THESIS

THE CYBER SECURITY RISK ASSESSMENT MATURITY OF HOSPITALS

Master thesis version 1.0
25-08-2014

Arnold Jeen Jansen
Master of Business Informatics
Institute of Information and Computer Science,
Utrecht University

Supervisors UU:
Ronald Batenburg
Marco Spruit

Supervisor Deloitte:
Jessica Conquet

Universiteit Utrecht

Deloitte.

Abstract

As cyber security becomes more important at hospitals, the components of cyber security should be improved as well. Cyber security risk assessment (CSRA) is one of these important components of cyber security. This research develops a Hospital Cybersecurity Risk Assessment Maturity Model (HCRAMM) to enable hospitals to measure the maturity of their CSRA process. The research starts with a systematic literature research and a comparison analysis of CSRA related methods to identify important concepts and requirements for the HCRAMM. The HCRAMM is then further iteratively improved by 17 expert interviews, of which four were used to validate final results, among security officers of hospitals and other cyber security experts in the health-care sector. The developed HCRAMM is translated into a survey, which in turn is distributed among hospitals in the Netherlands. From this thesis research it is concluded that the HCRAMM is a useful tool to measure the maturity of CSRA. Also hospitals have large opportunities to improve their CSRA by increasing the awareness and skills of human capital related to the risk assessment as well as the improvement of process structures, which then could enable the use of more tools and quantification as to improve the maturity. Finally a more sophisticated form of iterative improvement could be obtained from the use of centralized information storage and retrieval considering the data needed and processed during the CSRA process.

Key words: Cyber Security, Information Security, Risk Assessment, Cyber Threats, Threat Landscape, Maturity Model, Hospital, HCRAMM.

Acknowledgement

"A little learning is a dangerous thing.
Drink deep, or taste not the Pierian Spring;
There shallow draughts intoxicate the brain,
and drinking largely sobers us again."

-Alexander Pope

Here before you lays my final work of my master's thesis. A work which I hope you will read with pleasure as it took over seven months of hard work and dedication to complete. A period seemingly long but fast forgotten when the result is completed. My hope is that this hard work will provide hospitals and scientists with and increased insight in the cyber security risk assessment process and. That it will help them, even if a little, to secure our data in order to improve our safety and maintain our privacy. Because the words of Alexander Pope do not only describe the academic perspective, but apply as well to cyber security, because if one does not know into depth itself and if one does not knows the threats it faces into depth he will be in danger. Or in the words of the Chinese strategist Sun Tzu:

It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.

-Sun Tzu

During the process of this thesis I received great support from many people, in many ways. First I would like to thank Ronald Batenburg, who as first supervisor proved to be a valuable mentor, who guided me through the process. Secondly I would like to thank Jessica Conquet, my supervisor at Deloitte, for the sharp feedback as well as the connections she provided me with. Also I would like to thank Marco Spruit for the sharp feedback he gave me towards the end, enabling me to bring my thesis to a higher level. Furthermore I would like to thank all the people who participated to this research by providing me with interviews or survey results, security managers at hospitals, colleagues at Deloitte and other experts. Finally I would like to thank my father and mother for supporting me through this process and especially thank my girlfriend for supporting me during this thesis research as it was not always easy.

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Research Trigger

Information technology has brought many benefits to hospitals. Healthcare processes can be performed more efficiently and faster, the quality of patient information has been increased and new diagnosing and treatment options have sprung through the use of new medical devices. However without the appropriate defensive actions, these systems and devices are vulnerable to cyber attacks. Currently industry wide cyber attacks become more sophisticated, which might increase the changes of successful cyber attacks (Choo, 2011). Scenarios are possible in which information from systems is stolen, altered or deleted (Foltz, 2004). Cyber attacks at hospitals may include the hacking into an electronic patient file and changing the medicine prescription of a patient to a lethal dosage (Saint-Claire, 2011). Information systems can be disabled and communication networks can experience denial of service (Harries & Yellowlees, 2013). Medical devices can be implemented with viruses or hacked which may cause them to shut down or run amok. Implantable devices such as pacemakers and insulin pumps have already been hacked before (Fu, 2009) (Halperin et al., 2008). Most cyber attacks against hospitals focused on data. Between 2010 and 2012 94% of the healthcare organizations in America had at least one data breach. More than half of these data breaches had cost healthcare organizations over 500.000 dollar (Ponemon Institute, 2012).

Dutch hospitals as well became victim of such malicious activities. Several cases in which hospitals faced problems with their cyber security occurred. In 2012 for example a hacker gained access to a badly protected server of the Groene Hart hospital and demonstrated that 47 medical patient files and personal data of half a million people could be accessed. The hospital admitted it was already hacked several times before (Nu.nl, 2012).

1.2 Problem Statement

As information systems and networks in hospitals become more and more critical for operations, the amount of cyber security risks hospitals face increase in number and impact. To protect themselves against these cyber security risks hospitals must know what threats they are vulnerable to and at which cyber assets these are targeted. After all, hospitals have limited funds available for their cyber security and thus need to mitigate related risks in a resource efficient manner. Therefor hospitals must first know the threat landscape in which they operate. As this is a complex and fast changing threat landscape many hospitals may not include the full picture into their cyber security risk assessment (CSRA). Secondly the CSRA currently performed is expected to be less advanced than for example the CSRAs performed in the financial and telecom sector, which are often targeted by cyber attacks. However as cyber security risks are increasing for hospitals, a more mature CSRA process is needed to improve the overall cyber security. No clear measurement and roadmap to improve the CSRA seems to exist yet. This leads towards the following problem statement:

> *"Hospitals face an increasing amount of cyber security risks. They, however, are probably not fully aware of the whole threat landscape they face and do not seem to have a clear measurement tool and roadmap to improve their cyber security risk assessment."*

The objective of this research is to develop a CSRA maturity model for hospitals and research how mature the CSRA process at hospitals is at the moment and how they can improve this.

1.3 Research Question

The main research question is stated such that a solution for the problem statement is provided.

> *"How can hospitals improve the maturity of their cyber security risk assessments?"*

1.4 Sub Research Questions

The sub questions need to be answered to answer the main research question. They each represent a part of the research which will be conducted.

SRQ 1. What is known about the cyber security risk assessment context of hospitals?

This sub question will answer what is known in research and at hospitals about the context in which cyber security risk assessments at hospitals take place. A main focus will be on the threat landscape of hospitals, but attention will be given to relevant culture as well.

SRQ 2. How can hospitals perform cyber security risk assessment?

This sub question will answer how hospitals can identify important cyber assets, vulnerabilities and cyber security threats, analyze the probability and impact of the cyber threats resulting from these and evaluate them accordingly.

SRQ 3. How can a maturity model based on previous maturity models be constructed to measure the maturity of the cyber security risk assessment in hospitals?

This sub question will answer which related maturity models already exist and how they can provide the basis for a new cyber security risk assessment maturity model. This maturity model will show the maturity dimensions which are important for cyber security risk assessment and the different maturity stages of these.

SRQ 4. How mature is cyber security risk assessment in Dutch hospitals and how can they improve?

This sub question will try to answer up till what extend hospitals have the right people, processes and technologies considering cyber security risk assessment in place to ensure the continuity of their critical operations and how and what they should improve to gain a higher level of maturity.

1.5 Scoping

A clear scope of the research is important, since the research can be conducted in several ways and with a focus on several aspects or depts. In Figure 1 the research area is depicted and the relations with other research areas.

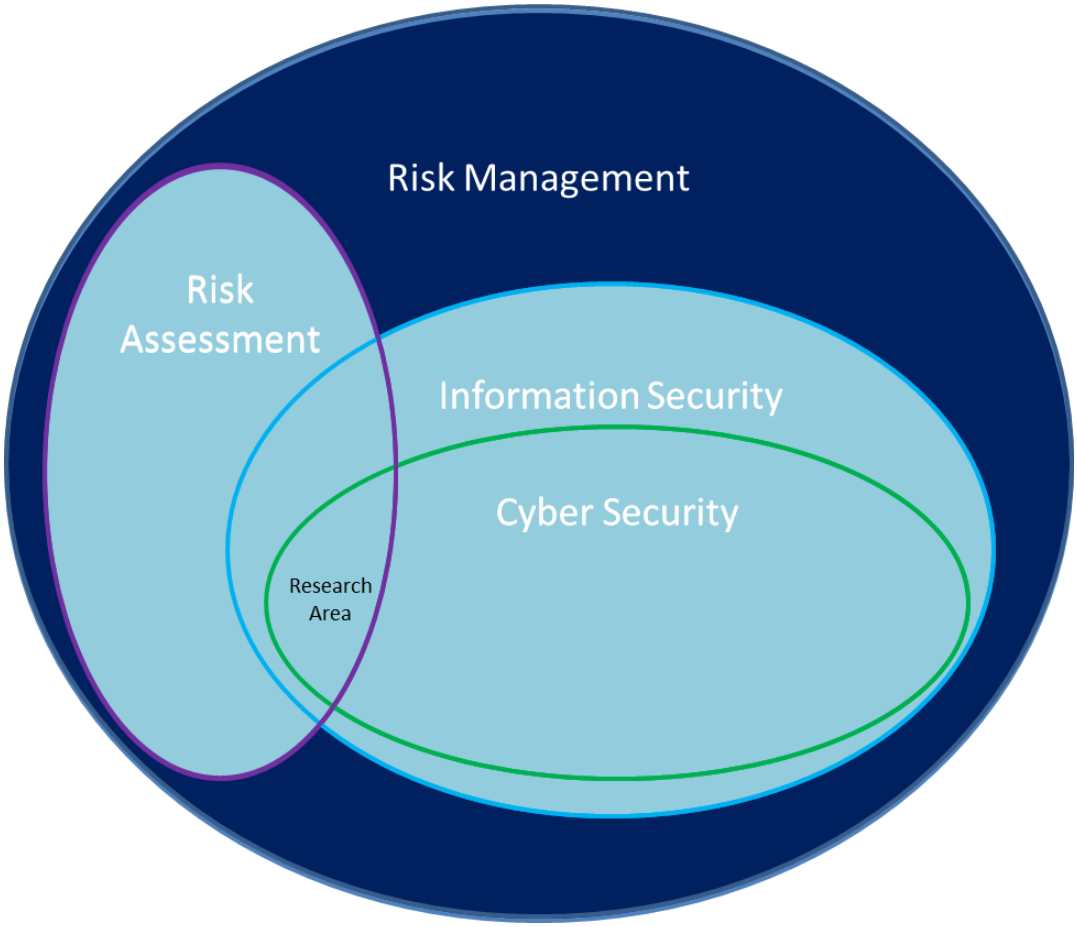


Figure 1: Positioning of the Research

Parts which are included in the scope are:

- Areas and topics related to cyber security risk assessment as component of information security risk assessment. Including the identification, analysis and evaluation of risks.
- Cyber security risk assessment and information security risk assessment approaches in general and concerning the hospital sector.
- Measurement methods to measure the maturity of processes within an organization.
- Context factors relevant for cyber security risk assessment in general and specifically for hospitals.

