisational availability to not be dependent on the availability of another organisation.

4.2.3 Value Delivery

Value delivery is where investments and risk management collide. The strategy an organisation chooses to execute risk management plays an important role in regard to all the future decisions. The investment in security will be determined based on the risk strategy. A good amount of security investments is when "*goals for security are achieved and an acceptable risk posture is attained by the organisation at the lowest possible cost*" (ISACA, 2006). It is important to notice that investments and costs mentioned in this paragraph to not only refer to monetary value but also to time, energy, skill costs etc.

When a risk accepting strategy is applied, the investment will be less heavy compared to when the organisation choses to be risk avoiding (which will demand more from resources). The objective of value delivery is to determine how much strain the information security controls are putting on the organisation, and if is this in line with the selected strategy. The strain of information security on the organisation can be defined in terms of financial value but also in terms of people, processes and other kinds of resources.

A good way to evaluate investments and information security is to create business cases upfront and evaluate the results with proper performance measurements. Within information security, it is very hard to evaluate business cases based on return on investment, since not all business cases can directly be translated in a monetary value. How do you determine what the price of security is? The best way to identify and create a security control is by using risk management (Tu & Yuan, 2014).

Security investments can be assessed according to the return on investment combined with a risk variable: this mindset is applied when calculating risks based on the *Annualized Loss Expectancy* (ALE) formula. The definition of the ALE is the expected monetary loss that can be expected for an asset due to a risk over a one-year period (Ciampa, 2011). To evaluate information security investments, it is important to have a proper risk assessment process with all the domain experts of the whole enterprise involved. When measuring the possible loss of a risk, it is important to consider how much financial damage the enterprise would suffer over a certain period of time in case something happens to the organisation's availability, integrity or confidentiality. Depending on the type of organisation, the impact can be different. What is most important for the survival of the organisation is part of the business continuity plan (ISO, 2018).

For example, in the hospital environment the confidentiality of data is not as high of a priority as are its integrity and availability. It is unfortunate if a medical dossier is viewed by the wrong doctor, however a patient's health won't be in (direct) danger because of it. On the other hand, if an operation cannot be executed because certain systems are unavailable during a medical emergency, this could have a direct effect on a patient. The same goes for the integrity of the data: consulting wrong data could lead to wrong diagnosis or even to a wrong execution of a medical procedure - like demonstrated by researchers from the Ben-Gurion University, where they were able to manipulate CT and MRI-scanners on the fly by inserting and removing tumours from scans; the manipulated data could not be identified by medical specialists (Zetter, 2019).

There are various scenarios that can be thought of with regards to the availability, integrity and confidentiality of the hospitals. It is extremely difficult to attach a monetary value to risks such as those of a life and death scenario.

Calculation example

Say for example a vulnerability has a high change of impacting the availability of a critical system which costs the business €100K for every hour it is not available. If the vulnerability occurs, it will take at minimum 2 hours to solve and at maximum 6 hours. The business cost of this vulnerability will be around €400K. By adding the cost to solve the vulnerability and the business cost, the total price of the possible financial damage of the vulnerability can be calculated. Depending on the type of risk (like a data-breach) this can be extended with a fine from certain regulators. This is the cost *if* the vulnerability happens: however, how likely is it to happen? The likelihood can be calculated with *vulnerability x threat*. If the likelihood that a vulnerability will occur is once every ten years, the cost of the vulnerability suddenly

becomes €40K every year. Depending on the price of a security control (and the maintenance of it) it could be a viable option to accept, mitigate or transfer the risk. However, this reasoning is only considering the financial part of a risk: there are other consequences at play which are harder to convert into a monetary value such as reputation damage. How much damage a company is willing to take is called risk appetite.

Besides executing a financial risk investment analysis, it is important for value delivery to check if security activities are executed in a cost-effective manner with regards to human-investments in terms of energy, time and resources.

In business, investments are usually seen as value when they deliver benefits to a customer or solve their issues. This customer can be the internal employees or the customers of the company. In terms of value delivery for non-financial ISG, value can be defined in terms of *trust* and *enablement of services* (ISACA, 2006).

An important metric to measure value delivery is the amount of perceived enablement of services. Security controls do not only safeguard the organisation's processes, they also enable organisations to pursue new (technological) changes for business benefits, for example data exchange between different geographically located branches of a company (if the organisation does that because of the security investment, that shows that security controls enabled the company to deploy new opportunities – which it would not have done before without trust).

Perceived trust is one of the main pillars in the information security industry. How is it possible to explain that something is well protected when it is not (directly) visible - since security is not a functional requirement? There is not one metric that explains that everything is secure. To create trust in the security program it is required to provide the end user with just the right amount of details about security and deliver the right amount of transparency. Transparency is required to create understanding and show that value is delivered, instead of untraceable *security by obscurity*. Security by obscurity is defined as "*keeping security mechanisms inside the black box and disabling explanations for transparency*" (Pieters, 2010).

For value delivery it is important to consider the financial value, but also to measure the new enablement of services and the amount of trust in information security (in terms of people and processes).

To summarize, for the information security governance body it is important to implement a proper strategy which encourages a risk-based approach, where domain experts work together to identify, assess and solve risks. The governance body has to guide, facilitate and monitor the process carefully and oversee the decision making and make sure the financial needs are met to align the security controls with the current and future business needs. Besides the financial needs it is also required to consider the clinical workflow and monitor if security doesn't require an excessive amount of resources in terms of time, energy and proceedings.

(ISO, 2018)

4.2.4 Resource Management

When investments have been made into information security it is smart to actually use the resources and embed these within the organisation. It would be ineffective to reinvent the wheel for every project. To use the resources (people, processes, knowledge and technology) effectively every time, it is required to capture and disseminate knowledge within the organisation. For processes, this can be achieved by standardizing them; for information, this can be achieved by incorporating the knowledge into standard project plans; for people, this could be the spreading of information about security resources that already exist through proper communication channels.

To achieve resource optimization, it is important to spread awareness about information security, where information can be gathered, where tools can be found etc. By making information security part of the culture, for example, employees will automatically seek information security knowledge when they start a new project, since it is part of their normal operations.

4.2.5 Performance Measurement

Security exists to support the business: it should be a safeguard and not hinder the business in any way. When security is not supporting the business or is even hindering the business, employees will find a way around the security controls. This 'alternative' route becomes a shadow process and is usually insecure and, even more importantly, unknown. Security controls therefore have to be established in cooperation with all layers of the organisation.

The performance of the security program has to be measured in terms of effectiveness. As described in chapter 4.2.3, it is very difficult to make a business cases for security controls using traditional metrics. However, it is also important to measure the intangible, which is required to measure the full effectiveness of an information security program.

There are various benefits of using metrics within information security:

- They help creating increased accountability, because the metrics will help identify if specific security controls are implemented wrongly, not at all, or are just ineffective. A specific metrics is able to identify and trace back to the personnel responsible for the specific metric and its attributes.
- Specific controls can be linked to the organisation's strategic goals and objectives and are therefore helpful to evaluate the whole information security program effectiveness.
- They can be used to demonstrate compliance with laws, rules and regulations.
- They constitute a new, quantifiable input and feedback for resource allocation.

(NIST, 2008)

To realize these four benefits, three types of measurements should be realized:

1. Implementation measurements

Implementation metrics are about the implementation of information security programs and their controls, policies and procedures. These measurements are not limited to

organisational controls but also include technical security controls. An example of these kinds of measurements is: "*The percentage of technical systems protected with an anti-virus solution*". (NIST, 2008)

2. Effectiveness and Efficiency Measures

Effectiveness and efficiency metrics are used to check, monitor and improve the implementation measurements. These metrics are important because once a metric is implemented it provides certain defending capabilities at that point in time, however these have to be continuously monitored and improved since erosion can occur and a security control can lose its effectiveness. (Jalali & Kaiser, 2018)

To measure the effectiveness from the previous example, the following metric could be used: "*The percentage of information security incidents caused by an out-of-date anti-virus solution*". If the percentage of information security incidents caused by an out-of-date anti-virus solution is high, that would mean that the security control is not effective and should be re-evaluated. If the percentage is low that would mean the control is implemented properly and is effective. (NIST, 2008)

3. Impact Measures

The impact measure looks at the impact of a security control on the whole business. Say for example *we implemented an anti-virus solution*, and *we see a significant decrease in information security incidents caused by viruses*: what does this mean for the business? Metrics such as these could be: "*By how many percent did the availability of our services increase?*" or "*What percentage of the total revenue was spent on disaster recovery specialists?*".

(NIST, 2008)

It is important to have timely, complete and transparent reporting of information security through implementation, effectiveness, efficiency and impact measures. These measures have to be the basis for constant improvement of the information security program. Which metric is important for a specific information security program depends on what the current situation regarding information security is, and what the desired situation is.

It has to be noted that there is a clear distinction between security governance and security management metrics. Security management is more focused on execution (operations), enforcing policies, deploying resources, executing implementations and 'doing things right'. On the other hand, security governance is more focused on planning, setting policies, allocating resources, keeping oversight and 'doing the right things'. Implementation, effectiveness and efficiency measures will generally be more used to create security management metrics, whereas security governance will be looking at impact measures.

Pironti (2007) created the following example metrics framework for information security governance:

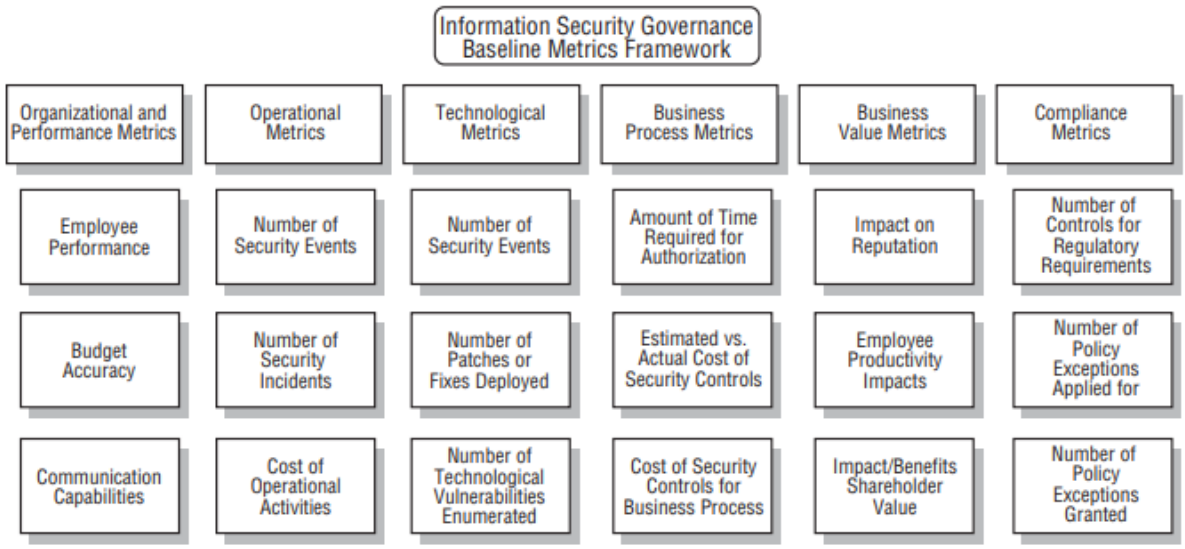


Figure 6. Example of Information Security Governance Metrics Framework. (Pironti, 2007)

The overall goal of securing an organisation is to prevent information security incidents from happening. For that reason, the amount of information security incidents which harmed the organisation could be a good measurement for information security governance.

Another important performance metric for information security governance is the perceived competence of the board room with regards to security governance. The perceived competence by the employees of the company about the board room says a lot about the validity of all the other metrics like strategic alignment, value delivery and resource management.

4.3 Information Security Governance challenges in the hospital environment

For an ISG maturity model to be specific for a certain industry it is important to look at trends within the industry. According to Williams et al. (2015) there are two major specific challenges in the hospital industry, which could have a possible relationship with ISG:

- Connected medical devices are a trend which is becoming increasingly important in the medical environment since these can generate better medical results, increase efficiency and, maybe even more importantly, reduce operational cost. (Zurkus, 2019)
- Hospitals are large organisations who are heavily reliant on reliable, confidential and available information. In order to design practical and effective security controls within a hospital, it is important to consider the clinical workflow. (Williams, 2001) The balance between security and workability is a challenge within the hospital environment because of the high stakes involved in emergency, life-and-death situations. Furthermore workability, in a hospital environment, does not only have to consider information security but also patient safety.

In the next paragraphs the researcher will determine if, and how these challenges are related to information security governance.

4.3.1 Connected medical devices

Connected medical devices are "*good for patient care, because it facilitates data integration, patient engagement, and clinical support*", however the implementation and security of connected medical devices brings challenges to the governance board with regards to the hospitals changing IT landscape. (Wetsman, 2019)

Like any (software) product, updates are required to improve its quality and keep the product safe. In the case of medical equipment, the information produced by the device has to be completely trustworthy, since a small deviation caused by a programming error can have serious consequences on patient health. Hospitals and manufactures of medical devices are not keen on updating (functional) working medical equipment. This is an understandable argument, since the sensitivity to errors is high and can lead to serious patient health risks, as shown by real incident statistics from the United Kingdom (Gregory, 2014).

Besides not being keen on updating, there are also a lot of practical implications which withholds hospitals and manufactures from updating connected medical devices. Medical devices undergo a strict assessment before they can be used in practice: this mainly is done to minimize risks regarding patient health.

The ISO 13485 is a compliance standard which focuses on the quality management system of medical devices. The downside of this compliance standard is the lack of software requirements; for that reason, The Netherlands has implemented the European *Medical Device Directive* which declared medical software as being a medical tool. In the United States and European Union all medical device software has to be assessed against the IEC 62304: this standard considers the full software life cycle of medical device software; however, it excludes cyber security considerations or network security (MT-Integraal, 2015). Even if a hospital or manufacture would want to update their medical devices more frequently (for security reasons), this would trigger a compliance certification process against the IEC 62304, which is time and resource demanding for medical device manufacturers (Williams & Woodward, 2015). Besides the impracticality of constantly having to recertify for compliance reasons, the whole recertifying process does not (necessarily) provide any security for information security vulnerabilities.

An example like WannaCry, which was responsible for multiple attacks on hospitals (but not limited to) around the globe, showed how vulnerable environments without up-to-date systems are. Even when it is not possible to update medical devices, WannaCry showed that it is important to have an overview of your assets, so that it is possible to identify vulnerable systems and take appropriate measures. Vulnerabilities in medical devices were already inherently existing but are enlarged by the connectedness property of devices which leads to the enlargement of the threat landscape and thus pose a larger risk of malicious intent. (Wetsman, 2019)

The researcher can conclude that it is hard to fix vulnerabilities by updating the medical equipment because:

- There is the risk of a malfunctioning functional requirements, which could form a patient health risk.
- A re-certification against standards for every software update is not a viable solution.
- Of practical difficulties of applying daily patching over a large amount of (medical) devices.

When software patching is not possible, it is not always a viable option to replace a medical device, since investments in new medical devices can cost up to millions of dollars. The challenge for information security governance is to find a way to work with vulnerable connected medical devices while still being resilient against threats (like WannaCry).

Connected medical devices and security governance

To make vulnerable systems resilient against external threats it is required to use a different approach, when patching or replacing them is not an option.

A connected medical device can be attacked through the digital network they are attached to, or by gaining physical access to the device. It is difficult to constantly protect the physical device within hospitals because these are large environments with an open perimeter. Furthermore, malicious programs can spread to other medical devices over the digital network or can even get infected by other medical devices in the same network. In order to add resilience to the medical devices which can't be physically protected, it could be beneficial to create network segmentation and apply specific technical security controls to monitor, detect and identify data leaks or other malicious tampering (Buecker, Andreas, & Paisley, 2008) (Williams & Woodward, 2015).

Security controls which do not directly solve the vulnerability but do provide a way to deal with a risk are called "*compensating security controls*" and are an alternative way to fulfil the organisation's security requirements when constraints (such as non-updateable devices) apply.