Excluded from the scope of this research are:

- Risks which to not utilize electronic attack vectors or do not threaten electronic assets.
- Events that may threat hospital information systems or equipment which occur due to a lack of regular maintenance.
- All other related research areas outside the defined research area of Figure 1.

1.6 Definitions

Certain core terms used in this thesis do not contain an unambiguous definition in both academic literature and business literature. To prevent confusion considering these important terms a clear and accepted definition is stated.

Cyber security:	*"Cyber security refers in general to methods of using people, process and technology to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyberspace."* (Bayuk, 2012)
Cyber security risk:	"*The combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.*" (WEF, 2012)
Cyberspace:	"*A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."* (Deibert & Rohozinski, 2010)
(Cyber) assets:	The electronic devices, information systems and databases existing in a company, such as laptops, medical devices, software programs, and the network environment for using them.
(Cyber) vulnerability:	A weakness in the security of an asset which allows an attacker to penetrate or disrupt a network or a system.
(Cyber) threat:	The possibility of a malicious attempt, which could reduce the accessibility, integrity or confidentiality of an (cyber) asset.
Threat actor:	An actor that possesses the ability to attack or increase the vulnerability of cyber assets. The cyber asset does not need to be targeted in a direct or specific manner.
Threat landscape:	An overview of threats and how these manifest themselves in combination with important assets and vulnerabilities.
Cyber security risk assessment:	The identification, analysis and evaluation of cyber security risks. Cyber security risk assessment is a sub-domain of information security risk assessment in which all the information assets are of an electronic (cyber) nature.

1.7 Study of Problem Relevance

1.7.1 Scientific Relevance

As the use of information technology in Dutch hospitals is increasing fast (Krediet et al., 2011), the adoption of new information systems for digital patient records, increased regulations and the increased need for information exchange between patients, providers and payers shows there is a need for better information security. However there still has been published little concerning security and privacy challenges in healthcare (Appari & Johnson, 2010).

The need for further research is more specifically phrased by Choo (2011): "*There is an ongoing need to conduct more strategic research and evaluation that can provide policy and practice relevant evidence that would enable policy makers and practitioners to design national regulatory measures and appropriate policy responses to address this new emerging cyber threat environment.*"

This need as defined by Choo (2011) will be satisfied by developing a maturity model, which will allow policy makers to measure and improve the maturity of their CSRA, an important process in the response and addressing of cyber threats. As the to be developed maturity model is focused on the hospital sector it simultaneously satisfies the problem statement by Appari & Johnson (2010) and fill a research gap in the scientific literature.

1.7.2 Social Relevance

Hua & Bapna (2013) argue that organizations that comprise the national critical infrastructure need to invest more heavily in cyber security than other organizations. When cyber attacks are targeted on hospitals with success, it will cost the hospitals large amounts of money to repair damages done. And in that extend also the taxpayers and patients to which the bill will be passed on.

Another result of a cyber attack may be a loss of privacy when for example medical records of patients are copied and publicized. It is difficult to estimate what exact consequences this may have on society, however legal consequences are already in place. In 2012 the Dutch bureau for protection of personal data (CBP) discovered that a large part of the Dutch hospitals had taken insufficient measures considering the confidentiality, integrity and availability of patient and medical data. This resulted in September 2012 towards the situation in which a hospital was reprimanded for infringement of the law (CBP, 2012). More often hospitals are fined or placed under increased control. And increasingly stronger privacy laws and regulations are developed at national and European Union level (European Commission, 2014).

The worst case scenario however may be when important information systems or medical equipment is purposefully shut down for example by infecting systems with viruses who use system resources until networks become ineffective (Saint-Claire, 2011). This may prevent hospitals to provide patients with the medical aid they need, causing risks on permanent health damage to these patients or even death.

To prevent such events from happening or at least decrease the impact of the results of cyber attacks, it is important that good policies are in place. Furthermore the Nationaal Cyber Security Centrum (2013) stated that to improve cyber security, an actual view on new developments, vulnerabilities, attack methods and defense mechanisms is needed in order to work effectively against cyber threats. This research will provide hospitals with a domain specific threat landscape and a method to improve CSRA, which is important for hospitals to optimize the effectiveness and resource efficiency of their cyber security.

2 Methodology

2.1 Design Science Requirements

Since the goal of this research is to research how hospitals can improve their CSRAs, a maturity model is developed in order to achieve this goal, the Hospital Cybersecurity Risk Assessment Maturity Model (HCRAMM). Furthermore as described before it should be based on a method that is scientific rigorous, evaluated and provides a good description of the process (Seale et al., 2004). A method that satisfies all these requirements and which was developed itself based on rigorous research is the IT maturity model development method of Becker et al. (2009).

In this method eight requirements are proposed for maturity models, which are based on the seven design science guidelines of Hevner et al. (2004) and the evaluation of 51 maturity models. These requirements for IT maturity models are as follows:

1. Comparison with existing maturity models: The maturity model must be substantiated by existing maturity models. The maturity model may as well be an improvement of an existing maturity model (Becker et al., 2009). The method of the HCRAMM contains a literature review of general cyber security maturity models and governance and risk compliance maturity models for hospitals.
2. Iterative procedure: Maturity models must be developed in an iterative manner (Becker et al., 2009). The method iteratively gathers information from experts as well as iteratively develop the method based on feedback.
3. Evaluation: All the principles and premises used in the development of the maturity model, as well as the usefulness, effectiveness and quality of the artifact must be evaluated in a iterative manner (Becker et al., 2009). The method uses the iterative expert interviews to evaluate the maturity model. Also a section of the questionnaire will request feedback which will be used to improve the HCRAMM.
4. Multi-methodological Procedure: The maturity model development process must contain a variety of research methods, which are well-founded and finely attuned (Becker et al., 2009). The method satisfies this requirement by using a systematic literature study as basis, complemented with a review of CSRA methods, followed up by expert interviews and finally a questionnaire is used.
5. Identification of Problem Relevance: The relevance of the maturity model for researchers and practitioners must be demonstrated (Becker et al., 2009). Both the scientific and social relevance are defined in the study of problem relevance. The scientific need is further extended in the systematic literature review.
6. Problem Definition: The prospective application domain of the maturity model, the conditions of its application and the intended benefits must be determined prior to design (Becker et al., 2009). In case of the HCRAMM the application domain is the CSRA of hospitals. Since the study is conducted in the Netherlands and as such a focus lays on Dutch hospitals. The HCRAMM provides a self-assessment tool to measure the maturity of a hospital's CSRA. From this measurement the gap towards an optimal CSRA can be identified and management solutions to improve the cyber risk assessment towards the optimal level can be taken.
7. Targeted Presentation of Results: The maturity model must be presented in such a manner that it meets the needs of its users (Becker et al., 2009). The method enables developed of the HCRAMM in such a way that hospital cyber security managers will be able to use it to improve their CSRA in a clear manner, by using the questionnaire based self-assessment tool.
8. Scientific Documentation: The design process of the maturity model must be documented in detail, considering each step of the process, the involved parties, the methods applied and the results (Becker et al., 2009). The process of developing the HCRAMM will be documented step by step in this thesis.

2.2 Research Process

Seven of the eight requirements are mapped in a procedural model for the development of maturity models (Figure 2). The last requirement is incorporated by the documents produced in the study of the maturity

model, combined in this thesis. The processes and deliverables of the procedural method are explained using a process-deliverable diagram (PDD) (van de Weerd & Brinkkemper, 2009).

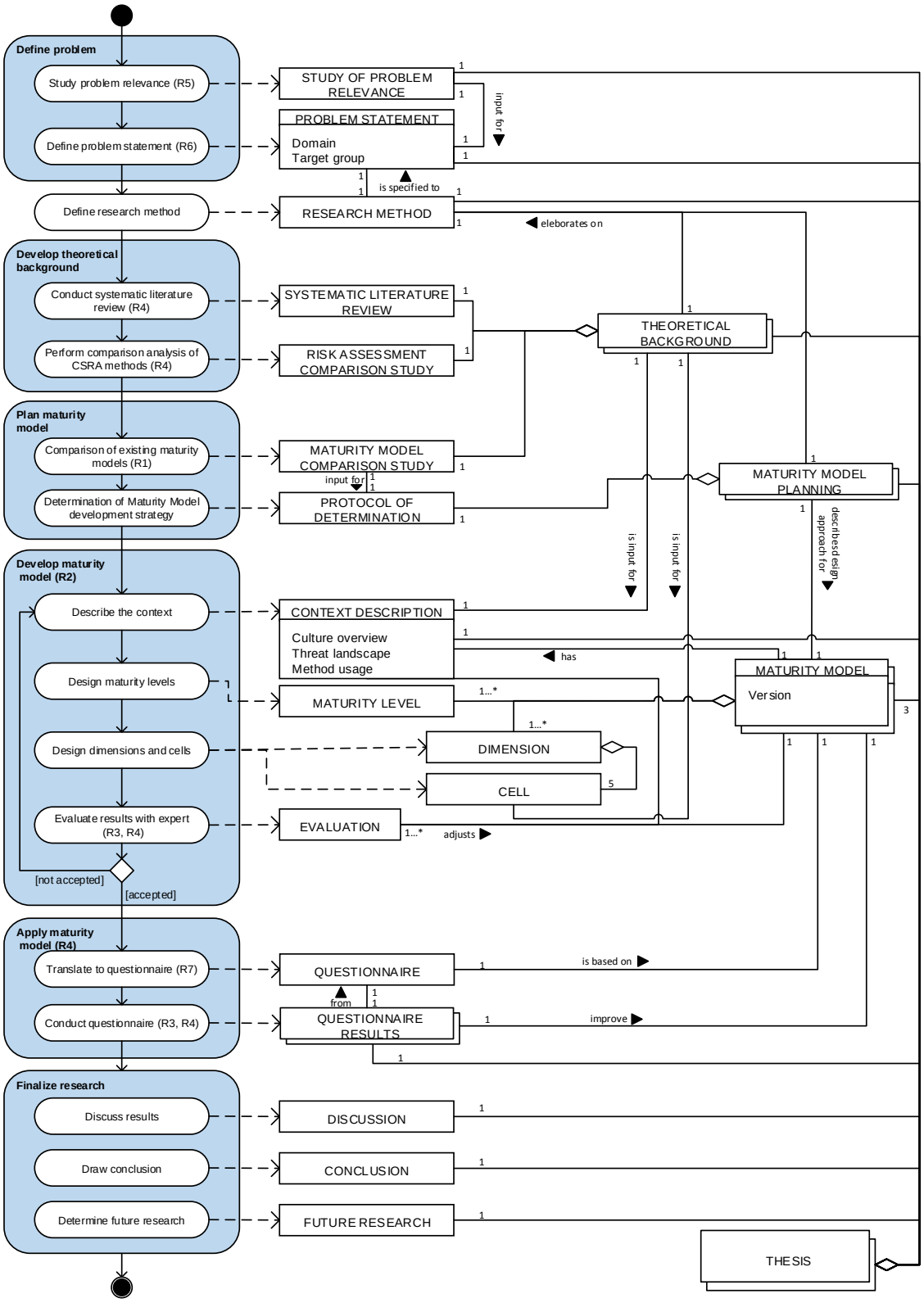


Figure 2: PDD of Research Method

The research method starts by defining the problem (chapter 1) and the research method (chapter 2). Subsequently the knowledge concerning the subject is broadened with a systematic literature research (chapter 3) and comparison analysis of CSRA methods (chapter 4). From here out a plan is formed to develop

the maturity model (chapter 5), which includes a maturity model comparison and the determination of the development strategy. After which an iterative process is started to develop the maturity model context (chapter 6) and the maturity model itself (chapter 7). This unfolds from the literature research already performed and iteratively increases by expert interviews. Of which the first set mainly fills the information gap and the second set is used to evaluate and adjust the results. After the completion of this process the maturity model is applied (chapter 8) due to a translation of the maturity model to a questionnaire, which is distributed among hospitals. Finally the research is finalized (chapter 9). All the chapters are combined in this thesis. An extensive overview of the activities in the method is given in the activity table (Table 1).

Activity	Sub Activity	Definition
Define problem	Study problem relevance	A literature research is conducted which results in the STUDY OF PROBLEM RELEVANCE.
	Define problem statement	The researcher defines the PROBLEM STATEMENT, which includes inter alia the Domain in which it will be used and the Target group(s) it is intended for.
Define Research Method		The RESEARCH METHOD used in this thesis is defined and certain aspects of it are explained into more detail.
Develop theoretical background	Conduct systematic literature review on CSRA	A literature review is conducted concerning CSRA using, a systematic method, resulting in found CSRA LITERATURE, which will be added into a QUALITATIVE LITERATURE SYNTHESIS.
	Conduct systematic literature review on threats	A literature review is conducted concerning the cyber security threats for hospitals, using a systematic method, resulting in found THREAT LITERATURE, which will be added into a QUALITATIVE LITERATURE SYNTHESIS.
Plan maturity model	Comparison of existing maturity models	The researcher compares relevant existing maturity models into a COMPARISON STUDY.
	Determination of development strategy	The researcher develops the design strategy for the maturity model in the PROTOCOL OF DETERMINATION
Develop maturity model	Describe the context	The context in which the MATURITY MODEL is used is described in the CONTEXT DESCRIPTION, containing a Culture overview, a Threat landscape and an overview of the Method usage.
	Design maturity levels	The number of MATURITY LEVELs is determined and the labels are defined to enable a basis for the MATURITY MODEL.
	Design dimensions and cells	DIMENSIONs and their CELLs are designed or redesigned and added to the MATURITY MODEL.
	Evaluate results with expert	A version of the MATURITY MODEL, or parts of it, are discussed in interviews with subject matter experts.
Evaluate results		An evaluation is performed on the MATURITY MODEL using expert interviews. The EVALUATION provides points on which to improve the MATURITY MODEL.
Apply maturity model	Translate to questionnaire	The MATURITY MODEL is translated into a QUESTIONNAIRE.
	Conduct questionnaire	The QUESTIONNAIRE is distributed among hospitals and results are collected and analyzed resulting in the QUESTIONNAIRE RESULTS.
Finalize research	Discuss results	The results of the research are discussed in the DISCUSSION.
	Draw conclusions	Conclusions are drawn from the research and added to the CONCLUSION.
	Determine future research	FUTURE RESEARCH OPTIONS are provided, on which could be continued in the future.

Table 1: Activity Table Maturity Model Development Method

An extensive overview of the deliverables and their definitions is given in the concept table (Table 2).

Concept	Description
STUDY OF PROBLEM RELEVANCE	A STUDY OF PROBLEM RELEVANCE is a literature review from which the actual demand for the maturity model is clearly stated (Becker et al., 2009).
PROBLEM STATEMENT	The PROBLEM STATEMENT consists of the determination of the domain and the target group. When a new maturity model is released by a third party this step might be skipped to evaluate an already existing maturity model with this new one (Becker et al., 2009).
RESEARCH METHOD	The RESEARCH METHOD describes the method used in this thesis and the principles it is based upon.
SYSTEMATIC LITERATURE REVIEW	The SYSTEMATIC LITERATURE REVIEW contains results of the literature review of a CSRA literature and hospital cyber threat search. The study is based on the PRISMA statement (Liberati et al., 2009) and search principles of Duff (1996).
RISK ASSESSMENT COMPARISON STUDY	The RISK ASSESMENT COMPARISON STUDY contains the results of in which different CSRA methods are analyzed in a structured way.
THEORETICAL BACKGROUND	The THEORETICAL BACKGROUND is the theory of the SYSTEMATIC LITERATURE and the RISK ASSESMENT COMPARISON STUDY combined. This adds to the need for a rigid research approach set up (Becker et al., 2009).
MATURITY MODEL COMPARISON STUDY	A MATURITY MODEL COMPARISON STUDY consists of a literature review of maturity models with similar domains and target groups (Becker et al., 2009).
PROTOCOL OF DETERMINATION	The PROTOCOL OF DETERMINATION explains the chosen design strategy. The most important basic strategies that can be chosen are: the NEW MODEL DESIGN, the ENHANCEMENT DESIGN, the COMBINATION DESIGN and the TRANSFER DESIGN (Becker et al., 2009).
MATURITY MODEL PLANNING	The MATURITY MODEL PLANNING describes the planning of the MATURITY MODEL, here for it combines the MATURITY MODEL COMPARISON STUDY and the PROTOCOL OF DETERMINATION, adding to the need for a rigid research approach (Becker et al., 2009).
CONTEXT DESCRIPTION	The CONTEXT DESCRIPTION describes the context in which a MATURITY MODEL is deployed. It includes an overview of the hospital culture, the threat landscape for hospitals concerning cyber threats and an overview of the methods used by hospitals.
MATURITY MODEL	A MATURITY MODEL is a model in which the maturity of a process can be mapped according to its maturity on certain subjects. It contains DIMENSIONS, MATURITY LEVELS and CELLS (De Bruin et al., 2005).
MATURITY LEVEL	MATURITY LEVELs determine the granularity of DIMENSIONs. Often four to six MATURITY LEVELS are used (De Bruin et al., 2005).
DIMENSION	DIMENSIONS are the categories which build up the different sub-domains of the MATURITY MODEL (De Bruin et al., 2005).
CELL	CELLs are on the intersection between MATURITY LEVELS and DIMENSIONS. In other words, each DIMENSION contains a CELL per MATURITY LEVEL. Each CELL contains cladistics concerning its position (De Bruin et al., 2005).
EVALUATION	In the EVALUATION the MATURITY MODEL and the CONTEXT DESCRIPTION are evaluated and adjustment components are proposed.
QUESTIONNAIRE	The QUESTIONNAIRE serves as a self-assessment tool to identify the overall maturity of a hospital's CSRA.
QUESTIONNAIRE RESULTS	The QUESTIONNAIRE RESULTS contains the results of the conducted QUESTIONNAIREs at hospitals.
DISCUSSION	The DISCUSSION consists of a discussion concerning the research and its limitations, as well the use of the main artifacts are discussed.
CONCLUSION	The CONCLUSION consists of the conclusion drawn from the research, providing an answer to the research question and its sub questions.
FUTURE RESEARCH	The FUTURE RESEARCH describes research gaps found in this research, who were out of scope of this research.
THESIS	The THESIS is the final document used to describe the research and its outcomes. It satisfies the requirement for a proper documentation the product in design science (Hevner et al., 2004).

Table 2: Concept Table Maturity Model Development Method

During this research four different approaches are used to (partly) answer the research questions: a systematic literature research, a comparison analysis, expert interviews and a survey. These approaches will be explained into more detail subsequently.

2.3 Systematic Literature Review Approach

To gain deeper knowledge of the domain of the subject a *systematic literature review* (SLR) will be conducted. Seale et al. (2004) argue that research should be conducted in a rigorous way, with and explicit methodology considering the design and execution. Furthermore as the research is in the information system field, which is an interdisciplinary field of research, a broad approach is needed in the literature research. In this broad approach literature from different disciplines and journals should be taken into account (Webster & Watson, 2009). The research boundaries and search terms are developed according to a predefined set of rules by Duff (1996), which describe the boundaries of the search term and the parameters used and the formulation. For the process of applying the found papers a method is provided based on the PRISMA statement, originally designed for clinical research comparison, this method describes a rigorous approach to compose a literature review in systematic way, describing the steps taken into detail.

To ensure a clear presentation of what was planned, done and found in a literature the PRISMA statement was developed, based on the QUOROM (QUality Of Reporting Of Meta-data) guidelines (Moher et al., 2009).

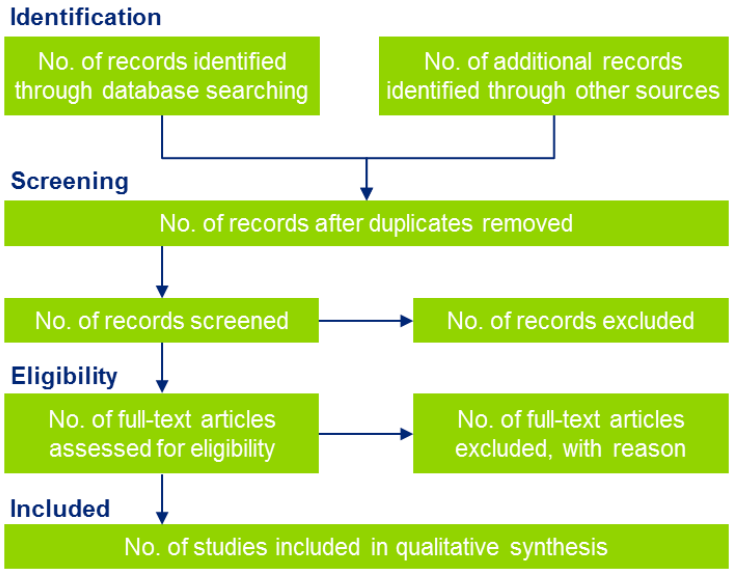


Figure 3: Flow of information through the different phases

The PRISMA statement consists of four stages: identification, screening, eligibility and the analysis of included papers (Figure 3) (Liberati et al., 2009). Important in the PRISMA statement is that the process should have a clear and repeatable protocol that is followed.

In the first stage, identification, information sources are identified. This occurs mostly by a systematic literature search, in which a search is conducted using a structured approach. Secondly in the screening stage the titles, abstracts and meta-data such as the quality of the source or the type of source, not published material are excluded. Based on the screening of the title and abstract, unfit or out of scope articles are excluded. In the third stage, the eligibility stage the research papers are fully read. Based on their content it is decided whether the article is included or not. In the final stage important information of the papers is collected. Such a structured approach to summarize the meta-data and important concepts is by compiling a concept matrix (Salipante, Notz, & Bigelow, 1982). In this approach important meta-data types or concept types are identified and entered in a table in which they are compared with the references of the articles read.

This analysis helps to put the found literature in context. The identified concepts are then described and methods and techniques considering these are presented.