Actively checking network and access monitoring helps to create reporting and feedback loops, which help the governing body to be in control. The combination of proper physical security - where possible, and compensating security controls, creates a multiple layer defence barrier, which should give the hospital resilience against attacks on connected medical devices. (Buecker, Andreas, & Paisley, 2008)

For information security governance in the hospital environment it is a priority to have a specific policy about the secure implementation of medical devices, which creates a multiple defence layer type of protection together with compensating controls. Also, the governance body should be aware of its assets and have classified them to be in control.

4.3.2 Workability

Workability within information security is the degree to which the organisation is able to execute a regular business task in a safe and efficient way. A more practical explanation of workability is the integration of security with business processes and determining how the end-user experiences the usability and user-friendliness of a security control. Workability is

the part of information security where practical security solutions and the clinical work processes collide. The integration of security controls within the business process is one of the requirements to fulfil for effective security.

Information security is about balance and being in control; too many security controls can paralyze an organisation or will introduce insecure shadow processes. Especially within hospitals, workability is an important issue since the stakes are different from a typical office organisation. If security blocks or delays a 'regular' business process, it will at most lead to a financial loss; instead, within the hospital environment it could cause serious harm to the patient (in case of a medical emergency). Choi et al. (2019) has calculated that the 30-day mortality rate (regarding acute medical emergencies) within hospitals significantly increases after a data breach has occurred. The mortality rate increases because of the extra security controls implemented by security departments and the delays these introduce in the caregiving process (Choi & Johnson, 2019).

4.3.3 Zero Trust as a solution

For security to be effective and workable, it could be feasible to look at the concept of Zero Trust. With the Zero Trust methodology, enforcement of information security doesn't happen on the physical level anymore but on other layers (Pratt, 2018). The Zero Trust methodology could be a beneficial solution, besides proper information security governance, for both the implementation of secure connected devices and workability of security controls, as stated by Yuan et al. (2018).

Zero Trust is not a tool or solution which can be purchased. Zero Trust is a methodology, a different approach to the implementation of information security. Zero Trusts is based on the following five principles (Kindervag, 2016):

- "Ensure all resources are accessed securely regardless of location"
- "Adopt a least privilege strategy and strictly enforce access control"
- "Inspect and log all traffic"
- "Always verify and never trust"
- "The network is designed from the inside out"

Zero Trust assumes that nothing is safe, since it disregards whether something is inside or outside a perimeter, which is beneficial in a hospital environment where a perimeter is difficult to secure. The Zero Trust concept could be a possible solution for connected medical devices and workability challenges; Zero Trust also leads to tailored security by creating micro-segmentation based on the identification of an asset (Pratt, 2018). Micro-segmentation can be created by using (usually already existing) technologies like network segmentation and firewalls. Authentication and authorization can be enforced by multi-factor authentication and proper configuration of services.

There are various models that can be used to implement a Zero Trust solution. The first step in the Zero-Trust process is to start with creating network zoning (using VLAN's) from the inside out. By creating network zones, different perimeters are created which can all have an individual set of access and privilege rights – called an authorization matrix. Which security

requirements, access and privilege rights have to be created depends on people, devices, departments, information and networks. In the authorization matrix employees would be assigned to one or multiple departments. The department properties contain employees with access rights. For each department different security requirements are created (depending on their operations and associated connected medical devices). For example, a medical research department which requires the highest degree of protection should have more security controls then departments where no high value information flows at all. (Buecker, Andreas, & Paisley, 2008)

One of the important aspects of information security governance with Zero Trust is to have an updated access policy which defines which employee roles belong to which department and which security requirements are required to each zone. The Zero Trust concept consists of verifying a user, validating a device and limiting access and privileges.

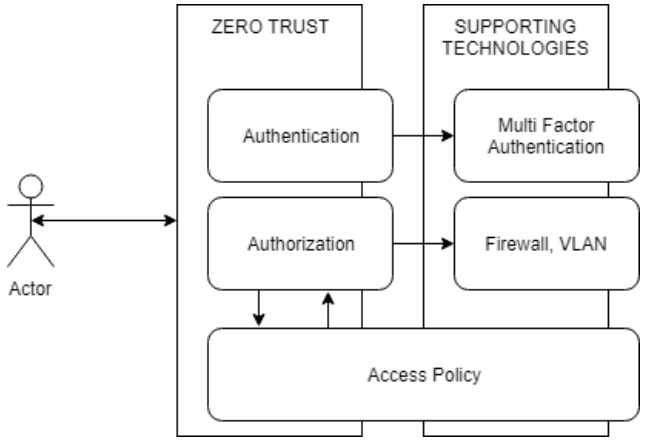


Figure 7. A simplified overview of Zero Trust.

In hospitals there are departments who would like to have no security at all, in order to provide the patient with the fastest care available - like the emergency room. An emergency room is difficult to physically protect (through a perimeter), but at the same time requires a high level of security because of the medical information flowing through it. However, multi-factor authentication would hinder the emergency process too much. One of the solutions would be to disable all authentication mechanisms and create separate network segments for the ER room, as well as investing heavily in monitoring and detection solutions like logging – as stated in the principles of Zero Trust. The need for security is there, however saving a human's life is more important: therefore, implementing security controls which hinder the medical process are not allowed. In this situation, controls which focus on detection and monitoring can still provide a lot of useful information (in case a hack happens), while not hindering the medical process at all.

When establishing an access policy, it is important to determine the level of security required through the cooperation with a Chief Medical Information Officer (CMIO). A CMIO is a new role introduced to bridge the gap between the end users (medical employees) and IT. CMIOs are largely doctors who have experience with IT and could provide the governance board with important information to increase the adoption and integration of effective and

workable security. Since the supporting technologies of Zero Trust are largely technical implementations, a CMIO could provide valuable information while maintaining an objective view. CMIOs are essential figures for the future digitalization of hospitals (subject to technological changes like e-Health and cyber security) because they have a large understanding of clinical care. (Peters, 2018)

To summarize, the concept of Zero Trust provides an alternative view on how security should be tailored towards individuals and departments. The key is to secure the hospital where possible and monitor extensively where workability has the priority, since at the end of the day security is a business enabler and not the other way around. The basis for Zero Trust lies in the access and implementation policy, which is being enforced by technologies like MFA, firewalls and network zoning. In this era of digital change and information security challenges, a CMIO is a new, essential role which can support hospitals in the process of adapting to changes and in facing the challenges that come with them.

5 Measuring Information Security Governance

The goal of a maturity model is to "provide a way for organisations to approach problems and challenges in a structured way, by providing both a benchmark against which to assess capabilities and a roadmap for improving them." (Caralli, Knight, & Montgomery, 2012)

The purpose of the model in this research is to capture the current status of information security governance within hospitals in a systematic and defined way. This tool should be used to determine a current situation and support hospitals in improving their ISG; this could potentially lead to better decision-making about information security in hospital boardrooms.

To systematically measure information security governance across an industry, the realization of a systematic maturity framework is essential. In order to systematically measure anything, conditions have to be clear and defined, otherwise the model could be interpreted differently, and results may become incomparable. This is the issue with Gashgari's proposed information security governance framework, which does not provide any measurable statements and doesn't define what the conditions are for each attribute; this means that such proposed framework isn't suitable to be used as a measuring tool, since it does not provide any details on *how* certain requirements *should* be executed. The same issue arises with the ISO 27014, which defines 6 unmeasurable principles that can only be used as guiding statements.

5.1 Structure

There currently are no proper information security governance maturity models which can be used to measure ISG. Frameworks have been proposed, which however are not detailed enough and focus on IT governance and information security management.

A maturity model can be categorized as a progression model or a capability model. A progression model 'measures' maturity by the presence of a specific characteristic, indicator or attribute, instead of looking at the attributes that specifically define maturity. It can be stated that progression models don't really live up to the expectations of a maturity model since they don't provide any capability maturity.
A capability model also looks at the presence of specific characteristics but adds another dimension to the model, implementing levels which "*reflect the maturity of the culture and the degree to which the capabilities are embedded in the culture*". Compared to the progression model, a capability model measures more than just the presence of certain activities, since it also focuses on the ability of the organisation to execute these specific activities. (Caralli, Knight, & Montgomery, 2012)

A well-established example of a capability model is the Capability Maturity Model Integration (CMMI). The CMMI model is a generic model which tries to describe the level of integration of specific activities; the CMMI model consists of five, distinct maturity levels. Based on the standard definition of CMMI, the researcher has to create new maturity level descriptions which are geared towards information security governance. To do this, the researcher chose to integrate the *direct*, *control* and *evaluate* process steps as described in the ISO 27014 - explained in chapter 4.1.3, together with the general descriptions of the

CMMI maturity levels. This aims to establish a clear link between the created maturity levels and the steps which can be taken to execute proper information security governance - according to the ISO 27014. A graphical representation of the linkage between the maturity levels and the ISO 27014 is displayed in figure:

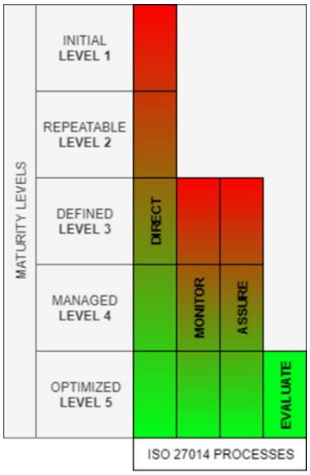


Figure 8. Graphical representation of the information security governance maturity levels.

In the next table there is a description of every maturity level:

Maturity Level	Description
Initial	This level is the starting point for organisations; directing is done in an informal way without a strategy, direction, objective or policy. Issues are solely dealt with in a reactive manner. There is no monitoring and evaluating of performance at all.
Repeatable	Organisations are directing in a more formal way; there are policies, objectives and a strategy, however the focus is limited, not organisation-wide and an overview is missing. The limited things the organisation does are starting to become repeatable however there is no monitoring and evaluating at all.
Defined	The organisation is directing in a formal way, is organisation-wide focused and the important aspects are considered. The organisation is trying to improve its processes because of a compliance-driven mindset. The organisation is starting to implement monitoring and seeks validation through audits because of regulatory requirements.
Managed	The organisation has a well-established information security management system which effectiveness is actively being monitored with proper metrics, and it proactively reacts to issues; the organisation seeks validation and assurance by in-depended audits and the organisation is in control. The organisation actively works to create strategic alignment between business and security and to create organisational-wide support for information security.
Optimized	The organisation is in full control of its information security and sees compliance as a baseline. The organisation monitors its information security management systems' effectiveness and is constantly trying to improve itself by evaluating and creating improvement plans. The

	governing body is aiming to deliver as much perceived value and trust as possible.

5.2 Maturity model definitions

Maturity models can be used for different goals within different contexts; however, maturity models always follow a consistent set of essential components. *Levels* are the defined transitional states in a maturity model. *Model domains* group *attributes* into an area of importance for a specific subject matter. Multiple subject matters (or *capability domains*) can together form the maturity of one large concept. *Attributes* are the most detailed core components of a maturity model: they are grouped together by the model domains and consist of different levels. Attributes can exist in the form of characteristics, indicators, practices, standards, expert knowledge or processes. The attributes display the maturity of specific qualities with regards to the model domain. (Caralli, Knight, & Montgomery, 2012)

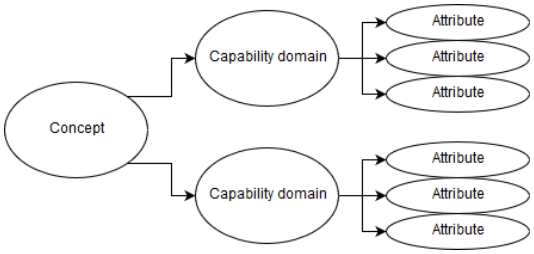


Figure 9. Overview of maturity model components.

5.3 Presentation of results

The presentation of results is what people in the end will see and use. The goal of the model is that it should be understandable but also provide enough detail for it to be used as an improvement tool.

A one-dimensional model will focus solely on one target measure, whereas a multi-dimensional model can focus on multiple divergent goals. (Mettler, 2011) Because ISG isn't measurable as one metric, a one-dimensional model would be too simplistic, inflexible, and would not provide enough valuable information which the organisation can use to make improvements.

De Bruin et al. (2005) proposes the use of a two-dimensional maturity model, since this provides the organisation with "*a better understanding of existing domain capabilities, enables benchmarking against a range of competitors, enables greater efficiency in the utilization of resources in improving domain capabilities and presents an opportunity for improved success in the domain*." (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005) In order to create a two-dimensional maturity model, De Bruin et al. (2005) propose to use a 'stage-gate' approach. In a stage-gate approach each individual capability domain consists of a set of attributes, which together form the evaluation of a single capability domain. Using this method, the maturity model integrates additional layers of detail. "*A layered model enables an organisation to gain a deeper understanding of their relative strengths and weaknesses in the domain and to target specific improvement strategies thereby enabling more efficient resource allocation. The ability to drill-down through the maturity assessment enables the*

maturity model to be tailored to varying needs of multiple audiences." (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005).

To display a two-dimensional maturity model, different visualizations can be used. For the ISG maturity model the use of a *radar plot* as a visual representation of the highest abstraction layer would be appropriate, since it would instantly show the maturity for each single capability domain; this can be a useful visualization method when comparing benchmarks, and is suited for board of directors who only want a quick overview of the current status of ISG.

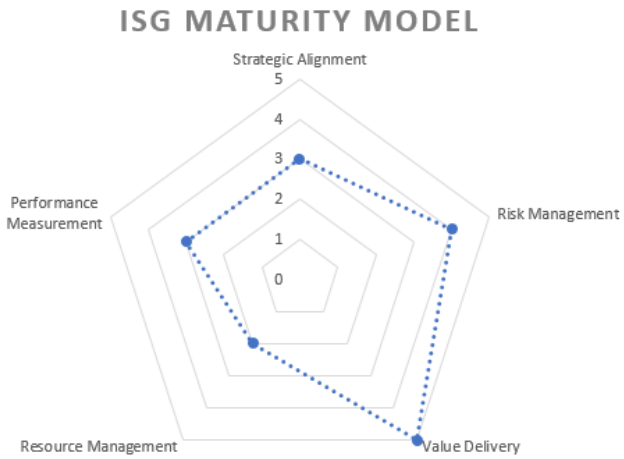


Figure 10. Example of a Radar Plot

Another proposed visual representation next to the spider plot is a *matrix diagram*, which can be used when a deeper insight into the attributes is required; this diagram fits with the by stage-gate proposed additional layered approach.

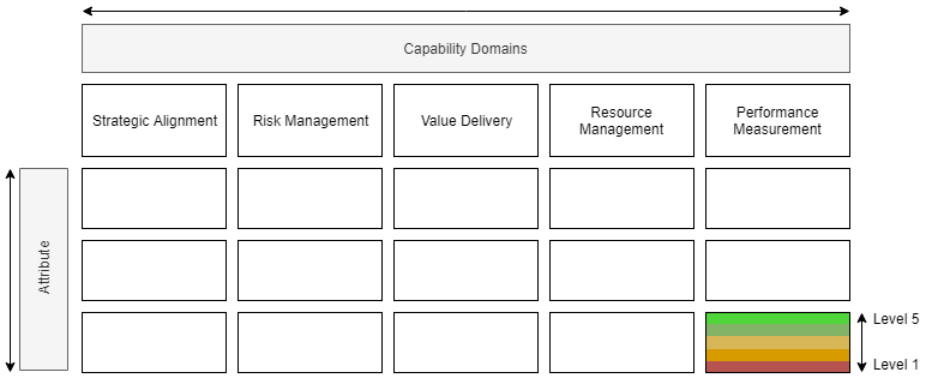


Figure 11. Example of a Matrix Diagram

5.4 Scoring Scheme

The maturity model has two alternative scoring schemes: it is possible to score each capability domain or to calculate an average ISG score based on all the capability domains. Each individual attribute has a possible score between level 1 till level 5, where level 1 is the worst and level 5 is the ideal situation. The level of each attribute corresponds with the amount of points which can be earned, so level 1 corresponds with 1 point, level 2 with 2

points etc. To calculate the average maturity of a single capability domain the total score in points has to be divided by the number of attributes in the capability domain. To calculate the total average of ISG maturity, the total score in points has to be divided by the total number of attributes. The maturity score should be stated at a maximum of one decimal.