2.4 Comparison Analysis

Outside the academic literature many CSRA methods exist. Therefore an additional literature research is done, which compares several CSRA methods. The comparison analysis serves two main goals. First an overview of widely used CSRA methods gives an improved understanding of CSRA in practice. Secondly the concepts these methods provide are useful as input for the Hospital CSRA Maturity Model, providing insight in different techniques and models used in CSRA.

Inclusion criteria are used to obtain CSRA methods. Exclusion criteria are then used to exclude less relevant methods, resulting in a set of CSRA methods relevant for hospitals. The methods compares both the risk models they use and any form of support they provide their user with. The support points on which the methods are compared are deducted from the literature research prior to the comparison.

2.5 Research at Dutch Hospitals

In the Netherlands 131 hospital units exist and 106 policlinics. Policlinics are external located subdivisions of hospitals. In Figure 4 a demographic overview is given of the hospital locations. These hospital locations and policlinics are organized in 87 organizations, of which eight are academic (RIVM, 2014). Of the remaining general hospitals 28 hospitals possess the predicate top clinical, which means they have a teaching responsibility and have research activities, although less than academic hospitals (STZ, 2014).

The research conducted at hospitals is twofold. First expert interviews are conducted to aid the development of the maturity model. When a maturity model is developed it is translated to a survey, which is distributed among the 87 hospital organizations.

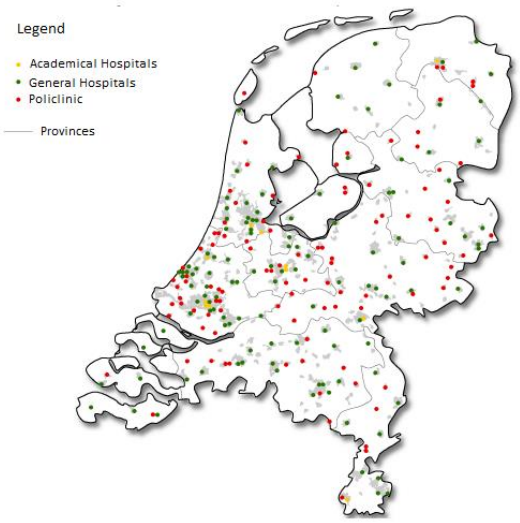


Figure 4: Dutch Hospital Locations in 2013 (RIVM, 2014)

2.5.1 Expert Interviews Approach

Expert interviews are performed to explore the subject to its fullest, as it is still a relatively lightly researched subject. These interviews are conducted with two groups of experts, i.e. cyber risk and security experts with experience in the hospital sector and cyber security and information security managers of hospitals. The first group has experience considering different hospitals and hospital types, the second group has more specific insights at hospitals themselves.

Interviews are conducted in a semi-structured form, using a protocol, which might change for each of the above mentioned targeted groups. Incrementally new subjects are added and discussed as these arise during previous interviews. These interviews are recorded and transcribed. To provide a scientific analysis of these interviews coding techniques are used. As the incremental improvement of the research is aided by a constant comparison coding technique (Bouije, 't Hart, & Hox, 2009), this technique is chosen. This is performed using computer-assisted qualitative data analysis (CAQDAS), using the software NVivo (QSR International, 2014).

2.5.2 Survey Approach

In the final stage the developed maturity model is used to gain information of the maturity level of CSRA at hospitals. In order to do this a self-assessment method in the form of a survey is distributed among hospitals in the Netherlands.

Categorical hospitals and independent treatment centers are disregarded from the survey since it might be difficult to translate the maturity model to these organizations. The survey is sent to all the 87 hospital in the

Netherlands in attempt to obtain a picture of the level of CSRA at Dutch hospitals. For hospitals who merged together by fusions or forms of cooperation the survey is send to their umbrella organization rather than the individual locations, as cyber security risk management might be regulated central within these organizations, skewing the outcomes.

The results from the survey provide an overview of the maturity of the CSRA of these hospitals and provide a benchmark for the hospitals. From these results it is possible to draw a general conclusion about the CSRA maturity of the hospitals and identify possibilities to improve this.

3 Systematic Literature Review

To obtain insight in the current state of research, concerning the subject, a systematic literature review (SLR) is performed. In this SLR two compounded search terms are used at three different electronic libraries. This results in a set of important sub processes, quality factors and a clarification of the research gap.

3.1 Systematic Literature Search Approach

To expand on the identification phase, Duff (1996) describes a method to conduct a systematic literature search in which five main stages are identified (Figure 5).

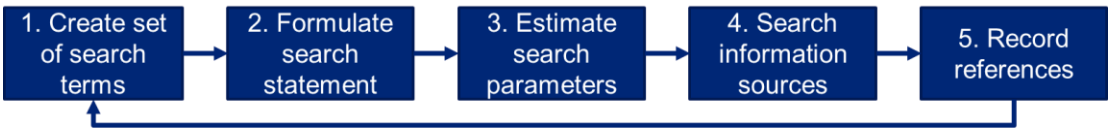


Figure 5: Model of Systematic Literature Search (Duff, 1996)

(1) The method starts by creating a set of search terms who give access to the domain related literature. These search terms should be broad enough to ensure a large enough amount of literature, but narrow enough to counter an information explosion. A possibility to facilitate this stage is to develop a conceptual taxonomy by positioning search terms in a framework of co-ordinate (synonymous), superordinate (broader) and subordinate (narrower) terms (Duff, 1996). In this research three literature domains are looked into: cyber risk assessment methods and cyber threats for hospitals.

(2) Next the logical search statement should be formulated. In case of computer-assisted literature searching this includes at least the proper use of Boolean operators and such conventions. In this aspect the best search strategies combine both natural language and thesaurus searching (Duff, 1996). For this research the search terms are formulated as such: ("information security" OR “cyber security”) AND (("risk assessment”) OR (" risk assessment method")); "cyber threat" AND (hospital OR "health care").

(3) The third stage involves setting the search parameters. Four of these parameters are used in most literature reviews: temporal, spatial, disciplinary and formal. Temporal parameters refer to the age of the research. In a fast moving field as information science old researches might be outdated and newer researches are generally more relevant. Spatial parameters refer to the area in which the research is conducted, since geographic or cultural differences might be a factor. Disciplinary parameters refer to the domain in which is sought. Since gaps between different fields of research might erode, important literature might be found outside the familiar domain. And finally formal parameters refer to the data sources that might be used such as journals, conference proceedings and books (Duff, 1996). Since types of cyber risks differ little all over the world and internet makes it possible to cyber attack from all over the world, no geographical parameters will be used. However since the field of cyber security is a fast developing one, a temporal constraint will be set. Only the literature of the last five years starting in 2009 will be embedded (the SLR is performed begin 2014). As for the high level view of this research a broad view is advised, no spatial constraints will be set. And finally since relative little literature is available in the field of cyber security, the only formal constraint will be the exclusion of thesis papers, as it is difficult to judge the quality of these.

(4) The fourth stage consists of searching for information sources. The main information source nowadays are web based libraries (Duff, 1996). To keep the research rigorous three proxies of search engines were included, with all a different focus. As the research is focused on hospitals, a search engine specified for the healthcare sector, PubMed, is included. To gain more computer science focused literature ACM is included. And finally Google Scholar is included with a general focus and this generally contains the most articles and may in some cases include papers of the other chosen databases, however these could not be accessed through the used proxy used for Google Scholar and are thus identified separate.

(5) Finally the search is conducted for research papers. The references of these papers are recorded and included in the bibliography (Duff, 1996).

In Figure 6 the overview of the search and exclusion process is provided. Four additional papers from other sources were added concerning SLR 2 to expand the given information concerning cyber threats. Exclusion of records was done based on the following arguments:

- The article was not available for free through the used proxies.
- The article consisted of a working paper or thesis.
- The content of the article was out of the scope of this research.

Theory of the included 36 research papers was included in a qualitative synthesis and quantitative synthesis (meta-data analysis). The results of the qualitative synthesis explain concepts which were found in this research and reveals research gaps. The articles from SLR 1 provide methods and techniques from a domain-independent perspective. The majority of articles from SLR 2, are domain-independent as well, however to apply to the criteria they all at least mention that the described threats and theories apply to hospitals or the health care sector in general.

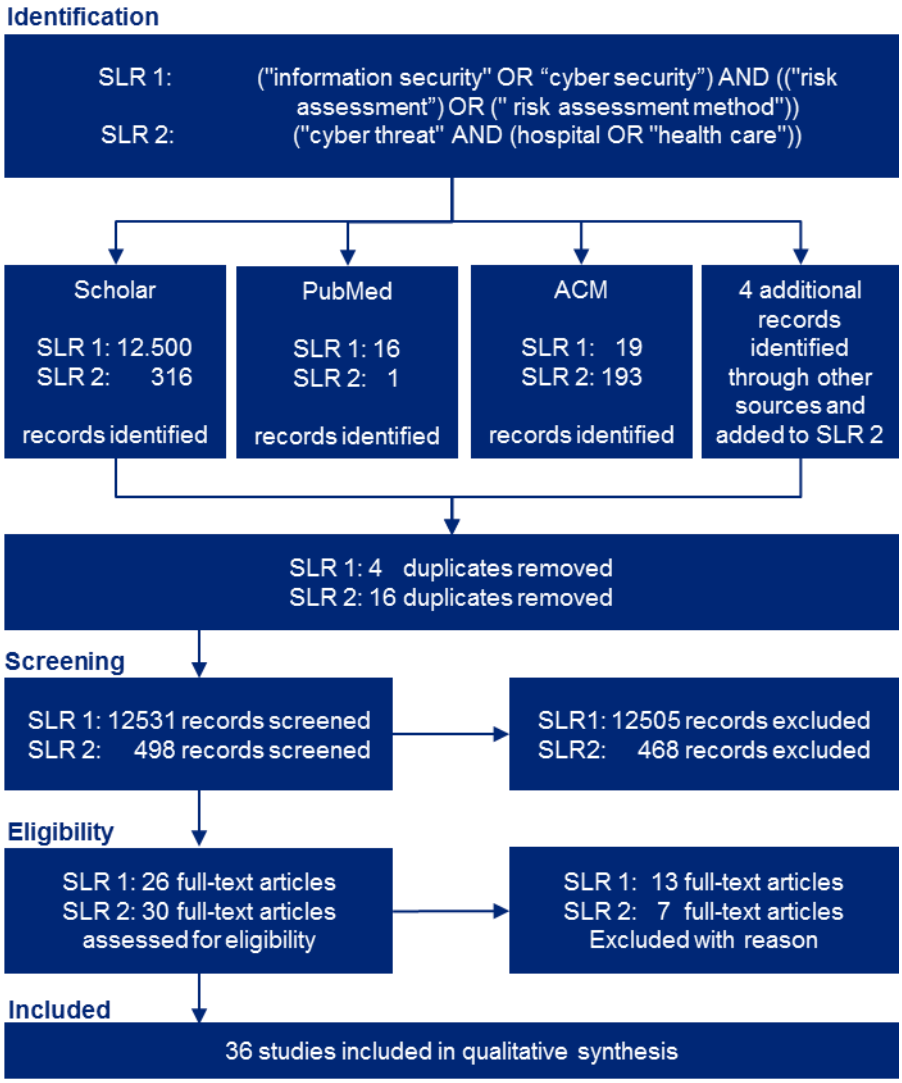


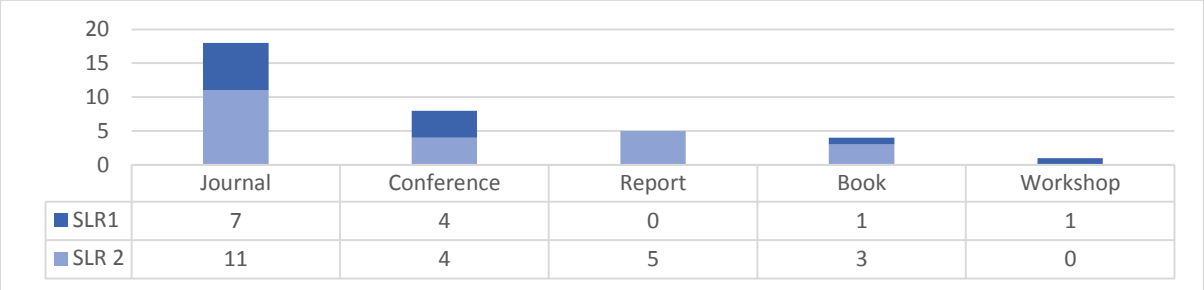
Figure 6: Literature Review Flow

3.2 Literature Analysis

Since all included literature was either based on qualitative research or design science research, as opposed to quantitative research, no meta-analysis was performed on research results of the included records. However

an analysis was performed on the meta-data of the articles themselves (i.e. the origin of the source and the type of source) and the concepts discussed in the included literature.

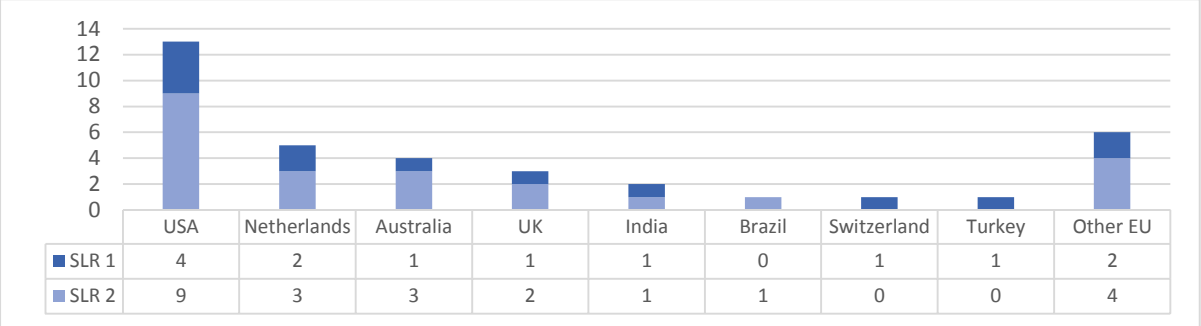
In Figure 7 the frequency of article types is given. Considering the type of the articles a clear majority of the articles consists of accepted academic sources, i.e. journals and conferences. As these sources barely provided an overview on macro threat trends four reports, containing threat landscapes, were added. The fifth report was found in the SLR through Google Scholar. To ensure the quality of the sources only grey literature from reliable governmental (n=4) and a non-profit organization (n=1) sources was used in the SLR. The books used consisted of bundled papers reviewed by the editor.



	Journal	Conference	Report	Book	Workshop
SLR1	7	4	0	1	1
SLR 2	11	4	5	3	0

Figure 7: Frequency of Included Articles per Type

In Figure 8 the origin of the research is given. More than a third of the research was American based. For SLR 1 the probability of bias is relatively low as the amount of American based literature is only slightly higher and the literature was mainly domain neutral. For SLR 2 care should be taken however that the American health care system may obtain specific extra threats as due to the political situation in the world America may be a more interesting target for cyber terrorists. Also the American health care system enables more possibilities to economic benefit from fraud opposed to for example the Dutch healthcare system, since the American system allows for identification through medical records itself.



	USA	Netherlands	Australia	UK	India	Brazil	Switzerland	Turkey	Other EU
SLR 1	4	2	1	1	1	0	1	1	2
SLR 2	9	3	3	2	1	1	0	0	4

Figure 8: Frequency of Included Articles per Country of Origin

In Appendix A, a concept matrix is provided, which maps the concepts discussed within the papers. In the qualitative synthesis the concepts will be discussed. However it is remarkable that event though SLR 2 was specifically healthcare focused, that even though the majority of papers mentioned that the threats they described applied for the healthcare sector as well as other sectors, only three researches were fully focused on cyber threats in the health care sector, of which two described risk assessment techniques and only one was focused on the threat landscape from an American point of view.

3.3 The Historical Development of Cyber Attacks

Many early cyber attacks and information disrupting operations were executed for the own amusement or challenge of the perpetrators. Websites would be defaced, servers would be taken down or simple computer viruses would be spread just to challenge other cyber professionals (Brockett et al., 2011). To illustrate this, one of the first computer viruses, the 'Brain', was written in 1986 by two brothers in Pakistan who worked in the software business and wanted to track piracy. Unfortunately the virus spread outside Pakistan as well and the world was introduced to the dark side of the internet (Singh, 2011). Since the internet has grown exponentially in size, new business models using the internet were developed and more business processes were conducted using the internet. Information systems became more and more common in organizations which in turn stored more and more data. Increasingly the systems and networks of organizations were connected to the internet, providing threat actors with more opportunities to attack these systems. Nowadays we are seeing a trends towards big data (Nationaal Cyber Security Centrum, 2013), the cloud (Harauz et al., 2009) and the Internet of Things (IoT): the connection of devices, including all kind of extra sensors, to the internet (Savola & Abie, 2013). Just as the increasing development of technological possibilities, cyber attacks have evolved over time (Brockett et al., 2011). Cyber attacks have become more complex and sophisticated, blending distinct attack types into more damaging combined forms and increasing in numbers. In the US alone the amount of reported incidents of malicious cyber activities have increased from 1415 in the year 2000 till 71661 in the year 2009 (Choo, 2011). In a report on cyber attacks the US homeland security illustrated how cyber attacks developed between 1980 and 2009 and became more sophisticated, while the needed knowledge for a cyber attack became lower due to the growing availability of tools as is illustrated in Figure 9. In the 1980s simple attack vectors were used such as the guessing of passwords, development of self-replicating codes, i.e. early viruses, and cracking of passwords by brute force. Nowadays threats have become more sophisticated with the use of tools that are able to scan networks and systems for vulnerabilities without being logged (stealth scanning), the use of botnets to distribute attacks from different servers, using staging servers to test the behavior of websites in efforts to find vulnerabilities, using sophisticated command and control (C2) media, i.e. using social media to attack its users pretending to be another user, and finally convergence between physical security and information security occurs. Between 2000 and 2009 also cases occurred in which wide spread cyber attacks were used in cyber warfare (Beggs, 2010). A full explanation of the threats is given in Appendix B

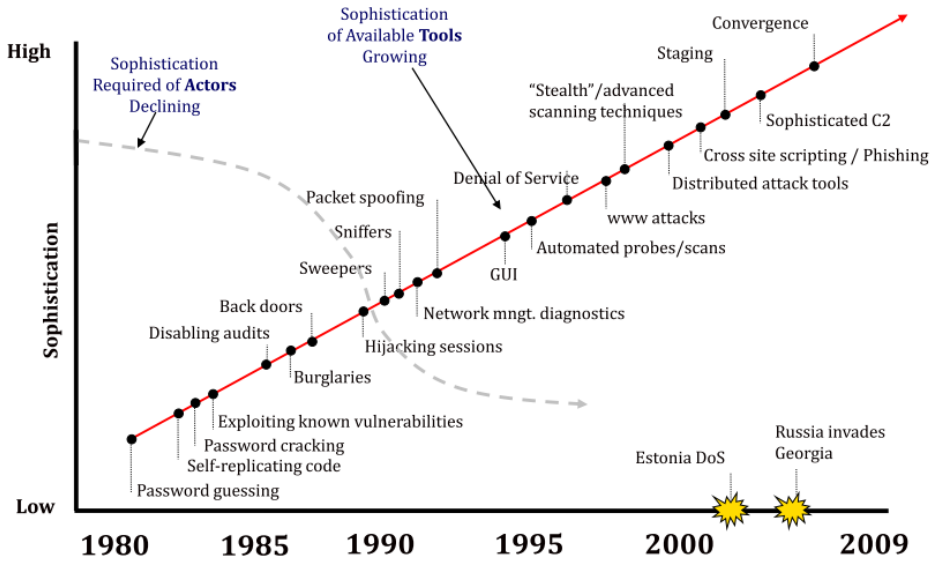


Figure 9: Cyber Threat Development (Beggs, 2010)

3.4 Threat Actors

To understand the different types of cyber threats that hospitals are exposed to, one must have a basic understanding of the different kind of threat actors. Each of these threat actors has its own motivation and legal actions and prosecution against these actors might prove difficult or even impossible since the use of internet has caused borders to be no issue anymore. Attacks can be executed from all over de world outside the jurisdiction of countries and their police (Brockett et al., 2011). The identified threat actors are listed in Table 3 and mapped against their main motivations.

		Motivation						
		Ideological	Economical	Military	Scientific	Demonstration of skills	Revenge	Accident
Threat Actor	State		x	x	x			
	Cyber terrorists	x						
	Cyber criminals		x					
	Script kiddies and Cyber Vandals					x		
	Hacktivists	x						
	Cyber researcher	x	x		x			
	Private organization		x					
	Social Engineers		x					
	Internal Actor	x	x				x	x
	No actor							x

Table 3: Threat Actor Motivation Matrix

3.4.1 Nation States

This group of threat actors consists of national states. Their main motives are gaining a military, economical or scientific advantage, which is mostly executed through cyber espionage (ENISA, 2013). Although an increased amount of cases have been reported in which cyber warfare methods are used, such as the Stuxnet virus, to target critical infrastructure (Nationaal Cyber Security Centrum, 2013). Usually the cyber attacks of these threat actors are highly knowledgeable. Also the motivation of this group is high.

3.4.2 Cyber Terrorists

Cyber terrorist are a sub group of terrorists, with the difference that they possess sophisticated hacking skills (Singh, 2011). Until now no major incidents performed by this group have been published. Authorities report some minor incidents have been documented, but most is kept confidential (ENISA, 2013). The motives of this group lay mainly in the disruption of critical infrastructure and gaining awareness for their case. The motivation of this threat actor is high due to ideological beliefs (Nationaal Cyber Security Centrum, 2013).

3.4.3 Cyber Criminals

Cyber criminals are professional operating actors with an economical driven motive. Their goal is to make money through malicious activities. The attacks of cyber criminals are becoming more sophisticated. Cyber criminals are sometimes working together in cyber crime organizations. However often there is now clear leader. The tasks are divided according to the skillsets of the individuals and most members only now each other online, e.g. through online forums (Europol, 2011). As well a large underground market exists in which cyber criminals offer their skills and malware in exchange for money. Sometimes constructions are found,

which can be described as cybercrime-as-a-service and malware-as-a-service (Nationaal Cyber Security Centrum, 2013).