5.5 Construction of capability domains

Based on the literature review, five capability domains have been identified which form the basis of information security governance.

The following five principles will be included in the initial design of the model:

1 Strategic Alignment
2 Risk Management
3 Value Delivery
4 Resource Optimization
5 Performance Measurement

These five capability domains have been identified by both ISACA and Gashgari et al. (2017), as explained in the introduction of chapter 4.2; these are the starting point of the ISG maturity model capability domains. The next step is to determine attributes for each capability domain; however, before doing so, it is essential to define what the capability domains actually mean and what the capability domain should measure, since many interpretations are possible from their generic definitions - as determined in the introduction of chapter 4.2.

To give context to the capability domains, and for supporting the creation of the attributes, *principles* can be used. Principles are generic, accepted rules for governance actions (NEN, 2013) and will be used as input for the creation of the attribute questions. Principles aren't however specific and measurable enough to be used as attributes. For that reason, literature review has been executed domains in chapter 4.2 and 4.3 into best practices regarding the before mentioned capabilities. This information will be used during the development of the capability domain attributes.

In the next table, the outcomes for each capability domain are defined by the researcher, based on a set of principles from Gashgari et al (2017), ISO 27014 and ISACA. The purpose of the outcomes is to determine what each capability domain should measure through its attributes.

Capability Domain	Outcome
Strategic Alignment	• How (well) information security is embedded within the organisation. • Leadership of information security. • Alignment between the strategic and operational layer regarding information security. • Responsibility of information security.
Risk Management	• A clear strategy regarding information security risk management • Leadership of information security risk management. • Information security risk decision making. • Handling of information security incidents. • Handing of third-party risks.

	• Being in control about configuration items. • Implementation of connected medical devices within the hospital environment.
Value Delivery	• Financial decision-making regarding information security investments. • Perceived value of trust and enablement of service because of information security.
Resource Optimization	• Adequate use of information security solutions and resources. • Overview of information security components.
Performance Measurement	• How the performance of information security management is being monitored. • The performance of the governance body of information security. • How the organisation checks validity of their information security activities.

Based on results from the first iteration round, experts suggested to add a domain called "Organisation", which should provide more context about the hospitals information security program; experts claim that this can help predict and validate results, as well as help executing a root cause analysis when the maturity model is used as a tool for an improvement plan.

Organisation	• Context about how information security is currently managed. • The attitude of the hospital regarding information security.

Experts also suggested to chance the capability domain name "Performance Measurement" into "Validation" because this was the preferred term within the information security industry.

Experts in the first iteration round also suggested to combine the capability domains "Value Delivery" and "Resource Optimization" into one capability domain called "Value Capturing & Delivery", since the capability domains on their own were too small and the combination of the two would complement each other.

Value Capturing & Delivery	• Financial decision-making regarding information security investments. • Perceived value of trust and enablement of service because of information security. • Adequate use of information security solutions and resources. • Overview of information security components.

5.6 Construction of attributes

The outcome and goals of each capability domain at this point has been determined; the next step is to realize attributes. The attributes have been based initially on literature review and have been improved by two iterations with experts (which will be described in more detail in chapter 5.7). The following is a summary of the attributes for each capability domain:

Organisation

For the *organisation* capability domain, six attributes have been created to measure how information security is currently being managed and what the hospitals attitude towards information security is. It is essential to measure whether a strategic information security position is created within the hospital, and how coordination of information security happens at a strategic level. To measure if the information security role and coordination is effective, the acknowledgement, representation and motivation of information security at the board of director level has to be considered. Furthermore, the hospital has to consider how it deals with information security, together with its stakeholders.

For the organisation capability domain, the following attributes have been created: *Security Role, Coordination, Acknowledgement, Representation Strategic Level, Motivation* and *Stakeholders*.

Strategic Alignment

For the *Strategic Alignment* capability domain, six attributes have been created to measure how the leadership, alignment and responsibility of information security are embedded within the hospital. Attributes regarding information security decision making are included, whereas other attributes concern how policies are implemented, how roles and responsibilities are defined, and whether usability is considered. The last two attributes aim to measure how the hospital executes leadership to create organisational support for information security and if strategic objectives are set.

For the strategic alignment capability domain, the following attributes have been created: *Decision Making, Policy Implementation, Roles and Responsibilities, Usability security controls, Leadership strategy* and *Strategic Objectives*.

Risk Management

For the *Risk Management* capability domain, ten attributes have been created to reach the desired outcome of the capability domain. The attributes focus on the maturity of decision making, the implementation of a risk management program, third party risks and what the attitude and strategy of the hospital is towards managing risks. Further, the attributes aim to measure who is participating in the risk management process. Other, more technical attributes aim to measure the way hospitals handle security incidents and the implementation of medical devices.

For the risk management capability domain, the following attributes have been created: *Decision Making Maturity, Management Program, Attitude & Strategy, Ownership, Assets,*

Strategy Security Incidents, Security Incidents Response, Third Party Risk Management, Secure Implementation Medical Devices and *Implementation Measures Medical Device*s.

Validation

For the *Validation* capability domain, eight attributes have been created to measure how the hospital checks the validity of its information security program, and how the performance of the governance body and of the information security management system is being monitored. The attributes focus on the information security management system (ISMS), its scope, metrics, performance, validity, audits, and desire to improve.

For the validation capability domain, the following attributes have been created: *Desire to improve, Management System, Scope of ISMS, Validity, Performance of ISMS, Metrics, Audit* and *Strategic Validity.*

Value Capturing & Delivery

For the *Value Capturing & Delivery* capability domain, six attributes have been created to measure how the hospital makes decisions regarding information security-related investments and adequate use of these purchased security solutions and resources, as well as what the actual perceived value of all these investments is. To achieve these attributes, the hospital should consider whether enough investments are available, how the investments are assessed, and if the hospital itself captures and utilizes the resources efficiently.

For the value capturing & delivery capability domain the following attributes have been created: *Investments, Investment Allocation, Resource Utilization, Security Architecture, Investment Estimation* and *Perceived Value*.

Example attribute

An attribute consists of an assessment question and five possible levels of maturity. The first answer corresponds to the lowest maturity possible (initial); the last answer corresponds to the highest maturity level possible (optimized). An example is displayed in figure X

	RM6	What is the strategy for information security incident response within the hospital?
1 (Initial)	○	The hospital doesn't have a plan regarding incident response.
2 (Repeatable)	○	The hospital has an informal process to respond to information security incidents.
3 (Defined)	○	The hospital has a formal process to respond to information security incidents, but this is not complete yet (there must be a BIA, IR DR and BC plan).
4 (Managed)	○	The hospital has a formal process to respond to information security incidents, which is complete but has not or partly been tested.
5 (Optimized)	○	The hospital has a formal process to respond to information security incidents, which is complete, tested and is continuously being improved.

Figure 12. Example of an attribute.

For a list of all the elaborated attributes, see Appendix A.

The following graphical overview has been created to show the result of combining capability domains and the attributes:

Figure 13. Graphical overview of the developed information security governance maturity model.

5.7 Validation and improvement of the maturity model

As described in the *Methods* chapter, the maturity model has to be validated before it can be applied in practice. Validation through expert feedback is an excellent tool since it provides insight about the industry which cannot possibly be grasped by the researcher; it also provides insight from people who have actual experience in the field of this research.

5.7.1 Iteration 1

In iteration one, the first version of the maturity model has been investigated by 6 experts (n =6). Out of the 6 experts, 5 are currently working in a hospital and are responsible for information security at the strategic level. The other expert has a large amount of experience with the subject (>20 years of experience within the information security industry).

The experts have been asked to fill out a standardized form for the evaluation of maturity models, proposed by Salah et al., which evaluates the maturity model on the basis of a set of criteria (see Appendix C). The question list also consists of 10 open questions which support

the collection of the feedback and which is required to improve the maturity model. The open questions have been discussed during a semi-structured interview, as described in chapter 3.

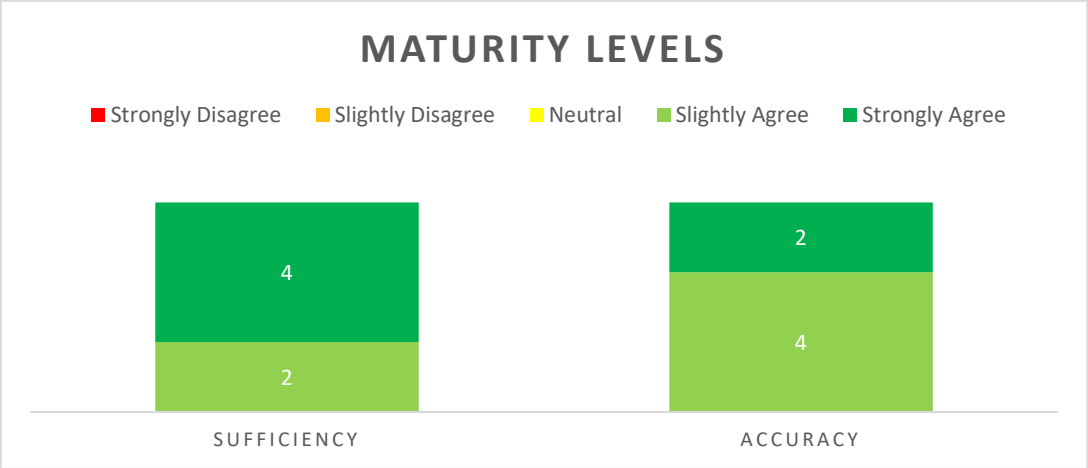


Figure 14. Maturity level Sufficiency and Accuracy.

All respondents were slightly or strongly agreeing with the current way the maturity levels have been created. The only improvement point regarding the maturity levels' *sufficiency* and *accuracy* is to create alignment between the maturity levels and the governance structure. The levels do not correctly correspond with the *Direct-Control-Evaluate* cycle which information security governance has to be executed according to. One of the experts responded: "*Directing should happen at every level of the model, and to reach level 3 the organisation should do some form of control, to reach level 4 and 5 the organisation should also do some form of evaluation on its results* ". The same expert also proposed to implement the ISO 27014 governance processes in the maturity levels.

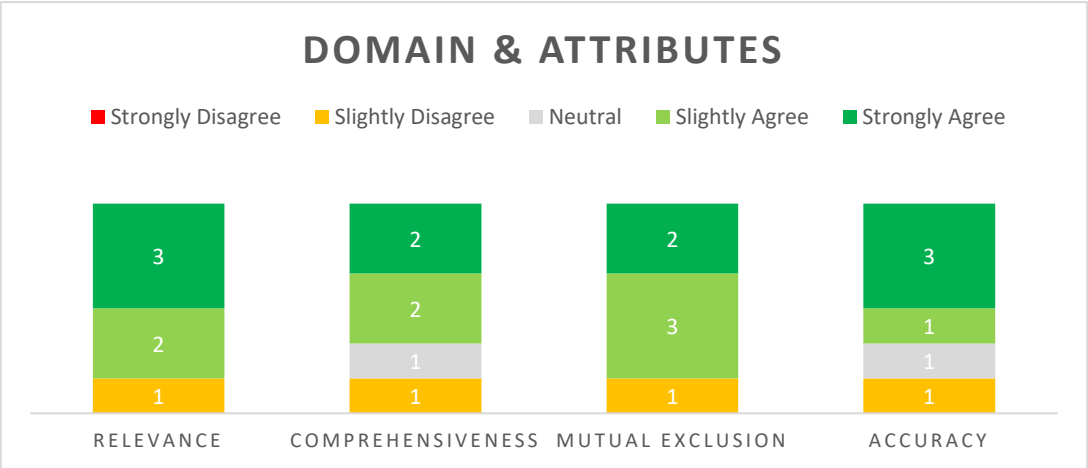


Figure 15. Domain and Attribute, Relevance, Comprehensiveness, Mutual Exclusion and Accuracy.

The results and feedback were a bit mixed in the category "Domain and Attributes". One of the main improvements which has been proposed by four experts is the creation of a new capability domain called 'organisation' or 'context'. The current model does not consider the context of the hospital enough, but experts explain that the context can actually predict a lot of results already and can sometimes also explain the root cause behind a lot of results.

Besides the creation of a new domain, it has been proposed by three experts to change the domain name “performance measurement” into something like “validation”, and add a bit more attributes related to auditing of the information security management system – since the task of governance within performance measurement is to validate the results generated by the ISMS. Some more generic feedback to improve the comprehensiveness and accuracy of the attributes was to look at the ISO 27001 standard and NEN7510 standard and use some of those security controls to improve the model attributes, this was proposed by three experts. There were some minor changes in the formulation and positioning of attributes between categories which will be further discussed in the changelog.

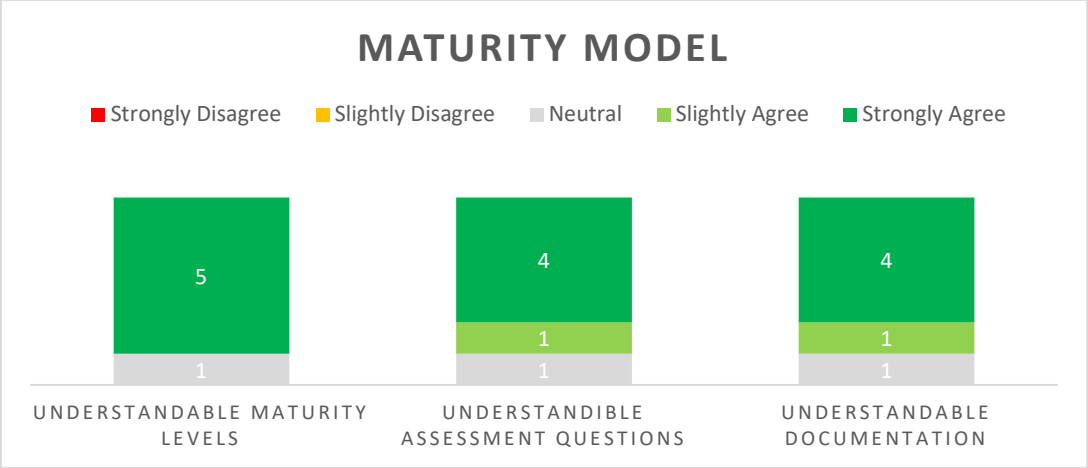


Figure 16. Maturity model understandability.

The understandability of the maturity model was largely well understood. One expert didn’t directly understand the maturity levels, but said that the understandability would be clearer if a definition/outcome of each capability domain was provided.

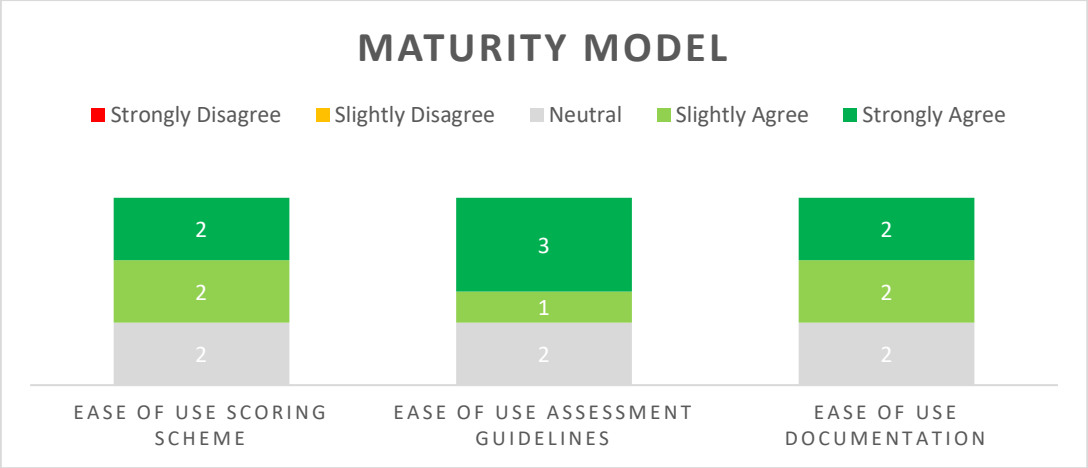


Figure 17. Maturity model ease of use.

The results were a bit mixed regarding the ease of use: the feedback of the experts who voted neutrally was largely caused by the model not providing clear guidelines and instructions on how to use the model and how the scoring worked. Additionally, the scoring scheme wasn’t clear enough. The model could be therefore improved by adding a tab of guidelines and by using some Excel functionality to make the model interactive - automatic

point calculation and a function to select answers would greatly improve the ease of use of the maturity model.

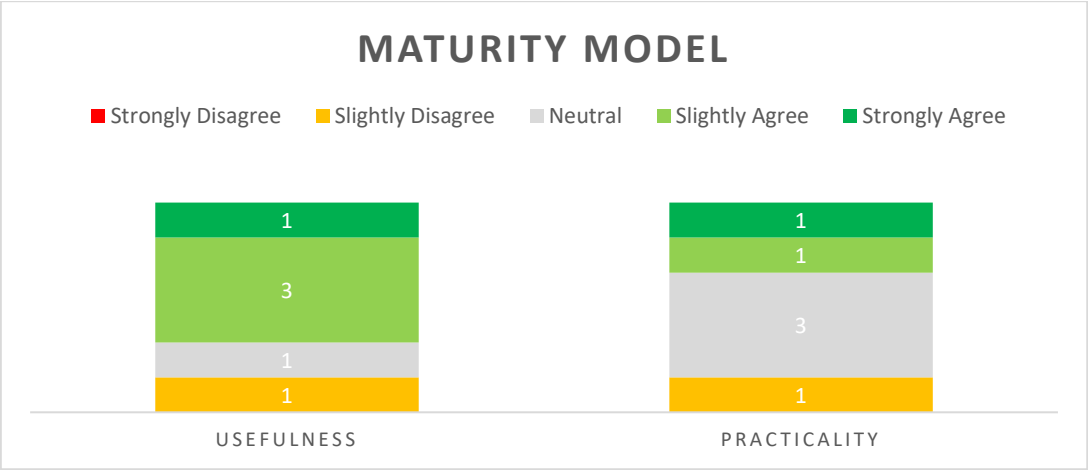


Figure 18. Maturity model usefulness and practicality.

The maturity model currently lacks a way to present the results. One expert suggested to use a spider chart to give a quick overview to the user after the model has been filled in. This feedback, together with the comments regarding the ease of use and the mixed opinions regarding the attributes, showed that the model needed another iteration. Another point of improvement to make the model more practical and useful, is to map some of the attributes, where possible, to ISO 27001/NEN7510 controls, since this is industry standard for the group who will use the model - largely strategic security management. A reference to the security controls also provides security experts with a starting point from where they can improve.

The following specific changes have been made to improve (the frequency is the amount of times a chance was proposed) :

Frequency	Change
1x	The description of the maturity levels has been changed to be aligned with the ISO 27014 governance processes.
1x	A graphical overview has been added to the maturity model to visualize the link between the ISO 27014 and the maturity levels.
1x	For each capability domain, a brief goal/explanation has been added to the maturity model.
4x	The capability domain “Organisation” and its corresponding attributes have been created.
1x	The capability domain “Value Delivery” and “Resource Optimization” have been merged together.
3x	The capability domain “Performance Measurement” has been renamed to “Validation” and extra attributes related to auditing have been added.
4x	Various attributes have been removed, added and changed.
4x	The scoring scheme has been integrated and results are presented dynamically.

3x	References to the ISO 27001 standard have been created for each attribute.

5.7.2 Iteration 2

In iteration two the second version of the maturity model has been investigated by 6 experts (n = 6). Out of the 6 experts 2 are currently working in a hospital and are responsible for information security at the strategic level. The other 4 experts have a large amount of experience with the subject.

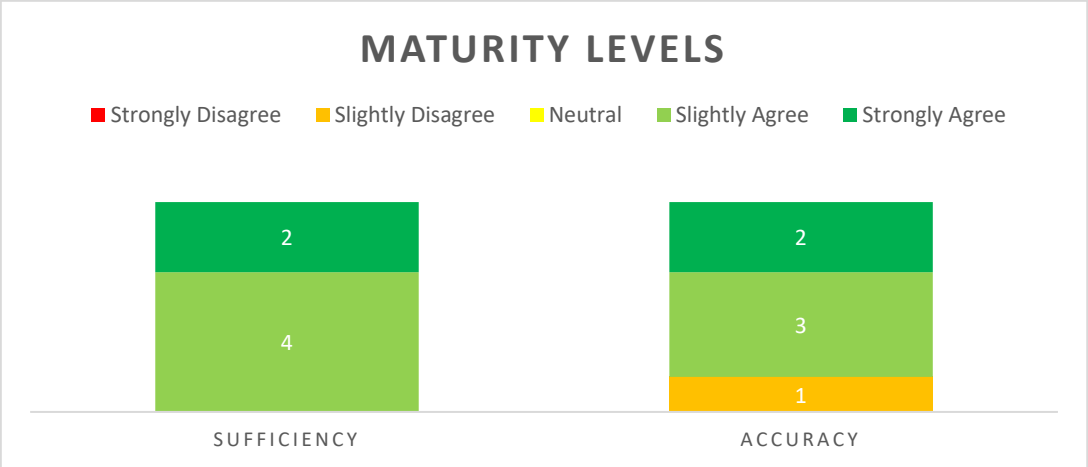


Figure 19. Maturity level Sufficiency and Accuracy.

All experts agreed that the five levels of maturity (based of CMMI and aligned with ISO 27014) are sufficient, meaning that all stages of maturity are represented well.

The accuracy of the maturity levels is about how well each attribute level is aligned with the description of the specific maturity level. The accuracy of the maturity levels is good and there is no overlap between the descriptions of the maturity level. One expert identified a few inaccuracies at level five of some attributes and suggested to do a consistency check.

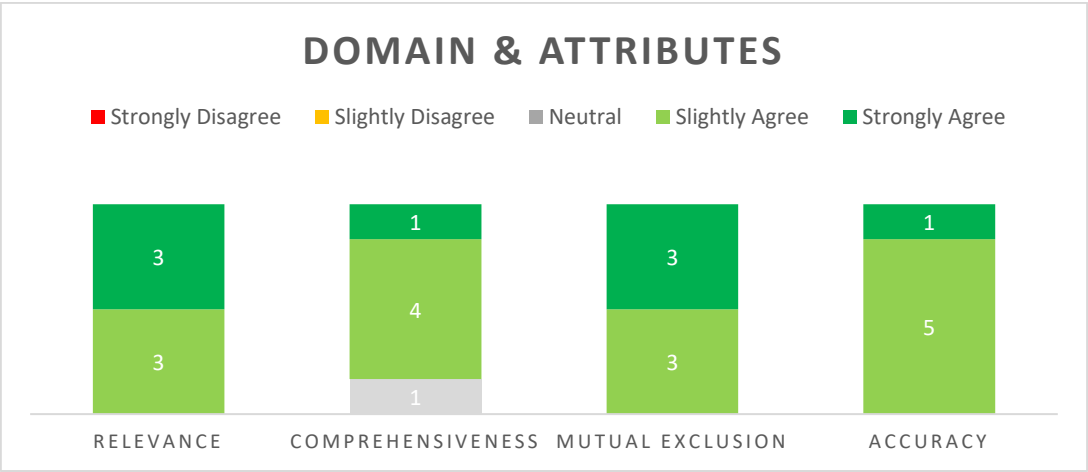


Figure 20. Domain and Attribute, Relevance, Comprehensiveness, Mutual Exclusion and Accuracy.

All experts validated the capability domains and attributes as relevant for the measurement of information security governance. The experts stated that the attributes do have a clear distinction and no overlap between attributes was detected. The accuracy of the attributes

is good, and all of them contribute to the actual capability domain the attributes themselves are trying to measure.

The comprehensiveness was largely rated as good, however one expert was neutral and suggested that extra attributes could be created to gain even more insight into a capability domain; on the other hand, the same expert also noted that extra attributes would lead to a too big and time consuming maturity model. The resulting feedback was therefore neutral.

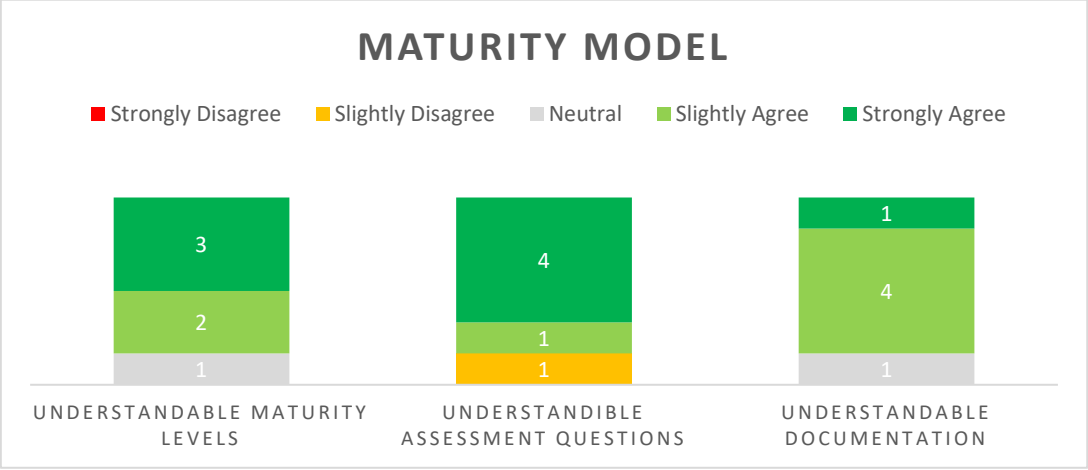


Figure 21. Maturity model understandability.

The maturity model is well understood and clear; one expert found an attribute which could be interpreted differently and therefore slightly disagreed with the *understandable assessment questions*-criteria. One expert said that the graphical image in the documentation about the maturity levels was too vague and suggested to make it clearer.

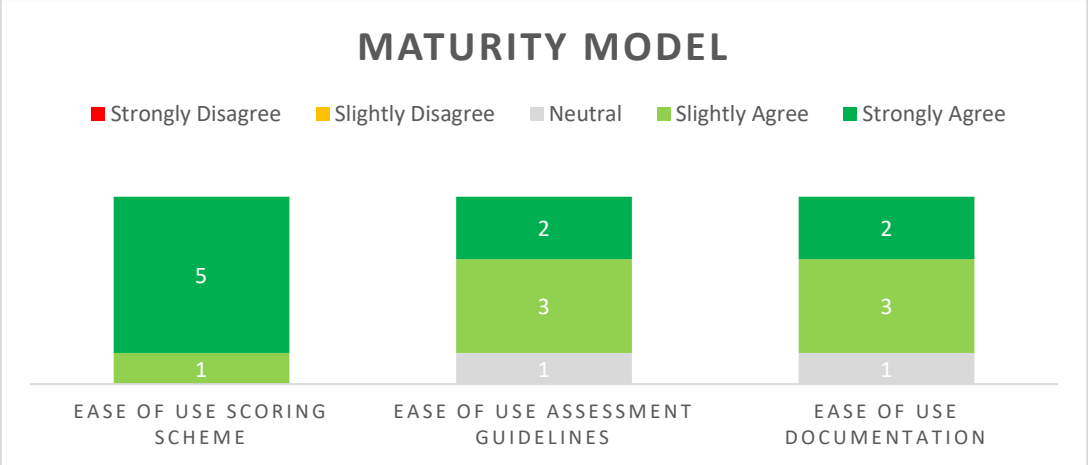


Figure 22. Maturity model ease of use.

The ease of use regarding the maturity model has increased dramatically since the first iteration. Two experts said the documentation could still be improved a bit by splitting up the overview into a separate overview and documentation tab which provides less information the first time you open the model - which could scare off first-time users.

One of the experts proposed the use of an online questionnaire tool which delivers limited amounts of questions each time. The problem with an online questionnaire is that, being

online, there is the risk to potentially share sensitive information (with the creators of the questionnaire tool). However, another benefit of having a complete overview is that the tool can be used as an improvement tool by zooming into the capability domains and attributes which are important for the user. For this reason, one expert was neutral regarding the *ease of use*.

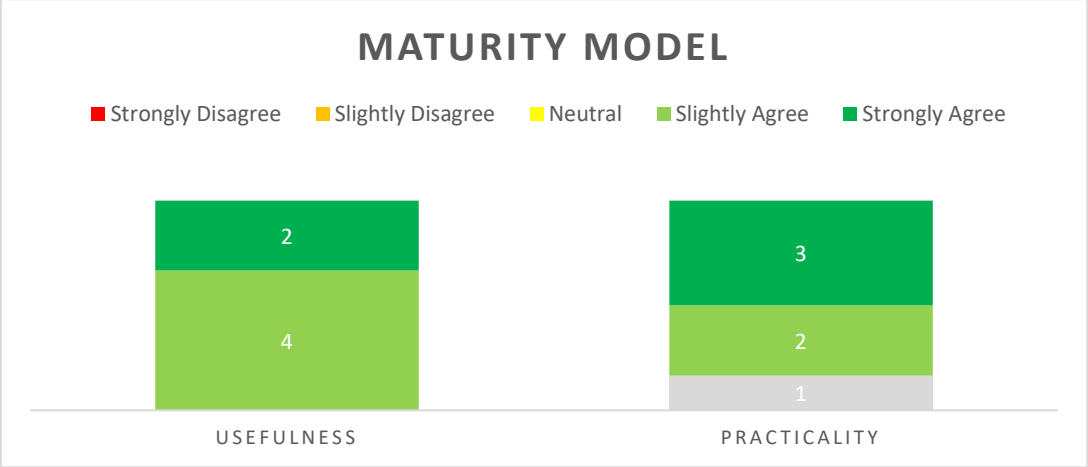


Figure 23. Maturity model usefulness and practicality.

All experts rated the model as useful in the sense that it could help them measure the current maturity of information security governance within hospitals. Some experts even noted that the model could be used as a basis to measure information security governance in (larger) enterprises. The model was largely rated as practical for the hospital industry specifically and experts specified that the important governance challenges within hospitals is considered in the model. One expert noted that the reference to the ISO 27001 standard could better be replaced with references to the NEN7510 standard (even though the standards are almost identical in the 2017 versions).

The following specific changes have been made to improve (the frequency is the amount of times a chance was proposed) :

Frequency	Change
2x	A separate documentation tab has been created with step-by-step information.
1x	The starting tab consists of less information so first-time users are not scared off.
1x	The maturity level description image has been altered to make it more easily understandable.
1x	The compliance references have been changed from the ISO 27001 standard to the NEN7510 standard.
1x	Minor changes to the formulation of a few attributes.

6 Results

The purpose of the case study is to use the developed maturity model and measure information security governance within an actual Dutch hospital. Applying the maturity model to a real case study will help validating the maturity model and determine whether it is able to produce valid results.

Participants (Dutch hospitals) have stated that the results produced by the maturity model contains sensitive information about the defending capabilities of the hospital and stated that for this reason they want full anonymity. Some details about the hospitals have been provided like location, size and type of hospital, but more details have been left out to preserve anonymity of the participants.

For the case study, the participants were e-mailed the *Maturity Model Assessment Tool* (see Appendix B), which is based on the previously created maturity model but with extra functions such as an integrated scoring scheme, selectable answers and references to compliance standards. The participants are all currently working in a Dutch hospital and within it are responsible for information security governance.

6.1 Case study 1

The hospital in the first case study is located in the province of Noord-Holland, is a general hospital and is classified as a big hospital (between 500 – 1000 beds).

In the first case study it can be concluded that the average overall maturity level of the hospital is, on average, just below level 3 (defined).