3.4.4 Script Kiddies and Cyber Vandals

Script kiddies are usually teenage hackers. The internet gives them the freedom they want at their age and they are usually not aware or interested in the consequences of their actions (Singh, 2011). They have limited knowledge and use techniques and tools, which are developed by others. The increased easiness with which these tools can be used and are made available gives them increasingly better possibilities to break into systems (Nationaal Cyber Security Centrum, 2013). This threat actor typically uses DDoS and Injections attacks (ENISA, 2013). Cyber vandals are very closely related, although often a little more experienced and older.

3.4.5 Hacktivists

Hacktivists are ideologically motivated individuals, which can form dynamical groups, usually without a central organization structure. Their motivation consists of the defense of ideas, which are sometimes manifested. In some cases threat actors of other groups join hacktivists in order to co-protest or for other purposes such as the distribution of knowledge or tools (ENISA, 2013). A number of successful cyber attacks executed by hacktivists has proven they contain the skills for large and successful hacks (Nationaal Cyber Security Centrum, 2013).

3.4.6 Cyber Researcher

Cyber researchers are actors who search for vulnerabilities and/ or break into IT-surroundings to denounce the weak security. This group contains ideological researchers, parties who have economical motives and academic researchers. The skills of cyber researchers can vary and they may hire skills from other hackers and professionals. Next to the positive contributions towards awareness for the cyber security of these organizations, these activities and publicity which cyber researchers generate, may make these organizations (temporary) extra vulnerable, since others may profit of the damage done to the image of these organizations (Nationaal Cyber Security Centrum, 2013).

3.4.7 Private Organization

Private organizations, e.g. companies, can as organization be a threat. Through the internet a lot of public information can be gained about competitors and customers to improve their competitiveness. The difference between a legitimate analysis and profiling of organizations and people within the law and illegal espionage and privacy breaches are not always clear (Nationaal Cyber Security Centrum, 2013). Organizations may hire other threat actors to achieve their objectives. Depending on their sector, size and level of engagement in areas of technology and secrecy organizations may possess high level cyber capabilities (ENISA, 2013).

3.4.8 Social Engineers

Social engineers usually have low to medium technological hacking skills. They however possess a high amount of psychological knowledge, which they use in social engineering attacks. They are able to analyze and understand the psychology of the people they target as individual or as part of an organization. They are able to generate false trust relationships and may through this cause significant impact in areas such as identity theft, collection of confidential personal data, user credentials, etc. (ENISA, 2013).

3.4.9 Internal Actor

An internal actor, e.g. a (former) employee, a contractor or a business partner, has the trust of the organization, its employees, is aware of the infrastructure of the organization and often has increased access to its IT systems (Brockett et al., 2011). Because of these increased trust and access towards the organizations' system internal actors can access otherwise protected data and systems relative easily. The motives of internal actors may vary significantly, i.e. lax handling of security procedures, user error, selling inside information for money or even revenge (ENISA, 2013). Internal actors can be viewed as important cyber threat actors, who can do large amounts of damage (Nationaal Cyber Security Centrum, 2013). Many organizations however fail to detect the presence of such insider threats (Legg et al., 2013).

3.4.10 No actor

No actor is the threat actor which stands for all the unintentional malfunctions of IT systems and infrastructure that are not caused directly by any of the other actors, e.g. malfunctions in software which present themselves, external failure of infrastructure (e.g. a power outage) and natural disasters. In this thesis this actor is excluded from the scope.

3.5 Attack Vectors

To gain better insight against what hospitals need to protect themselves an overview of attack vectors, i.e. attack methods and types, is provided. These attacks exploit vulnerabilities. Vulnerabilities are openings in the system or organization through which an asset can be reached by using an attack vector. An extensive list of attack vectors and vulnerability trends is given in appendix B.

Cyber attacks can be divided into syntactic attacks, semantic attacks and combinations of these attacks, the blended attack. Syntactic attacks are cyber attacks that exploit technical vulnerabilities in software and hardware. Semantic attacks on the other hand exploit social vulnerabilities (Choo, 2011). The latter is often referred to as social engineering. In Figure 10 an overview is given from the different types of attacks used in information breaches in the USA 2010.

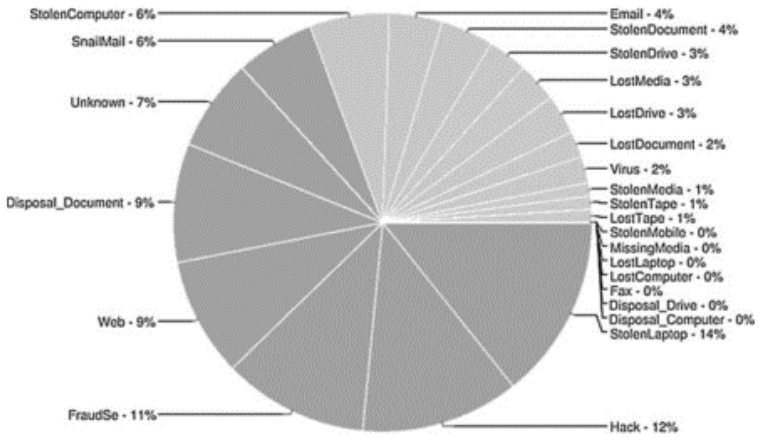


Figure 10: Information breech types in the USA 2010 (Choo, 2011)

3.5.1 Syntactic Attacks

Different types of syntactic attacks exist. One of the simplest forms of a syntactic attack is password guessing. Supervisory control and data systems for example often have simple standard passwords such as “administrator” (Nicholson et al., 2012). More advanced is the use of malware or code injections and even though malware and code injections are getting more sophisticated over the years, the knowledge needed to use these methods is decreasing (Beggs, 2010). Exploit kits give threat actors a relative easy to use weapon against their target. These exploit kits may contain malware which seek for vulnerabilities in a targets system. Often these vulnerabilities consists of buffer overflows (Saint-Claire, 2011). Buffer overflows or buffer overruns are anomalies in programs, while writing data into a buffer, the buffer’s boundary is overrun and adjacent memory is overwritten. This can result in errors, incorrect results, crashes and system security breaches (Princeton, 2014). Such a breach is then used to install malware on an IT system such as a Trojan, spyware or ransomware. Another tool often available in such an exploit kit are code injections such as Cross-Site Scripting (XSS), SQL injection (SQLi), Directory Traversal and Cross-Site Request Forgery (CSRF). These automated attack tools give hackers the position to launch large vulnerabilities in short time (ENISA, 2013). The Open Web Application Security Project (2013) gives a high level application security risk model (Figure 11), which gives a clear overview of cyber attacks executed on an organization’s applications.

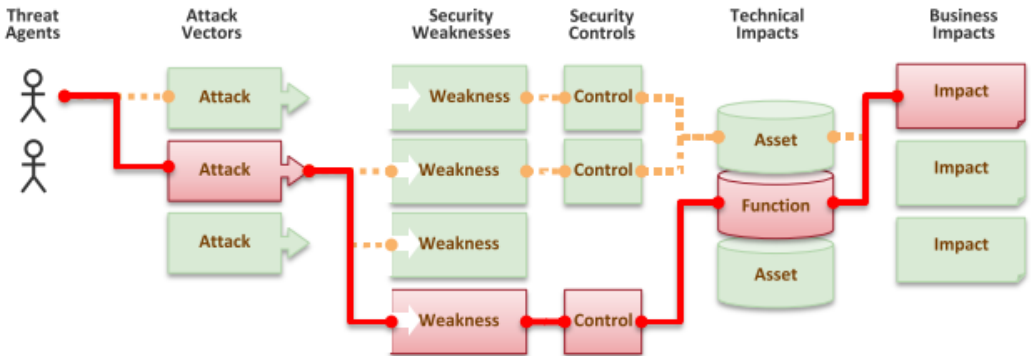


Figure 11: Application Security Risk Model (OWASP, 2013)

Toolkits often have options as well for malware to be downloaded in a drive-by-download approach. This refers to the immediately downloading of malware, viruses, Trojans or worms on a computer when a target visits a website. A direct search is done for weaknesses in the targets defense, which is then immediately exploited (ENISA, 2013).

Another form of cyber attacks is spreading malware as a virus. Most viruses in fact are some kind of worms (Saint-Claire, 2011), which is a type of malware which copies itself and sends itself to other potential targets through which is has access. Worms and other malware are often used to open backdoors on computers. If systems are compromised this provides opportunities for threat actors to exploit the security holes and seize sensitive data, disrupt services or incorporate them into botnets (Harries & Yellowlees, 2013). In the latter case computers are turned into zombies and often used to commit DDoS attacks (Nationaal Cyber Security Centrum, 2013) or encipher encryption (Kellermann, 2010). A very sophisticated form of such a worm is 'Conficker'. This worm operates with autonomy, permanently and independently scanning for new victims. And although most botnets use a central computer to direct their bots, which when found can be taken down relative easily to stop the botnet, the Conficker worm uses a peer-to-peer network structure to direct its bots, making it difficult to stop (Porras, 2009).

3.5.2 Semantic Attacks

The common denominator in semantic attacks is the exploitation of the human trust or naivety. One of the most used type of semantic attacks are phishing attacks. Phishing occurs when a threat actor sends emails to people which masquerade as a legitimate request from the organization whose letterhead and logo they copied. They ask the recipient to click on a link to supply information (Legg et al., 2013). In the case of spear phishing these attacks are directed at one person or group, based on their access rights and position in the organization, to gain access to this IT system. This group is kept as small as possible to stay under the radar (Nationaal Cyber Security Centrum, 2013). (Spear) phishing variations exist with mediums used such as calling, text messaging, chatting or face to face contact.

A variant on phishing, pharming, is a technique used to direct the unsuspecting victim to a malicious website where password and account numbers can be harvested in bulk numbers. Because often people use the same password for many sites this is likely to give the threat actor entrance to his e-mail, social media websites or web portal of his work environment (Legg et al., 2013). Also malware can be downloaded in a drive-by-download approach. A variation on this method, more aimed towards the hacking of the IT systems of organizations is the 'watering hole' method. First research is done towards the interests of a small group of chosen people. Then websites of their interest are build, hacked, or DNS servers are hacked to direct the targets towards malicious websites while thinking they visit their trusted website. These websites are then used to infect the computers of the visitors with malware (ENISA, 2013).

Many other examples of semantic attacks are possible. A USB stick may be found on the parking lot next to a company. The naïve employee wants to see what content it contains so it might be able to locate the owner of it, since it might be one of his colleagues. But when he plugs the USB stick into his computer the USB stick downloads malware on this computer, which allows the threat actor to get into the company's IT system.

Not all threats come from external threat actors though. It is argued that in fact an insider might even be most damaging to an organization (Legg et al., 2013). Removable mobile devices give for example disgruntled employees the opportunity to extract large amounts of sensitive data from an organization's IT system (Saint-Claire, 2011). Thumb sucking, using a UBS or thumb size device, and Pod-Slurping, using an iPod, are methods to steal gigabytes of data in a couple of minutes (Brockett et al., 2011). Organizations should be careful with the access employees have in their organization's IT systems.

3.6 Threat Awareness

A recurring element in articles in the SLR was the need to improve the resilience of organizations. Organizations should have appropriate measures in place to secure important information systems. The protective measures are available in the market, but many organizations do not research and manage their cyber threats appropriately in relation to the size of the threat they face (Harries & Yellowlees, 2013). Organizations should be aware of the speed with which sophisticated and organized perpetrators utilize emerging technologies to their benefit (Jamieson et al., 2009). Organizations with successful IS security mostly have the right funding, executive accountability and the right culture (employees must have a high regard for IT) (Jamieson et al., 2009). Increased awareness of the threat is a useful first step to improve this culture. For this improved awareness and better understanding of the cyber threats increased research and literature about information security is needed. Centralizing IS security management knowledge into an online crowd sourcing platform could help to improve this (Canabarro, 2013). Governments should furthermore support and subsidize IS security investment, develop IS security policies, certify compliance and periodic IS security audit firms that contain operations and information critical to a country (Hua & Bapna, 2013). In the worst case scenario, governments should not be afraid to punish the attackers, even if the threat actors are nation states. Prevention only against attacks might not prove a credible and effective enough strategy to defend critical information infrastructure of a country (Geers, 2010). Finally, although increased awareness and measures are severely needed, it is important to view current cyber attack scenarios for what they are. Often politicians use cyber doom scenarios to restrict freedom or privacy (Gregory & Glance, 2013). However Lawson (2013) argues that when these cyber doom scenarios are viewed in a historical context it correlates strongly with old fears of "technology-out-of-control" in Western societies and that most of these doom scenarios are in fact unrealistic. Therefore it is important to make a good assessment of the probability of occurrence of such an event.

3.7 Impact Modelling

For a better understanding of the possible risks an organization deals with the impact of these are assessed. For hospitals a cyber attack can have impact on several aspects, such as privacy, health and costs. Although health and especially privacy are difficult to measure concretely, costs on the other side, are relative easy to measure concretely. Brockett et al. (2011) discuss that the economical impact of a cyber attack can be measured by the negative return on the stockprice of a company. This approach however does not work well for hospitals, one can only view the impact afterwards and in the Netherlands hospitals are not listed on exchanges. Another approach they discuss are methods that attempt to model the attackers decisions as random variable or uncertain attributes of threats. This approach is usefull to gain insight in the costs of attacks (Brockett et al., 2011).

Hua & Bapna (2013) propose an impact methodology to calculate the needed investment in the cyber security of an organization by using the game theory as foundation. Their model is depicted in Table 4. In their model player 1, the attacker, is a threat actor, which has two possible strategies, attack and do not attack. The method of attack does not matter in this model, i.e. it can be a DDoS attack, a social engineering attack, the use of a buffer overflow, etcetera. Player two, the targeted organization has two strategies as well: invest more in information system (IS) security or do not invest more in IS security. The formulas on the left insight the cells are the formulas depicting the reward for the attacker. The formulas on the right depict the negative reward for the target organization.

The symbols stand for the following:

- P_1 and P_0: The respectively future and current change an IS breach occurs.
- M: The maximum instant damage in case of an IS breach.

- z_1 and z_0: The respectively future and current investment in IS security or the cost to take it down.
- λ: The discount rate, which represents the ratio of the attacker's gain to the investment made by the target in securing its systems.
- μ: The ratio of the attacker's gain to the maximum instant loss of the target. Not all of the losses of the target will gain benefit to the attacker.
- Q_1 and Q_0: The respectively future and current concerns about potential punishment.

An extra rule in the model is given that $z_1 > z_0$ and $P_1 < P_0$.

Player 1: Attacker	Player 2: Target organization	
	Invest More in IS Security	**Do Not Invest More in IS Security**
Attack	$[\mu P_1 M + \lambda z_1 - Q_1], [-(P_1 M + z_1)]$	$[\mu P_0 M + \lambda z_0 - Q_0], [-(P_0 M + z_0)]$
Do not attack	$[\lambda z_1], [-z_1]$	$[\lambda z_0], [-z_0]$

Table 4: A General-Sum IS security game (Hua & Bapna, 2013)

The formulas for the targeted organization work as follows:

- $[-(P_1 M + z_1)]$: If the attacker chooses the action "Attack" and the target chooses "Invest More" the target would lose $[P_1 M + z_1]$.
- $[-(P_0 M + z_0)]$: If on the other hand the attacker chooses "Attack" and the target chooses "Do not invest more", the target would lose $[P_0 M + z_0]$.
- $[-z_1]$: If the attack is not conducted, but an increased investment is made, the target will only pay the investment.
- $[-z_0]$: If the attack is not conducted and no increased investment is made, the target will only pay its invested IS security budget.

For the attacker the following applies: the attack will be successful if $[\mu P_1 M + \lambda z_1 - Q_1] > [-(P_1 M + z_1)]$.
Using this model for two types of attackers Hua & Bapna (2013) simulate a IS security game. In this game attacker type 1 is a hacker with economical motives and a low discount rate. Type 2 is a cyber terrorist with a high discount rate, since their gains are in disruption and not in gaining wealth. From this simulation they conclude that organizations with which are critical to a country's information infrastructure need to invest more in their IS security (Hua & Bapna, 2013). Parts of the critial information infrastructure of a country consists of the information systems hospitals work with, e.g. patient files (Luiijf, 2012). Therefore hospitals should invest more in their IS security than other organizations who do not contain systems which are part of the critical information infrastructure of a country.

Pau (2009) developed a impact methodology specific for the costs of distributed dinial of service (DDoS) and dinial of service (DoS) attacks. He argues that this type of attack is specifically prone for quantitative analysis. Related types of attacks, such as virusses, malware, identity theft and vulnerability exploring of systems all show a hugh impact as well, but estimations of such attacks are best interview based (Pau, 2009). In this methodology Pau (2009) assumes the target applies different time preferences to the IT assets in its portfolio. The time preference profiles express the urgency at which restoration of capabilities must be carried out in the light of a attack degrading suddenly specific assets in the portfolio. Time preference of discounting, in economics, pertains to how large a premium a user will place on usage nearer in time over more distant usage. These time preferences are used in a model, which calculates three different types of costs coming forth from a DDoS or DoS attack:

1. The short term costs needed to restore business and social capabilities and the costs of gaining or using the needed funds in in a short term.
2. The long term investments needed to rebuild and improve capabilities.
3. The value of the IT assets, decreased by the cyber attack, as the short and long term restoration measures are implemented.

With this model based on those three types of costs and the use of traditional analysis of tangible and intangible services it is possible, but still somewhat limited, to measure the impact of DDoS or DoS attacks on public and critical infrastructural organizations as it is better fit for purely commercial organizations (Pau, 2009).

Finally Thomas et al. (2013) propose an impact methodology to calculate the costs of an impact using an ex ante decision frame consistent with rational economic decision-making, and measures breach consequences via the assessed costs of recovery and restoration by all affected stakeholders. This methodology has a more holistic view than the previous mentioned methodologies, as it also takes into account the loss of privacy and legal consequences. The method, used for a single breach type, contains 8 steps:

Step 1: Define the scope of the breach episode in terms of affected people and organizations, and as well in time.
Step 2: Identify and list the primary evidence sources.
Step 3: Construct a timeline for historical events and possible future events.
Step 4: List Indicators of Impact using the primary sources from Step 2.
Step 5: Identify missing information, uncertainties, ambiguity, etc.
Step 6: Draw a branching activity model, similar to Figure 12.
Step 7: Estimate parameters for the cost function for each activity (e.g. time, resources, money).
Step 8: Estimate aggregate impact statistics with the use of a Monte Carlo simulation. (Thomas et al., 2013)

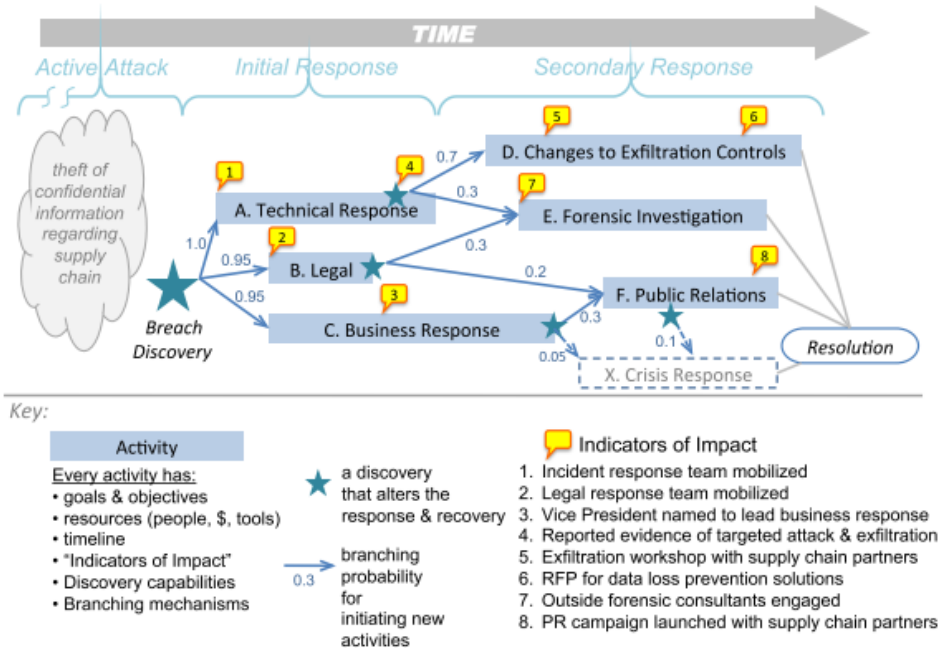


Figure 12: Example of a Simplified Branching Activity Model

The model in Figure 12 starts with the information breach, followed by the discovery of the attack. From this point first the routine activities are applied, such as a. technical response, b. legal response and c. business response. Secondly the less routine activities are applied, such as d. changes to exfiltration controls, e. forensic investigation, f. public relations and x. crisis response. Of all the activities the total costs (*C*) are calculated. A Monte Carlo analysis is used to gain insight in the probability (*P*) that an individual activity occurs. The total costs of the information breach (*I*) are calculated as following in the case of Figure 12:

$$I = Pa * Ca + Pb * Cb + Pc * Cc + Pd * Cd + Pe * Ce + Pf * Cf + Px * Cx$$

The activity costs are all multiplied with their probability of occurrence and those costs are then summed, resulting in the total cost of the information breach (Thomas et al., 2013). The holistic view of this methodology gives (i.e. not only view the economical side of the impact) seems a large advantage when compared with other impact methodologies. The main restriction of this methodology however is that it is best used when a breach already occurred, the types of breaches which might occur are difficult to predict and thus this methodology is difficult to use in a preventive information security risk assessment for hospitals, but could be useful as tool when a data breach occurs.