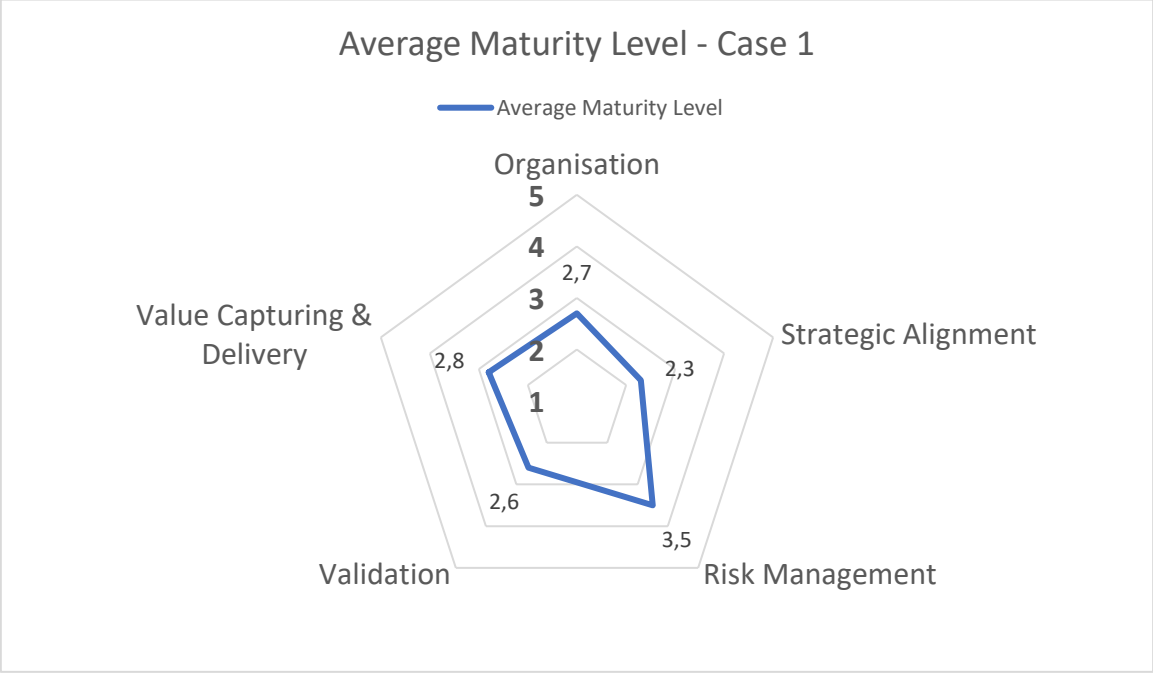


Figure 24. Radar plot of "Average Maturity Level" for case study 1.

The average, overall maturity score is 2.8; the capability domains score between 2.3 and 2.8, exception made for the positive outlier represented by the risk management capability domain, where the hospital scores a 3.5 average maturity level.

We can conclude from the results that the hospital is having troubles executing proper information security governance and is largely focused on being compliant with rules and regulations and not necessarily on improving its information security governance program to truly become more secure. This statement is being confirmed by the level 2 maturity scored by the "*Motivation*" and "*Security Role*" attributes within the *Organisation* Capability domain.

The hospital would greatly benefit from an independent strategic security role who would be able to advocate for information security in the boardroom. The next step after the appointment of information security in the boardroom would be to create an information security program with a clear mission, vision and strategy; this plan would guide the hospital towards the achievement of security improvements. In the current situation, most attributes have a maturity level of 3, which means that there is an information security management system but that it is not actively being improved right now (and only exists for compliance reasons). The hospital would benefit the most from improving mainly on the *Organisation*, *Strategic Alignment* and *Validation* capability domains.

The hospital scores better on some aspects of risk management, but this could be explained by the core business of hospitals which is intertwined with patient safety risks (which is where most of the concerns of the board of directors go towards).

The hospital scores a maturity level of only 2 on the "*Usability Security Controls*", which shows that the hospital does not consider the clinical workflow when designing security solutions. However, the hospital does score well on both attributes regarding the safe implementation of connected medical devices with a maturity level of 4.

Figure 25. Complete graphical overview for information security governance maturity for case study 1.

6.2 Case study 2

The hospital in the second case study is located in the province of Gelderland, is a general hospital and is classified as a small hospital (below 500 beds).

In the second case study it can be concluded that the average overall maturity level of the hospital is, on average, just below level 3 (defined).

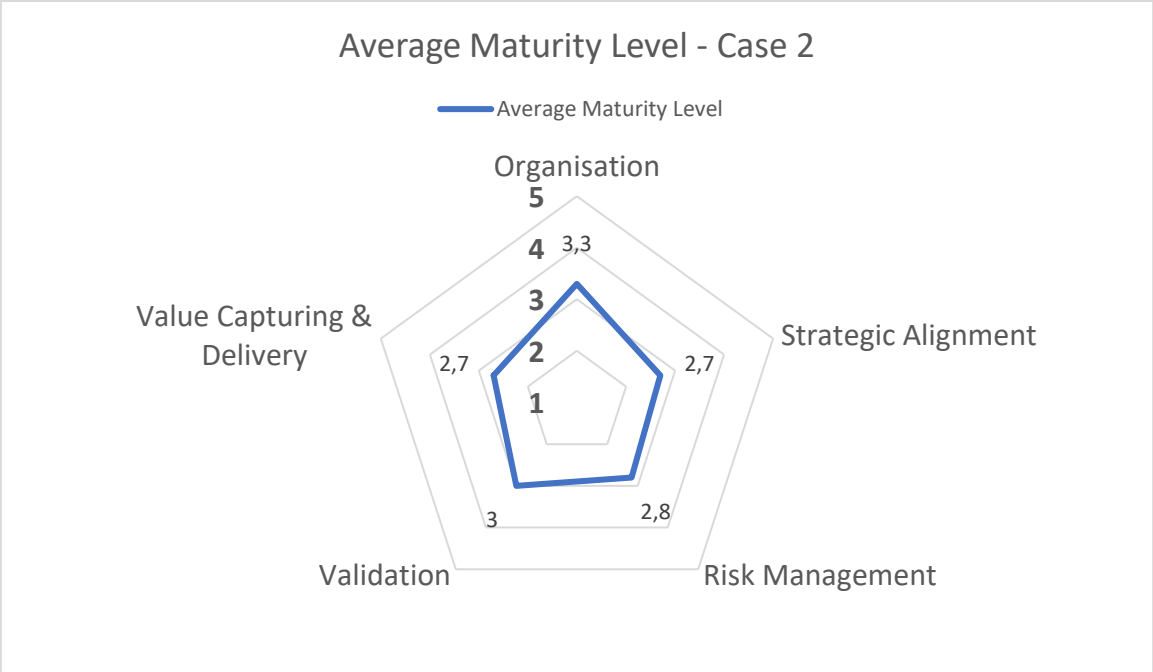


Figure 26. Radar plot of "Average Maturity Level" for case study 2.

The average, overall maturity score is 2.9; the capability domains score between 2.7 and 2.3, a slight outlier represented by the organisation capability domain, where the hospital scores a 3.3 average maturity level.

From the results it can be concluded that the hospital focuses on an information security management system because all the attributes relevant for the management system score at least a maturity level of 3, some even around level 4. Even though the focus is on the management system, crucial attributes in the *validation* domains like "*Metrics", "Audit", "Performance"* and "*Management System"* are not reaching level 4 (yet). The hospital does not seem to invest in an information security management system for compliance reasons but really wants to use it as a basis to improve the overall information security program. This is supported by the "*Motivation"*, "*Coordination"* attributes in the *Organisational* Capability domain and the "*Desire to improve"* and *"Scope of ISMS"* attribute in the *Validation* Capability domain which all have a maturity level 4.

On the more domain specific attributes, the hospital is scoring below the maturity level of 3: attributes such as *"Secure Implementation Medical Devices"* and *"Implementation Measure Medical Devices"* are not reaching maturity level 3 yet. Neither the clinical workflow is considered specifically and has a maturity level of 2.

The hospital has a solid basis regarding information security governance but still has lots of potential to improve, especially in the capability domains *Strategic Alignment* and *Risk Management*.

Figure 27. Complete graphical overview for information security governance maturity for case study 2.

6.3 Case study 3

The hospital in the third case study is located in the province of Noord-Brabant, is a general hospital and is classified as a big hospital (between 500 – 1000 beds).

From the third case study the model shows that the average overall maturity level of the hospital, on average is between the maturity level *repeatable* (level 2) and *defined* (level 3) with an average overall maturity score of 2.5.

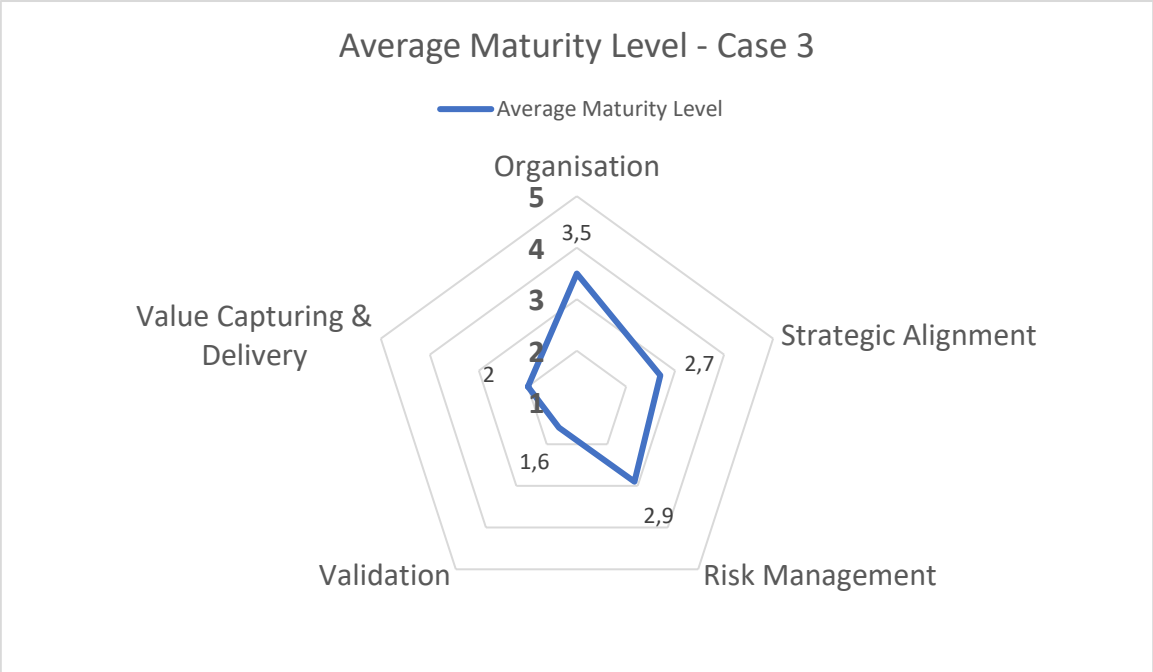


Figure 28. Radar plot of "Average Maturity Level" for case study 3.

This hospital is unlike the other two hospitals; the scores on the domains are not so well balanced out and the model shows extreme results in certain domains. The hospital excels in the Organisation domain with an average overall maturity score of 3.5 but significantly lacks maturity in the Validation and Value Capturing & Delivery capability domains.

It seems that the hospital has a strategic layer that is aware of the need of information security, acknowledges it and is motivated to improve, but it looks like it does not have an organisation-wide plan and strategy to actually make improvements. The hospital does not have an information security management system of any form, which is also reflected by the other attributes in the Strategic Alignment and Validation capability domains. It seems that the hospital does engage in some activities which it deems important but doesn't seem to be creating a structured information security program at all. The hospital would greatly benefit from implementing an information security management system, which would allow them to manage basic IT security hygiene and establish an organisational wide view.

On the domain specific attributes, which are especially important for hospitals, such as "*Usability Security Controls*", "Secure Implementation Medical Devices" and "Implementation Measures Medical Devices" the hospital scores only a maturity level of 2.

Figure 29. Complete graphical overview for information security governance maturity for case study 3.

6.4 Overall results

Based on the results collected in the case study, it is difficult to make a statement about all hospitals in The Netherlands regarding their information security governance maturity, due to the limited number of hospitals surveyed. However, what can be concluded is that the investigated hospitals are all on a similar information maturity governance level. The hospitals are at best trying to create an information security management system in order to be compliant, but none of the hospitals had one capability domain which on average had the maturity level *managed* (level 4).

Regarding workability - one of the hospital-specific governance challenges, only one hospital had a maturity level of 4 regarding the implementation of medical devices; the other two hospitals had a level 2 maturity.

The graph below shows a comparison of the scores on each domain of the three hospitals surveyed.

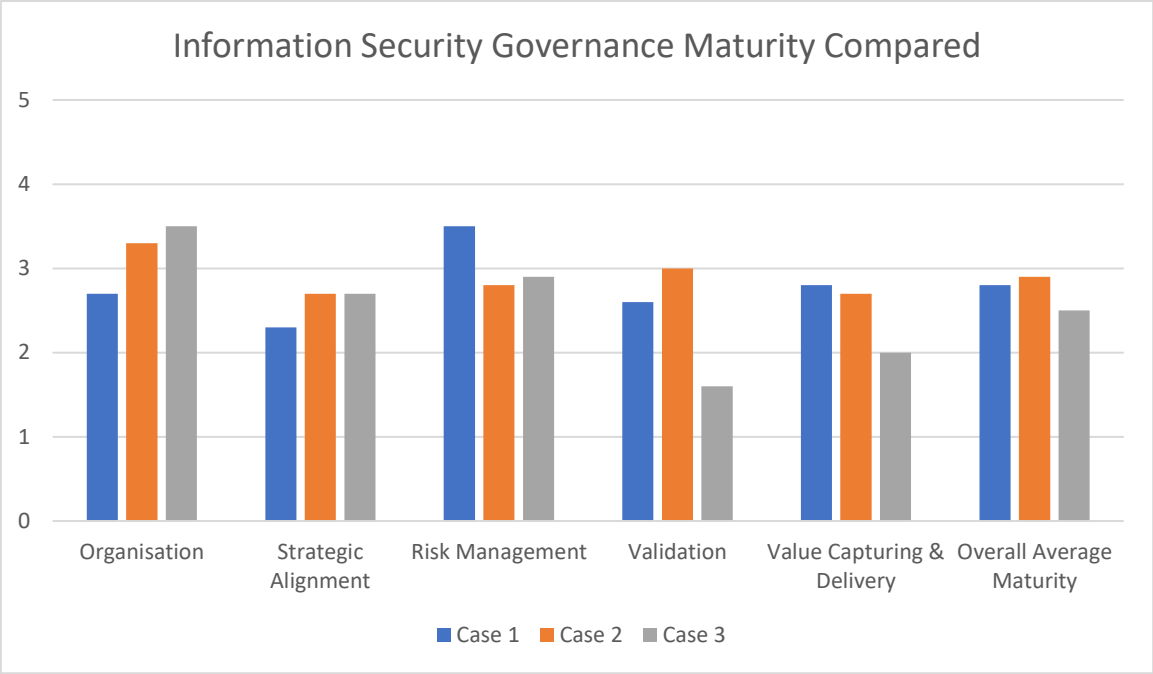


Figure 30. Comparison of information security governance maturity between all case studies.

The existence of 5 maturity levels does not implicate that level 5 is the norm that all the hospitals should realistically aim for. Level 5 maturity is most of the time a theoretical best case scenario which will not always be possible in practice due to (practical) constraints. From a practical point of view, it is not even desirable to aim for level 5 maturity because in most cases the costs might outweigh the benefits. It could be stated that, in practice, a level 2 maturity is too low and has to be improved to a minimum of maturity level 3. The practical goal should be to aim for maturity level 4 since it implies that information security within the hospital is managed and that the hospital is in control of the information security-related challenges they might face.

7 Discussion

The goal of the discussion chapter is to evaluate and reflect on the research process and its results. Also, limitations and internal and external validation will be discussed.

The goal of the research was to measure information security governance in Dutch hospitals, because in the recent past hospitals have been a victim of cybercrime. It was found in literature that not much research has been done into information security governance, and that tools to measure information security governance do not exist, let alone for the hospital industry specifically.

As described in the *Methods* chapter, the research has been executed in three phases:

1. Literature review to gather the information necessary to create an initial model.
2. Iterative improvement process according to structured interviews with experts to improve on the initial model and create a definitive maturity model.
3. Application of the created maturity model through the execution of case studies; gathering of data about the information security governance maturity of some Dutch hospitals.

7.1 Phase 1

The literature review was executed to gather insights on what exactly information security governance is, since this concept is not discussed in the well-known industry standards such as ISO 27001. It was concluded that the governance domain acts as an overarching function for directing, controlling and preserving its information security activities; further, research into how information security governance can be measured was executed. Well established literature described what the outcomes of effective information security governance should be, but didn't describe how well information security governance should be executed. For that reason, further research into how well information security governance should be executed was conducted. In order understand how to apply information security governance in the hospital industry, research into hospital specific governance challenges was executed. With a set of outcomes and detailed information on how these outcomes can be achieved, the second phase started.

7.2 Phase 2

During the second phase, the building of the actual maturity model occurred. An initial version was drafted based on all the information that was gathered during phase one. The initial version then got improved by an iteration round. In the iteration round, experts studied the model and then agreed to have a semi-structured interview with the researcher. After six experts had given their feedback over the initial draft, the iteration round ended, and all the feedback was collected and analysed. Based on the feedback, the maturity model got improved and underwent another identical iteration round with other experts. The feedback of six experts was, again, collected and analysed and small improvements were made. No significant improvement points could be found, and the maturity model was classified as "ready for testing".

The maturity model structure did change based on the feedback of the experts, compared to the initial version. Experts suggested the creation of an “Organisation” capability domain, since they explained that context is important within the governance domain and this new domain would help predict and explain the other capability domains within governance.

7.3 Phase 3

In the last phase the “ready-for-testing” maturity model got introduced to three real case studies within Dutch hospitals. It is not possible to generalize the results of three case studies across all hospitals in The Netherlands, since this population is not big enough. The results collected by the maturity model are sensitive, since they disclose information about the current information security resilience of the surveyed hospitals; this was often mentioned as a reason not to cooperate with the researcher – even though full anonymity was offered. A possible explanation could also be that the participants were afraid of the results of the maturity model and therefore chose not to cooperate.

7.4 Internal Validity

The internal validity of the research is dependent on various factors. For what concerns the iteration rounds, the quality of the feedback is heavily dependent on the expertise of the experts. To mitigate this risk, experts in the iteration rounds were diverse: experts who were currently working in a Dutch hospital in a strategic information security role were included, ranging from experts with less than 5 years of experience and experts with more than 30 years of experience; also, experts who were not directly working in a hospital but had a large amount of experience in other industries with the subject were included. All iterations had a combination of both “hospital-experts” and “non-hospital-experts” to get as much of a diverse feedback as possible.

7.5 External Validity

For what concerns the case studies, the external validity is affected by the lower amount of participating hospitals. Results could be generalizable if more hospitals would have participated in the research, however due to the limited time and means to make hospitals participate, the maximum amount of case studies possible was only of 3.

It is difficult to compare the result of this research with other literature since similar research does not exist (yet); the initial model is however based on literature review and it is at least consistent with other research conducted in the domains of governance and information security. Furthermore, the maturity model did go through multiple iteration rounds with 12 experts (from 7 Dutch hospitals and 5 corporations) and was tested in practice.

8 Conclusions

The goal of the conclusions is to answer the research question and evaluate whether the research objective has been reached. The main research question was: "*How can the maturity of information security governance in Dutch hospitals be measured objectively?*". To answer this question, it is required to first answer the identified sub-questions, which support the answering the main research question.

What is the role of governance within information security?

Even though governance has been a predictor of an effective information security program, it was an underrated element of information security within literature. Information security governance is the process by which the organisation's information security activities are directed and controlled to preserve the availability, integrity and confidentiality of its people, processes, information and infrastructure. Governance works closely together with information security management and risk management.

What are the information security governance challenges within the hospital environment?

This research focused specifically on Dutch hospitals and therefore not only considered 'generic' information security governance, but also included governance challenges which are specific for the hospital industry.

Connected medical devices constitute a challenge for governance bodies in hospitals because they pose a large threat to the continuity of patient care in hospitals, as shown for example by the ransomware attacks that occurred in 2017.

Workability is the part of information security where practical security solutions and the clinical work processes collide. Especially in hospitals where every second could make a difference in saving a life, workability is an important factor to consider when executing information security governance.

Is it possible to develop a valid maturity model to effectively measure information security governance within hospitals?

According to ISACA and Gashgari et al. (2017), information security governance can be measured according to five categories, which are: Strategic Alignment, Risk Management, Resource Management, Performance Measurement and Value Delivery. The problem with that literature is that specific criteria, which define what good security governance is, is missing.

For this reason, an information security governance model was developed using the five categories of ISACA and Gashgari et al. (2017) as a basis for its construction. Through further literature review the initial criteria about good security governance have been established.

In order to determine the current maturity level of information security governance in Dutch hospitals it was required to create a measurement tool in the form of a maturity model. No maturity models for information security governance existed, so one had to be developed.

Based on the information gathered through a literature review, an initial maturity model was developed. Through two rounds of improvements, executed according to the Design Science Research methodology, strategic information security experts, both within and outside the hospital industry, have been involved to improve the initial developed model. Based on the input of the experts, the capability domain 'Organisation' was created and two existing capability domains were merged together. In the final model there were five capability domains which together consisted of 36 attributes.

If so: what is the current maturity level of information security governance within Dutch hospitals, using the developed maturity model?

In total, 3 Dutch hospitals have participated in the case study and the maturity model was used to assess their current maturity level. Even though 3 hospitals are not representative enough for the whole of the Netherlands, the case studies did provide a lot of information. It can be concluded that all the surveyed hospitals are aiming to a maturity level of 3 (defined) but have not achieved this yet. Also, hospitals are largely investing in information security because they are afraid for compliance and regulatory issues. The hospitals have a basic information security management system, but this is not on a *managed* level yet.

8.1 Future work

For future work it could be beneficial to use the maturity model on a larger scale across other hospitals in the Netherlands, in order to make results more generalizable. The benefit of a larger scale research would be to compare the average information security governance maturity level between Dutch hospitals. The comparison would help each individual hospital understand where they are positioned in the industry in terms of information security governance; furthermore, the comparison would highlight the domains where each hospital scores strongly and weakly, and would allow them to learn from the other's strengths and weaknesses in order to advance together as an industry - in terms of maturity of information security governance.

Another possibility for future research would be to make the maturity model non-industry specific by removing the hospital specific attributes and test the maturity model in other industries (preferably containing large enterprises, since these are comparable to hospitals).

Finally, another option would be to measure which capability domains are the predictor of an effective information security governance.

References

Baumn, F. (2017). *Securing IoT Medical Devices - Are We There Yet?* https://www.electronicdesign.com/iot/securing-iot-medical-devices-are-we-there-yet: ElectronicDesign.

Blakley, B., McDermott, E., & Geer, D. (2001). *Information Security is Information Risk Management - Proceedings of the 2001 workshop on New security paradigms.* http://ns2.datacontact.dc.hu/~mfelegyhazi/courses/EconSec/readings/03_Blakley2001infosec.pdf: Cloudcroft.

Buecker, A., Andreas, P., & Paisley, S. (2008). *Understanding IT Perimeter Security.* https://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf: IBM.

Burgess, C. (2014, 8 19). *CISO vs. CRO: What's the Difference?* Retrieved from Security Intelligence by IBM: https://securityintelligence.com/ciso-vs-cro-whats-the-difference/

Caralli, R., Knight, M., & Montgomery, A. (2012). *Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability*. Retrieved from Carnegie Mellon University: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58916

CGI. (2016). *IT Security Governance - A holistic approach.* https://www.cgi.com/sites/default/files/white-papers/it-security-governance.pdf: CGI Group Inc.

Choi, S., & Johnson, M. (2019). *Do Hospital Data Breqaches Reduce Patient Care Quality?* https://arxiv.org/pdf/1904.02058.pdf: Vanderbilt University.

Ciampa, M. (2011). *Security+ Guide to Network Security Fundamentals.* Cengage Learning.

Coertze, J. (2012). *A Framework for Information Security Governance in SMMEs.* https://www.researchgate.net/publication/258432030_A_Framework_for_Information_Security_Governance_in_SMMEs: Nelson Mandela Metropolitan University.

Curry, S. (2017). *Boards Should Take Responsibility for Cybersecurity. Here's How to Do It.* https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it: Harvard Business Review.

Da Veiga, A., & Eloff, J. (2007). *An Information Security Governance Framework.* https://doi.org/10.1080/10580530701586136: Information Systems Management.

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). *Understanding the Main Phases of Developing a Maturity Assessment*. Retrieved from Australasian Conference on Information Systems (ACIS): https://eprints.qut.edu.au/25152/

Deloitte. (2015). *Cybersecurity of networkconnected medical devices in The Netherlands 2015*. Retrieved from Deloitte: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/public-

sector/deloitte-nl-risk-cybersecurity-of-network-connected-medical-devices-in-the-netherlands.pdf

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

Donald Rumsfeld. (2002). *DoD News Briefing - Secretary Rumsfeld and Gen. Myers.* http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636: U.S. Depertment of Defense.

Dutton, J. (2017). *The Three Pillars of Cyber Security.* https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security.

Gashgari, G., Walters, R., & Wills, G. (2017). *A Proposed Best-practice Framework for Information Security.* https://www.scitepress.org/papers/2017/63031/63031.pdf: University of Southampton.

George, T. (2013). *Risk and Compliance - For Better or Worse?* https://m.isaca.org/Journal/archives/2013/Volume-4/Documents/13v4-Risk-and-Compliance.pdf: ISACA.

Ghazouani et al. (2014). *Information Security Risk Assessment — A Practical approach with a mathematical fomulation of risk.* Casablanca.

Gregory, A. (2014). *At least 1,400 'killed by NHS equipment failures' - and worker shortage means fatalities are rising.* https://www.mirror.co.uk/news/uk-news/least-1400-killed-nhs-equipment-3909340: Mirror.co.uk.

Harris, S. (2006). *Information Security Governance Guide.* https://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide: TechTarget.

Hofstee, E. (2006). *Constructing a good dissertation : a practical guide to finishing a Master's, MBA or PhD on schedule*. Retrieved from https://www.researchgate.net/figure/The-funnel-method-of-structuring-a-literature-review-adapted-from-Hofstee-2006-p-96_fig1_267512601

ICO. (2019). *Data Protection Officers.* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/: Information Commissioners Office.

ISACA. (2006). *Information Security Governance Guidance for Board of Directors and Executive Management 2nd Edition .* https://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf: IT Governance Institute.

ISACA. (2009). *An Introduction to the Business Model for Information Security.* https://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf: ISACA.

ISACA. (2016). *CISM Review Manual 15th Edition.* USA: ISACA.

ISO. (2015). *Information technology -- Governance of IT for the organization - ISO/IEC 38500.* Internation Organization for Standardization.

ISO. (2018). *Information technology — Security techniques — Information security risk management (ISO\IEC 27005).* International Organization for Standardization.

Jalali, M., & Kaiser, J. (2018). *Cybersecurity in Hospitals: A Systematic, Organizational Perspective.* https://doi.org/10.2196/10059: MIT Sloan School of Management.

Kindervag, J. (2016). *No More Chewy Centers: The Zero Trust Model Of Information Security.* http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf: Forrester.

Kosutic, D. (2014). *ISO 31000 and ISO 27001 - How are they related?* https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/: Advisera.

Kosutic, D. (2015). *How to use ISO 22301 for the implementation of business continuity in ISO 27001.* https://advisera.com/27001academy/blog/2015/06/15/how-to-use-iso-22301-for-the-implementation-of-business-continuity-in-iso-27001/: Advisera.

Lazarikos, D. (2015). *How Do You Secure An Environment Without a Perimeter?* http://ptc2.revacomm.net/assets/uploads/papers/ptc15/PTC_version1%201%20cgb%20Laz%20Final.pdf: BlueLava.

Leffingwell, D. (2010). *Agile Software Requirements - Lean Requirements Practices for Teams, Programs, and the Enterprise.* Pearson Education.

Mahncke, R. (2013). *The Applicability of ISO/IEC27014:2013 For Use Within General Medical Practice.* https://doi.org/10.4225/75/5798124731b3f: Edith Cowan University.

Marosin, D., van der Linden, D., & Sousa, S. (2014). *A Collaborative Risk Management Framework for Enterprise Architecture.* https://doi.org/10.1109/RCIS.2014.6861045: IEEEE.

Mettler, T. (2011). *Maturity assessment models: a design science research approach.* https://www.alexandria.unisg.ch/214426/1/IJSSS0301-0205%2520METTLER.pdf: University of St. Gallen & SP Research CEC.

Morse, A. (2017). *Investigation: WannaCry cyber attack and the NHS.* https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/: British National Audit Office.

Moulton, R., & Coles, R. (2003). *Applying information security governance.* https://doi.org/10.1016/S0167-4048(03)00705-3: Elsevier.

MT-Integraal. (2015). *Het hoe en waarom van Certificering van Medische apps.* https://mtintegraal.nl/artikelen/269/het-hoe-en-waarom-van-certificering-van-medische-apps: MT-Integraal.

NEN. (2013). *Information technology - Security techniques - Governance of information security (ISO/IEC 27014:2013, IDT).* NEN.

NEN. (2019, 1 10). *Is het gebruik van NEN 7510 verplicht?* Retrieved from Werken met NEN7510: https://www.werkenmetnen7510.nl/vragen

NIST. (2008). *Performance Measurement Guide for Information Security (800-55).* National Institute of Standards and Technology.

Nominet. (2019). *Life Inside the Perimeter - Understanding the modern CISO.* https://media.nominet.uk/wp-content/uploads/2019/02/12130924/Nominet-Cyber_CISO-report_FINAL-130219.pdf: Nominet Cyber Security.

Overheid.nl. (2017, 11 28). *Besluit van 10 november 2017, houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders (Besluit elektronische gegevensverwerking door zorgaanbieders)*. Retrieved from Staatsblad van het Koninkrijk der Nederlanden | Overheid.nl: https://zoek.officielebekendmakingen.nl/stb-2017-446.html

Peters, E. (2018). *Chief Medical Officer CMIO essentieel voor digitalisering zorg in het ziekenhuis.* https://www.nictiz.nl/nieuws/chief-medical-officer-cmio-essentieel-voor-digitalisering-zorg-in-het-ziekenhuis/: NICTIZ.

Pieters, W. (2010). *Explanation and trust: what to tell the user in security and AI?* https://link.springer.com/article/10.1007/s10676-010-9253-3: Springer.

Pironti, J. (2007). *Developing Metrics for Effective Information Security Governance.* http://iparchitects.com/wp-content/uploads/2016/07/Developing-Metrics-and-Measures-for-Information-Security-Governance-ISACA-Member-Journal-March-2007.pdf: ISACA.

Posthumus, S., & von Solms, R. (2004). *A framework for the governance of information security.* https://doi.org/10.1016/j.cose.2004.10.006: Elsevier.

Pratt, M. (2018). *What is Zero Trust? A model for more effective security.* https://www.csoonline.com/article/3247848/network-security/what-is-zero-trust-a-model-for-more-effective-security.html: CSO.

Rosenstock, C., Johnston, R., & Anderson, L. (2000). *Maturity model implementation and use: a case study.* Project Management Institute Annual Seminars & Symposium, Houston, TX: Project Management Institute.

Salah, D., Paige, R., & Cairns, P. (2014). *An Evaluation Template for Expert Review of Maturity Models.* https://link.springer.com/chapter/10.1007/978-3-319-13835-0_31: Springer International Pbulishing Switzerland.

Schellevis, J. (2017, 06 25). *Zeker vijftien ziekenhuizen geïnfecteerd met ransomware*. Retrieved from NOS: https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware.html

Singh, H. (2018). *The Internet of Things: IoT solutions and its Benefits.* http://customerthink.com/the-internet-of-things-iot-solutions-and-its-benefits/.

Sinnett, W. (2015). *The CFO's role in cybersecurity.* http://www.financialexecutives.org/ferf/download/2015%20Final/2015-009.pdf: GrantThornton.

Siponen, M. (2003). *Information Security Management Standards: Problems and Solutions.* Finland: Oulu University.

Tu, Z., & Yuan, Y. (2014). *Critical Success Factors Analysis on Effective Information Security Management: A Literature Review.* https://pdfs.semanticscholar.org/aa02/0f53503050a6e53d6403c6aa48f5dcbc3b9c.pdf: McMaster University.

Ula, M., Ismail, Z., & Sidek, Z. (2011). *A Framework for the Governance of Information Security in Banking System.* https://doi.org/10.5171/2011.726196: Journal of Information Assurance & Cybersecurity. Retrieved from Journal of Information Assurance & Cybersecurity: https://doi.org/10.5171/2011.726196

University of Colorado Boulder. (2017). *Security Awareness - Hardening Your Computer.* https://oit.colorado.edu/it-security/security-awareness/hardening-your-computer: University of Colarado Boulder.

Vaishnavi, V., & Kuechler, W. (2012). *Design Science Research in Information Systems.* http://www.desrist.org/desrist/content/design-science-research-in-information-systems.pdf.

van den Berg, J. (2018). *Cyber Security for Everyone.* https://link.springer.com/chapter/10.1007/978-3-658-21655-9_40: Springer Vieweg, Wiesbaden.

von Solms. (2000). *Information Security - The Third Wave?* https://doi.org/10.1016/S0167-4048(00)07021-8: Elsevier.

von Solms, B. (2005). *Information Security Governance - Compliance management vs operational management.* https://doi.org/10.1016/j.cose.2005.07.003: Elsevier.

von Solms, B. (2005). *Information Security governance: COBIT or ISO 17799 or both?* https://doi.org/10.1016/j.cose.2005.02.002: Elsevier.

von Solms, R., & van Niekerk, J. (2013, 4 10). *From information security to cyber security*. Retrieved from https://ldc.usb.ve/~torrealba/sti-242/4ta_Clase/solms-2013.pdf

von Solms, R., & von Solms, B. (2006). *Information Security Governance: A model based on the Direct–Control Cycle.* http://dx.doi.org/10.1016/j.cose.2006.07.005: Elsevier.

Wetsman, N. (2019). *HEALTH CARE'S HUGE CYBERSECURITY PROBLEM.* https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation: The Verge.

Whitman, M., & Mattord, H. (2012). *Principles of Information Security.* Course Technology.

Whitman, M., & Mattord, H. (2014). *Information Security Governance for the Non-security Business Executive.* Journal of Executive Education.

Williams. (2001). *Information Security Governance.* https://doi.org/10.1016/S1363-4127(01)00309-0.

Williams, H. (2008). *When trust defies common security sense.* https://www.ncbi.nlm.nih.gov/pubmed/18775827: Health Informatics J.

Williams, P., & Woodward, A. (2015). *Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem.* https://www.ncbi.nlm.nih.gov/pubmed/26229513: Dovepress.

Yuan, S., Fernando, A., & Klonoff, D. (2018). *Standards for Medical Device Cybersecurity in 2018.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6134300/: J Diabetes Sci Technol.

Zetter, K. (2019). *Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists.* https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?noredirect=on&utm_term=.caac57673340: The Washington Post.

Zijlstra, W. (2013). *ZIN EN ONZIN OVER BUSINESS CONTINUITY MANAGEMENT – BCM.* https://zbc.nu/security/business-continuity-plan-security/zin-onzin-business-continuity-management-bcm/: ZBC Kennisbank.

Zijlstra, W. (2016). *NEN 7510 SCHUIFT VERDER OP NAAR ISO 27001 EN WORDT VOLWASSEN.* https://zbc.nu/security/nen-7510-informatiebeveiliging-in-de-zorg/nen-7510-schuift-op-naar-iso-27001-en-wordt-volwassen/: ZBC Kennisbank.

Zurkus, K. (2019). *What Does Healthcare Cybersecurity Look Like in a Future of Connected Medical Devices?* https://securityintelligence.com/what-does-healthcare-cybersecurity-look-like-in-a-future-of-connected-medical-devices/: SecurityIntelligence by IBM.

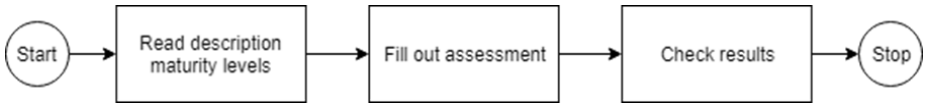
Appendix A – Maturity Model

Version: FINAL

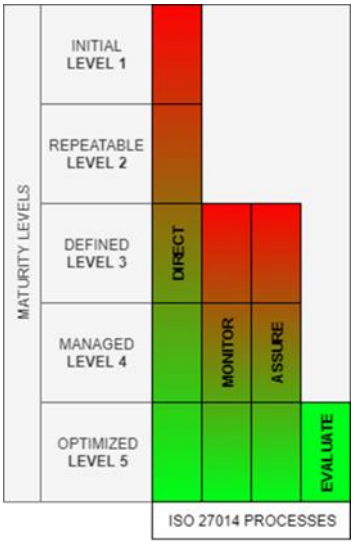
Introduction

The goal of the maturity model is to measure information security governance in Dutch hospitals.

1. Read the descriptions of the maturity levels in the Description of maturity levels-tab.
2. There are five capability domains which all measure a specific attribute of information security governance competence. Each of the capability domains consists of a set of assessment questions which have to be answered.
3. The assessment questions can be answered by selecting the button which reflects the current situation of your hospital.
4. When all the assessment questions are answered the results can be viewed in the Results-tab.
5. Results are calculated according to the following formula: each maturity level has a specified amount of points (level 1 = 1 point, level 2 = 2 points etc.). The total amount of points in each capability domain is divided by the amount of questions and an average for each capability domain is calculated.



Description of maturity levels



This tool can be used as an instrument to measure information security governance within the hospital environment. The five capability domains are 'Organisation', 'Strategic Alignment', 'Risk Management', 'Validation' and 'Value Capturing & Delivery'. Each capability domain will capture an important part of Information Security Governance. Every capability exists of a series of questions (attributes) which will be used for the assessment of the capability domain. Every question can be assessed according to the five maturity levels which are determined for each individual question. When all the questions have been answered the results will be displayed in the 'Results'-tab.

Maturity Level	Description
Initial	This level is the starting point for organisations; directing is done in an informal way without a strategy, direction, objective or policy. Issues are solely dealt with in a reactive manner. There is no monitoring and evaluating of performance at all.
Repeatable	Organisations are directing in a more formal way; there are policies, objectives and a strategy, however the focus is limited, not organisation-wide and an overview is missing. The limited things the organisation does are starting to become repeatable however there is no monitoring and evaluating at all.
Defined	The organisation is directing in a formal way, is organisation-wide focused and the important aspects are considered. The organisation is trying to improve its processes because of a compliance-driven mindset. The organisation is starting to implement monitoring and seeks validation through audits because of regulatory requirements.
Managed	The organisation has a well-established information security management system which effectiveness is actively being monitored with proper metrics, and it proactively reacts to issues; the organisation seeks validation and assurance by in-depended audits and the organisation is in control. The organisation actively works to create strategic alignment between business and security and to create organisational-wide support for information security.
Optimized	The organisation is in full control of its information security and sees compliance as a baseline. The organisation monitors its information security management systems' effectiveness and is constantly trying to improve itself by evaluating and creating improvement plans. The governing body is aiming to deliver as much perceived value and trust as possible.

Capability Domain: Organisation

The goal of the organisational capability domain is to:

- Context about how information security is currently managed.
- The attitude of the hospital is regarding information security.

ORG1	Does the hospital have a CISO?
1 (Initial)	The hospital has not specified an independent role which is responsible for the information security program.
2 (Repeatable)	The hospital has specified a role responsible for the information security program however this is largely focused on operational information security.
3 (Defined)	The hospital has specified a role responsible for the organisational-wide security program however this is vested with another role like CEO/CIO/CTO.
4 (Managed)	The hospital has an independent Chief Information Security Officer (CISO) which is responsible for the coordination, development, implementation, maintenance and improvement of the information security program.
5 (Optimized)	The hospital has a Chief Information Security Officer (CISO) and an Information Security Risk Manager who together are responsible for the coordination, development, implementation, maintenance and improvement of the information security program.

ORG2	Who coordinates information security within the hospital?
1 (Initial)	There is no coordination
2 (Repeatable)	There is no security department. Security is being executed in an ad-hoc manner (every department on its own), there is no alignment within the hospital. OR Security is solely being managed by the IT department.
3 (Defined)	Security is being managed by an information security department but in an ad-hoc way.
4 (Managed)	Security is being coordinated by a security department in correspondence with the other hospital departments.
5 (Optimized)	Security is internally being coordinated by a security department and actively stimulates external cooperation with other hospitals to create and support knowledge sharing.

ORG3	Is the need for information security acknowledged by the board members of the hospital?
1 (Initial)	The board isn't informed about information security at all.
2 (Repeatable)	The board acknowledges information security but actions are missing/not being acted upon/no priority/informal.
3 (Defined)	The board acknowledges information security and has made some plans but isn't organisationally wide focused.
4 (Managed)	The board acknowledges information security at the organisational wide level and is communicating their vision for information security top-down to the security department.
5 (Optimized)	The board acknowledges information security at the organisational wide level, has active communicated their vision for information security through the whole hospital and all it's employees and is actively carrying out their own vision themselves (leading by example).

ORG4	How well is information security represented at the strategic level?
1 (Initial)	There is nobody representing information security in the boardroom.

2 (Repeatable)	Somebody has the portfolio of information security however qualifications for the portfolio is missing.
3 (Defined)	An existing role (like CTO/IT/CIO) has the portfolio information security.
4 (Managed)	There is an independent information security role which has the required qualification and is held responsible for information security.
5 (Optimized)	An independent information security role is existing but information security related responsibilities are shared among all board members.

ORG5	Why does top management want to improve their information security maturity?
1 (Initial)	They don't want to improve at all.
2 (Repeatable)	They want to improve because they are afraid of fines from regulatory bodies.
3 (Defined)	They want to improve because they recently have been in a security incident and want to improve because of availability bias.
4 (Managed)	They want to improve because they see information security as a necessity.
5 (Optimized)	They want to improve because they see information security as a business enabler and see the added value to the business.

ORG6	Has the hospital determined its stakeholders regarding information security?
1 (Initial)	The hospital has not determined it stakeholders regarding information security.
2 (Repeatable)	The hospital has determined internal stakeholders at the adhoc level.
3 (Defined)	Organisational wide the hospital has determined its internal and external stakeholders regarding information security.
4 (Managed)	Organisational wide the hospital has determined its internal and external stakeholders regarding information security. The hospital has classified the amount of power each stakeholder has on the business of the hospital.
5 (Optimized)	Organisational wide the hospital has determined its internal and external stakeholders regarding information security. The hospital has classified the amount of power and interest which each stakeholder has on the business of the hospital.

Capability Domain: Strategic Alignment

The goal of the strategic alignment capability domain is to:

- How (well) information security is embedded within the organisation.
- Leadership of information security.
- Alignment between the strategic and operational layer regarding information security.
- Responsibility of information security.

SA1	Are information security issues considered in all important decisions within the hospital?
1 (Initial)	Information security issues are not considered in important decisions at all.
2 (Repeatable)	Information security issues are considered on an ad hoc basis.
3 (Defined)	Information security is embedded within decision making at a basic level (like integration in templates) and is integrated during strategic planning cycles. Risk management for information security is accepted during decision making.
4 (Managed)	Information security is embedded within all the important decision making (strategic and operational planning cycles) since risk management is part of the hospitals decision making culture.
5 (Optimized)	Information security is embedded within all decision making and is part of every process and department. Decision are later on evaluated and improved if possible.

SA2	How are relevant information security policies implemented within the hospital?
1 (Initial)	Policies are (almost) non-existent within the hospital.
2 (Repeatable)	Policies are documented and published.
3 (Defined)	Policies are documented, published and have been approved by management.
4 (Managed)	Policies are documented, published, approved by management and are clearly communicated to the rest of the hospital.
5 (Optimized)	Policies are documented, published, approved, communicated and we regular check if employees are aware of the policies. Policies are constantly being reviewed and updated if required.

SA3	Are the roles and responsibilities regarding information security clearly defined and implemented?
1 (Initial)	Roles and responsibilities are created, but unknown, and haven't been communicated towards the involved parties.
2 (Repeatable)	Roles and responsibilities are informally communicated towards the involved parties
3 (Defined)	Roles and responsibilities are in accordance with security policies, are formally communicated towards the involved parties.
4 (Managed)	Roles and responsibilities are in accordance with security policies and are defined in a RACI chart and are communicated towards the involved parties
5 (Optimized)	Roles and responsibilities are in accordance with security policies, are formally communicated and are regularly checked with towards the involved parties (up to date RACI chart), to assure an up-to-date role and responsibility definition.

SA4	Is the usability/user-friendliness/workability of a security control considered when designing security solutions?
1 (Initial)	Security controls are not adapted to the business processes at all.
2 (Repeatable)	Some security controls have been adapted to fit the business processes however this is designed by the security department themselves.
3 (Defined)	To create usable, user-friendly security controls the security department evaluates general feedback from hospital employees.
4 (Managed)	There is tight collaboration between the security department and medical employees to ensure the creation of user-friendly but effective security controls.
5 (Optimized)	There is a tight collaboration between the security department, medical employees, and a Chief Medical Information Officer (CMIO) has been appointed to oversee this process to create user-friendly and effective security controls.

SA5	What strategy does the hospitals leadership use to create and maintain organisational support for information security?
1 (Initial)	Leadership doesn’t communicate about information security at all.
2 (Repeatable)	Leadership only briefs specific departments about information security like the IT department.
3 (Defined)	Leadership sends a generic briefing about the status of information security once in a while to the whole organisation.
4 (Managed)	Leadership reports top down about information security statistics to create organisational support.
5 (Optimized)	Leadership reports top down and actively collects feedback (using a process) from the whole organisation to improve the organisational wide information security support.

SA6	How are information security responsibilities and objectives implemented at the strategic layer?
1 (Initial)	There are no security KPI's on the strategic level at all.
2 (Repeatable)	There are some general objectives for information security however they are not being acted upon (nobody is really responsible, the objectives are unclear, no real KPI's).
3 (Defined)	Only the CISO is responsible for information security and has proper KPI's (which are only for the CISO him/herself).
4 (Managed)	The CISO and board have a shared responsibility however there is a conflict of interest with other KPI's (or we never payed attention to conflicting KPI's).
5 (Optimized)	The whole board is responsible and the CISO take the authority and responsibility to achieve those KPI's. Hospital wide KPI's are aligned and a conflict of interest is appropriately managed (alignment between security KPI's vs other KPI's like efficiency).

Capability Domain: Risk Management

The goal of the risk management capability domain is to:

- A clear strategy regarding information security risk management
- Leadership of information security risk management.
- Information security risk decision making.
- Handling of information security incidents.
- Handing of third party risks.
- Being in control about configuration items.
- Implementation of connected medical devices within the hospital environment.

RM1	What is the maturity of information risk management decision making at the directors level?
1 (Initial)	The board of directors is unaware of any information risks in the hospital.
2 (Repeatable)	The board of directors is limited aware of information risks but (deliberately) doesn't take action.
3 (Defined)	The board of directors is generally aware of information risks and wants action be taken.
4 (Managed)	The board of directors is aware of risks, it has identified threats, vulnerabilities, analysed the likelihood and knows the impact of risks on the business.
5 (Optimized)	The board of directors is aware of risks, it has identified threats, vulnerabilities, and has assessed the likelihood. A risk appetite and improvement plan has been created and the board of directors acknowledges residual risks (and has signed for this).

RM2	Is there a risk management program implemented where information security is considered?
1 (Initial)	The hospital is managing information risk, vulnerabilities or threats at a minimal level.
2 (Repeatable)	Information risks are being identified without a standardized process and are limited to silo thinking.
3 (Defined)	Information risk management is being executed accordingly to a proper risk management strategy however risks are being managed in a formalized process like the ISO 27005/31000 but mainly for compliance reasons.
4 (Managed)	Information risks are being managed using a formalized process and is being monitored closely to check if the process is in-line with the risk management strategy expectations.
5 (Optimized)	Information risks are constantly being assessed and evaluated against the impact on the hospitals integrity, availability and confidentiality.

RM3	What is the attitude towards managing risks?
1 (Initial)	There is no formal attitude towards (information security) risks.
2 (Repeatable)	Risks are generally addressed in a reactive manner (curing when occurring). Security is usually seen as obstructive and a technical-'thing'.
3 (Defined)	Risks are being dealt with whenever they occur, however there are some preventive security controls implemented (mainly to achieve compliance).
4 (Managed)	Risk are mitigated for security reasons and not compliance reasons, however this is not a continuous process but the organisation is trying to stimulate a pro-active attitude.
5 (Optimized)	Risk are dealt with in a pro-active manner. Risk management is a continuous process which is monitored and improved. Securing is seen as a business enabler.

RM4	Who participates in the information risk management decision process?
1 (Initial)	Information risk management is not being executed at all.
2 (Repeatable)	Information risk management is being executed by the IT department.
3 (Defined)	Information risk management is being executed by just the CISO/Risk Manager.
4 (Managed)	Information risk management is largely being executed by the CISO/Risk Manager, with support of the departments and the board of directors is briefed when required.
5 (Optimized)	Information risk management being executed by departments themselves (collaborative risk management) and are being managed and guided by the CISO/Risk Manager. The board of directors is being briefed when required.

RM5	Has the hospital identified and classified its configuration items (assets)?
1 (Initial)	No.
2 (Repeatable)	Partially identified and classified.
3 (Defined)	The hospital has identified the full lifecycle of the configuration items but has not classified the items (yet).
4 (Managed)	The hospital has identified and classified the full lifecycle of the configuration items.
5 (Optimized)	The hospital has identified and classified the full lifecycle of the configuration items and the hospital reviews this process continuously.

RM6	What is the strategy for information security incident response within the hospital?
1 (Initial)	The hospital doesn't have a plan regarding incident response.
2 (Repeatable)	The hospital has an informal process to respond to information security incidents.
3 (Defined)	The hospital has a formal process to respond to information security incidents, but this is not complete yet (there must be a BIA, IR DR and BC plan).
4 (Managed)	The hospital has a formal process to respond to information security incidents, which is complete but has not or partly been tested.
5 (Optimized)	The hospital has a formal process to respond to information security incidents, which is complete, tested and is continuously being improved.

RM7	How are information security incidents collected and acted upon?
1 (Initial)	The hospital does not have a process to collect information security incidents.
2 (Repeatable)	Information security incidents are being collected but are not actively being analysed.
3 (Defined)	Information security incidents are being collected but are only acted upon when there is an immediate threat.
4 (Managed)	Information security incidents are being collected and are always analysed and acted upon if required.
5 (Optimized)	Information security incidents are actively monitored (for trends) and the root cause analysis will lead to (new or additional) mitigating measures that will improve the general information security management program.

RM8	Has the hospital included third party risk management in its information risk management program?
1 (Initial)	Third party suppliers are not part of the information risk management program.

2 (Repeatable)	The hospital has security requirements for third party suppliers, however these are not always enforced.
3 (Defined)	The hospital has security requirements for third party suppliers and actively enforces these security requirements on the third party vendors.
4 (Managed)	The hospital has security requirements for third party suppliers and actively enforces these security requirements on third party vendors and check this by validation through independent audit reports.
5 (Optimized)	The hospital has security requirements for third party suppliers and actively enforces these security requirements on third party vendors and validates this with independent audit reports and constantly improve our third party contract by applying third party contract management.

RM9	How does the hospital ensure the secure implementation of (connected) medical devices?
1 (Initial)	The hospital has no policy to implement connected medical devices.
2 (Repeatable)	Connected medical devices are implemented using an informal process
3 (Defined)	Connected medical devices are implemented according to a specific policy and have security controls according to the set security requirements, however not all medical devices are currently implemented according to that specific policy.
4 (Managed)	Connected medical devices are implemented according to a specific policy with proper security controls according to the security requirements and we have a process to ensure all devices are implemented according to the security requirements.
5 (Optimized)	Connected medical devices are implemented according to a specific policy with proper security controls according to the security requirements and we test the effectiveness of this policy by executing independent pen tests and vulnerability scans.

RM10	What kind of implementation measures has the hospital taken to enhance the security of (connected) medical devices?
1 (Initial)	The hospital has not implemented any security controls with regards to (connected) medical devices.
2 (Repeatable)	The hospital has some compensating controls however this doesn't fulfil the security requirements (network segmentation, monitoring and detection systems).
3 (Defined)	The hospital has compensating controls like network segmentation, monitoring and detection systems for connected medical devices however the hospital has not implemented all the intended devices according to these requirements (or has on idea about the coverage).
4 (Managed)	The hospital has some compensating controls like network segmentation, monitoring and detection systems for connected medical devices however this isn’t implemented across all the connected medical devices.
5 (Optimized)	The hospital has compensating controls like network segmentation, monitoring and detection systems for connected medical devices and this is actively being applied for all the connected medical devices and the hospital checks this.

Capability Domain: Validation

The goal of the validation capability domain is to:

- How the performance of information security management is being monitored.
- The performance of the governance body of information security.
- How the organisation checks validity of their information security activities.

VA1	How is the hospital trying to improve its general information security maturity?
1 (Initial)	The hospital has no ambition to improve, they have implemented a security baseline once and assume this is still effective.
2 (Repeatable)	The hospital has a basic understanding about its current situation and has a limited view on what their desired situation is. Plans to achieve the desired situation are missing.
3 (Defined)	The hospital knows it's current and desired situation and has plans to improve the system, however only wants to improve for compliance reasons (because the auditors says so).
4 (Managed)	The hospital actively measures its current situation by a set of metrics and wants to improve because of its intrinsic motivation to be secure.
5 (Optimized)	The hospital measures the current situation using a wide set of metrics and create and adapts plans to reach the desired situation.

VA2	Does the hospital have an information security management system to manage the hospitals information security?
1 (Initial)	The hospital does not have an information security management system.
2 (Repeatable)	The hospital has a limited information security management system however this is not according to any best practice (like an ISO 27001/NEN7510)
3 (Defined)	The hospital has an information security management system based on a best practice but the system is still in progress/development.
4 (Managed)	The information security management system is implemented, audited but has not been certified.
5 (Optimized)	The information security management system is implemented, audited, certified and continuously provides feedback to the governing body.

VA3	Has the hospital established an effective scope for its information security management system?
1 (Initial)	The hospital has not identified an effective scope at all.
2 (Repeatable)	The hospital has focused on a limited scope (like only the IT department) and is not organisational wide focused.
3 (Defined)	The hospital has created an information security management system for its critical components.
4 (Managed)	The hospital has created an information security management system for its critical components and aims to implement its information security management system organisational wide.
5 (Optimized)	The hospital has created an organisational wide information security management system and focusses specifically on important components which it aims to constantly improve.

VA4	How is the hospital checking the validity of its information security management system?
1 (Initial)	The hospital has no checks on its information security management system.

2 (Repeatable)	The information security management departments checks a limited scope at an irregular interval.
3 (Defined)	An independent internal department executes a regular audit of a limited scope.
4 (Managed)	An independent internal department executes a regular audit of the whole information security management system.
5 (Optimized)	An independent internal and external audit gets regularly executed on the whole information security management system.

VA5	How is the performance of the information security management system being monitored?
1 (Initial)	The hospital does not have any active measurements on its information security management system
2 (Repeatable)	The hospital monitors just a few things but the hospital don't know exactly what, and for what reason. It's largely an informal process.
3 (Defined)	The hospital has implementation measures.
4 (Managed)	The hospital has implementation measures and monitors the security controls effectiveness with effective and efficiency measures.
5 (Optimized)	The hospital monitors the implementation, effectiveness and impact of a security and monitor the (business) impact the security control has on the hospital.

VA6	What metrics does the hospital use to measure the impact of the information security program?
1 (Initial)	Information Security Governance metrics are not available.
2 (Repeatable)	Some metrics are available but those are mainly metrics which are part of information security management.
3 (Defined)	The hospital has metrics with regards to information security governance like; reputational damage, critical infrastructure monitoring
4 (Managed)	The hospital has metrics for a number of important governance metrics like; reputational damage, all critical components monitoring (software, hardware, infrastructure) and the amount of delayed projects because of security concerns. The hospital also includes their own competences perceived by others as a metric for information security governance.
5 (Optimized)	The hospital has metrics which completely reflect the status of information security governance, like; reputational damage, all critical components monitoring (software, hardware, infrastructure), the amount of delayed projects because of security concerns and security awareness among the whole organisation. The hospital also includes their own competences perceived by others as a metric for information security governance.

VA7	What are the conditions of an internal audit of its information security management system?
1 (Initial)	There is no standardized process for internal auditing.
2 (Repeatable)	Auditing is executed ad-hoc and with a limited scope. The audit only looks at its own internal requirements (if there are any at all).
3 (Defined)	Auditing is executed with an organisational wide focus according to a formalized process (scope and criteria have been established). The audit is executed conform the hospitals internal and external requirements.
4 (Managed)	Auditing is executed with an organisational wide focus according to a formalized process (frequency, priority , scope and criteria have been established). The audit is

	executed conform the hospitals internal and external requirements. Results are reported to relevant management.
5 (Optimized)	Auditing is executed with an organisational wide focus according to a formalized process (frequency, priority , scope and criteria have been established). The audit is executed conform the hospitals internal and external requirements. The auditor is independent and retains results as evidence. Results are reported to relevant management.

VA8	How does top management ensure the reviews of the suitability, adequacy and effectiveness of the hospitals information security management system?
1 (Initial)	Top management does not execute any form of management review of the information security management system.
2 (Repeatable)	Top management only considers (external and internal) issues that are a serious threat to the information security management system.
3 (Defined)	Top management reviews collected information by the information security management system like fulfilment of security objectives, audit results, incidents and solutions.
4 (Managed)	Top management reviews new and previously collected information (trend) by the information security management system like fulfilment of security objectives, audit results, incidents and solutions for improvement. Feedback is collected from stakeholders for improvement.
5 (Optimized)	Top management reviews new and previously collected information (trend) by the information security management system like fulfilment of security objectives, audit results, incidents and solutions for improvement. Feedback is collected from stakeholders and there is cooperation with information risk management for continuous improvement.

Capability Domain: Value Capturing & Delivery

The goal of the value capture & delivery capability domain is to:

- Financial decision making regarding information security investments.
- Perceived value of trust and enablement of service because of information security.
- Adequate use of information security solutions and resources.
- Overview of information security components.

VCD1	Does the hospital invest enough in information security resources (money, time and energy)?
1 (Initial)	No, there is a complete lack in resources because the board does not view information security as a top priority.
2 (Repeatable)	The willingness from top management to invest is present, and some resources are available however they are limited.
3 (Defined)	Resources are sufficiently available to preserve the current state of the information security management system.
4 (Managed)	Resources are sufficiently available to preserve and improve the current state of the information security management system.
5 (Optimized)	Resources are sufficiently available, captured and efficiently (re)used to preserve and improve the current state of the information security management system.

VCD2	How are information security related investments made within the hospital?
1 (Initial)	Investments regarding information security are not made according to a formalized process.
2 (Repeatable)	Investments regarding information security are only briefly evaluated when large amounts of money are involved.
3 (Defined)	Investments regarding information security play an important role in any IT related project.
4 (Managed)	Security investments are identified, assessed and evaluated in accordance with the domain experts within the hospital, there is largely a financial stake and is considered in all types of project within the hospital (not just limited to IT).
5 (Optimized)	Security investments are identified, assessed and evaluated in accordance with the domain experts within the hospital and is supported by previously collected statistics from the information security management system.

VCD3	How does the hospital capture and utilize their information security related resources (efficiently)?
1 (Initial)	The hospital does not have a process to capture or utilize information security related resources at all.
2 (Repeatable)	The hospital has some documentation about its security related resources however this is very limited and shared adhoc at most. Information is usually added once by a CISO.
3 (Defined)	The hospital has one central point where information about security related resources are collected (like a wiki/intranet) however this is not actively promoted or being updated.
4 (Managed)	The hospital has a knowledgebase which is up-to-date with all the information regarding information security related issues. The hospital checks if employees are aware of the resources and where they can find more information about them.
5 (Optimized)	The hospital actively promotes the use of information security related resources, has an up-to-date knowledgebase, repeatedly checks this with the hospitals employees (by gathering feedback) and tries to update the knowledgebase collectively with input from employees.

VCD4	How has the hospital created a security architecture?
1 (Initial)	The hospital has no security architecture at all.
2 (Repeatable)	The hospital has a limited security architecture of a few departments (like just the IT department). No structured methods are used for the creation of the security architecture.
3 (Defined)	The hospital has a basic security architecture according to a standard however this is not complete yet.
4 (Managed)	The hospital has a complete enterprise security architecture and uses this to design information security within their hospital.
5 (Optimized)	The hospital manages its information security resources according to the enterprise security architecture and constantly improves this while aiming for resource optimization.

VCD5	Is there a process for the estimation of investments in information security (solutions)?
1 (Initial)	There is no formal process for the estimation of investments in information security (solutions).
2 (Repeatable)	Estimations are largely created based on their monetary value, other criteria are not considered (or available).
3 (Defined)	There is increased awareness for security investments and an investment program has been created. Business cases are starting to be required for at least some (important) investments.
4 (Managed)	There is full understanding about security investments and business cases are constantly being made using basic metrics. The focus switched from largely a cost perspective to business outcomes. A few tools exist to manage the investments.
5 (Optimized)	There is full understanding and commitment for security investments, business cases are comprehensive and complete and are constantly being monitored using metrics. Investments are revised, cancelled or improved when required. There is a large set of tools and required skills to manage the investments. and the full economical life-cycle, and (non)-financial aspects are considered.

VCD6	Does the hospital measure the amount of perceived value within the organisation?
1 (Initial)	The hospital does not measure how information security is experienced within the organisation.
2 (Repeatable)	The hospital measures adhoc if employees trust the information security program.
3 (Defined)	The hospital measures adhoc if employees trust the information security program and measure the enablement of services because of the possible increased trust in the information security program.
4 (Managed)	The hospital measures organisational wide if employees trust the information security program, measure the enablement of services because of the possible increased trust in the information security program and collect feedback about the perceived skill of the hospitals strategic layer.
5 (Optimized)	The hospital measures organisational wide if employees trust the information security program, measure the enablement of services because of the possible increased trust in the information security program and collect feedback about the perceived skill of the hospitals strategic layer. The hospital uses this information to change their information security governance program.

Appendix B – Maturity Model Assessment Tool

ISG_MaturityModel
_v0.5_FINAL.xlsx

Appendix C – Structured Interview Form

Information Security Governance Maturity Model – Feedback form

Name	
Date	
Organisation	
Position	
Years of experience in Information Security	

Criteria	Strongly Disagree	Slightly Disagree	Neutral	Slightly Agree	Strongly Agree
The maturity levels are sufficient to represent, all maturation stages of the domain (Sufficiency).					
There is no overlap detected between descriptions of maturity levels (Accuracy).					
The questions are relevant to the domain (Relevance).					
The questions cover all aspects impacting/ involved in the domain (Comprehensiveness).					
The questions are clearly distinct (Mutual Exclusion).					
The questions are correctly assigned to their respective maturity level (Accuracy).					
The maturity levels are understandable .					
The assessment questions are understandable.					
The documentation is understandable.					
The scoring scheme is easy to use.					
The assessment guidelines are easy to use.					
The documentation is easy to use.					
The maturity model is useful conducting assessments.					
The maturity model is practical for use in the hospital industry.					

Question 1	Would you add any maturity levels? If so please explain what and why?

Question 2	Would you update the maturity level description? If so please explain what and why?

Question 3	Would you add any questions? If so please explain what and why?

Question 4	Would you remove any of the questions? If so please explain what and why?

Question 5	Would you redefine/update any of the questions? If so please explain what and why?

Question 6	Would you suggest any updates or improvements related to the scoring scheme? If so please explain what and why?

Question 7	Would you suggest any updates or improvement related to the criteria for each question? If so please explain what and why?

Question 8	Would you like to elaborate on any of your answers?

Question 9	Could the model be made more useful? How?

Question 10	Could the model be made more practical? How?

Appendix D – Interviews With Experts

Confidential