3.8 General Information Security Risk Assessment Methods

Not all cyber threats are evenly important. CSRA methods analyze which threats are around and which the organization is vulnerable to, and thus form a risk for the organization. For CSRA often information security risk assessment methods are used, since almost all cyber structures contain information or are information based. To protect this information the systems, networks and the infrastructure need to be protected as well. Information security risk assessment methods document, evaluate and manage specific risks that arise from the malfunction or abuse of information systems. They are geared towards information security and enable organizations to evaluate the threats and vulnerabilities to information systems (Köster et al., 2009). Threat analysis methods and threat catalogues are used to assist in this process (Ongsakorn et al., 2010). These risks are rated in importance by the dimensions probability and impact. Probability gives a measure to the change a threat occurs or a vulnerability is exploited. Impact measures the damage towards the organization when a threat occurs successfully (Atay & Masera, 2011). Once risks are identified and the importance is assessed evaluate the risks and decide which are most relevant to the organization and for which risks resources should be reserved first to be mitigated (Shedden et al, 2010).

Information security risk assessments however often have a generic approach. For a better in-depth documentation on how risks and constructs of these, such as threats, occur in certain sectors more domain-specific methods are needed (Köster et al., 2009). Furthermore Köster et al. (2009) detect several differences between traditional IT systems and security assessments that should be taken into account:

- The risk assessment should be performed from different abstraction levels (e.g. policy and on a technical level).
- The risk assessment should obtain collaboration of experts from other domains to include their specific knowledge to the risk assessment.
- The risk assessment should be reported to the company's management level and possibly even to governmental security organizations depending on the sector and types of risks identified.
- The risk assessment should include a way to validate the findings.

Furthermore in a comparison between the information security risk assessment methodologies COBRA, CORAS, CRAMM, OCTAVE, SOMAP and NIST Guide it shows that most information security risk assessments do only sparsely or not include the key attributes for risk assessment confidentiality, integrity and availability, which are the basic pillars of information security and of crucial importance for the cyber security of hospitals who often contain large amounts of confidential data (Pandey & Mustafa, 2012). Also Pandey & Mustafa (2012) plead for the use of tooling to streamline and improve the performance of the process.

Method	Evaluation scale	Impact evaluation	Risk evaluation
CRAMM	Qualitative	Based on open damage scenarios	Type 1
EBIOS	Qualitative	Based on security needs	Type 2
ISAMM	Quantitative	Based on monetary loss	Type 3
ISO 13335-2	Both	Based on the business harm	N/A
ISO 17799	Qualitative	Based on the business harm	N/A
ISO 27001	Qualitative	N/A	N/A
IT-Grundschutz	Qualitative	Based on open damage scenarios	Type 5
MEHARI	Qualitative	Based on fixed damage scenarios	Type 1
OCTAVE	Qualitative	Based on critical assets	Type 4
NIST SP 800-30	Qualitative	Based on open damage scenarios	Type 1
AS/NZS 4360	Both	Based on a balance between business harm and business advantages	Type 5
CORAS	Both	Based on open damage scenarios	Type 5

Table 5: Risk Assessment Evaluation (Zambon et al., 2010)

Zambon et al. (2010) provide a comparison between twelve risk assessment methods (Table 5). Of these ten were selected from the European Network and Information Security Agency survey for risk assessment

methods (ENISA, 2014). The non-English methods, methods who only were available in one country and insufficiently documented methods were not included in this comparison. The AS/NZS 4360 and CORAS were extra included. The methods were compared on three factors: the scale used to evaluate risks and risk factors, the proposed factors to evaluate the impact of risks and the structure how risks are evaluated. The evaluation scale determines if the risk level measures are quantitative, i.e. something which can be expressed in numbers (e.g. money) or qualitative, i.e. if something is only expressed with labels (e.g. low, medium, high). The quantitative measures are done on an interval or ratio scale, while the qualitative measures are done on an ordinal scale. The impact evaluation indicates which factors influence the impact of a security event, such as a threat, vulnerability or incident. As well it evaluates to which extent the method is constrained by these factors. Some methods only give general guidelines while others define a specific set of parameters. The final evaluated parameter, risk evaluation, investigates what determines the risk level of a security event and in which manner different properties are combined. Five profiles are defined and presented in Table 6 as formulas.

Type	Risk =	Likelihood Assessment *	Impact Assessment
Type 1::	*Risk (Threat, Asset) =*	*Likelihood (Threat) * Vulnerability (Threat, Asset) **	*Impact (Threat, Asset)*
Type 2::	*Risk (Threat, Asset, Needs) =*	*Vulnerability (Threat, Asset)**	*Impact (Threat, Needs)*
Type 3::	*Risk (Threat, Asset) = Annual Loss Expectancy (Threat, Asset) =*	*Probability (Threat, Asset) **	*Average Loss (Threat, Asset)*
Type 4::	*Risk (Threat, Critical Asset) =*	*Vulnerability (Critical Asset) **	*Impact (Threat, Critical Asset)*
Type 5::	*Risk (Incident, Asset) =*	*Likelihood (Incident) **	*Consequences (Incident, Asset)*

Table 6: Risk Model Types (Zambon et al., 2010).

The qualitative evaluation based risk assessment methods mentioned in Table 5 use a risk matrix for risk evaluation, in which risks are mapped from high to low on the dimensions consequence and likelihood. When it is difficult to quantify risks or subject matter experts find it difficult to give a score for likelihood and consequence than it should not be used as it provides no additional value (Levine, 2011). Another danger Levine (2011) warns about concerning risk matrices is the use of a three point qualitative scale (low, medium, high) as a minor change in likelihood and impact could push a risk from the right top corner of green into the lower red corner at position A or B (Figure 13, left). An alternative method to reduce risk evaluation bias is to use logarithmically scaled risk matrices (Figure 13, right), which uses an extra step between the risks. Also with the use of more quantified measurement scales this problem would not occur anymore and the accuracy of the evaluation would increase ((Pandey & Mustafa, 2012).

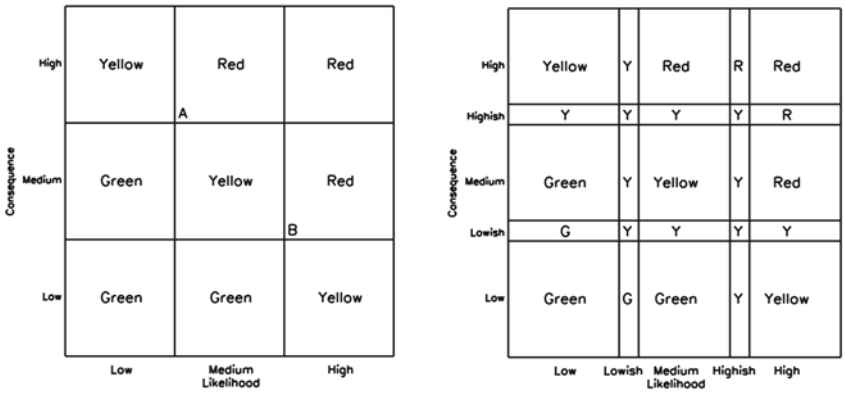


Figure 13: Demonstration of Dramatic Risk Transition (left) and solution (right) Levine (2011)

3.9 Specific Information Security Risk Assessment Methods

Often when risk assessment methods are more specified they are targeted at specific systems or network structures. An example of such a method in the healthcare sector is given by Savola & Abie (2013), who developed a context-aware Markov game theoretic model for security metrics risk impact assessment to measurably evaluate and validate the run-time adaptively of Internet of Things (IoT) security solutions. This model is developed for e-health applications in an IoT environment, e.g. in hospitals. In this approach a quantitative risk impact assessment is combined with decision making on protective measures. This approach gives an insight which allows the user to understand threats to the IoT system, assesses the potential risk of security threats and impacts and utilizes security metrics for measurable evaluation, validating the run-time adaptively of IoT security solutions (Savola & Abie, 2013).

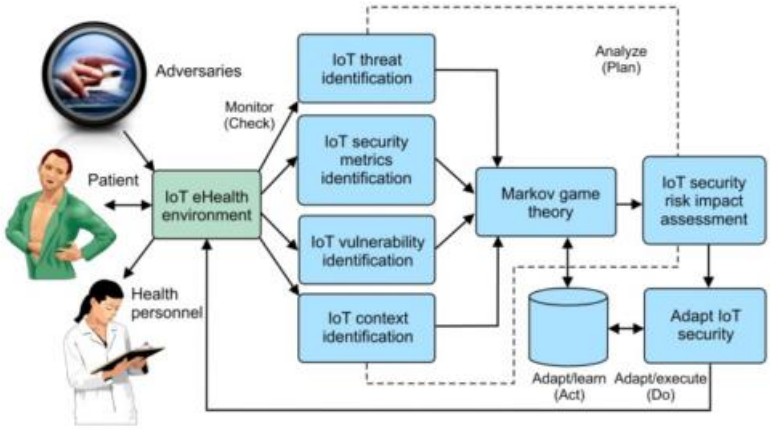


Figure 14: Framework for context-awareness and impact assessment (Savola & Abie, 2013)

In Figure 14 the framework for the model is given. Threat, security metrics, vulnerabilities and context are identified from the IoT e-health environment by modules of the system and input for the Markov game theory module. A Markov game theory simulation is then used to test the environment. From this simulates the potential risk impacts of threats to the security services, calculated using the metrics that measure the effectiveness of those services. If these risk impacts are low, no adjustments are needed, high risk impacts should be addressed accordingly to improve the IoT e-health environment (Savola & Abie, 2013).

No other healthcare or hospital related risk assessment method was found in the SLR. Several other technical risk assessment methods which had no health domain approach, but could also be used in hospitals were the ADversary VIew Security Evaluation (AD- VISE) method to quantitatively evaluate the strength of a system's security (Lemay et al., 2010), the telecommunications network risk assessment method with Bayesian networks (Szpyrka et al., 2013) and the real-time automated risk assessment in protected core networking method (Wrona & Hallingstad, 2010). A management level information security risk assessment for hospitals or hospitals was not found in this literature review.

3.10 Cyber Assets of Hospitals

As hospitals are complex organizations they contain a large amount of cyber assets in with different functions such as administrative and financial systems, electronic patient records and medical devices and systems. Harries & Yellowlees (2013) provide an example list of such cyber assets (Table 7).

Type of Cyber Asset	Applications
Administrative billing and financial	Administrative billing and financial Patient registration
	Billing
	General ledger
	Cost accounting systems
	Personnel and payroll
	Electronic materials management
Clinical	Computerized provider order entry for drugs, lab tests, procedures
	Electronic health record
	Picture archiving and communication systems
	Results reporting of laboratory and other tests
	Clinical decision support systems
	Prescription drug fulfillment, error-alert, transcriptions
	Electronic monitoring of patients in intensive care units
Infrastructure	Desktop, laptop, cart-based, and tablet computers
	Servers and networks
	Wireless networks
	Voice recognition systems for transcription, physician orders, medical records
	Bar-coding technology for drugs, medical devices, and inventory control
	Information security systems

Table 7: Examples of Cyber Assets of Hospitals (Harries & Yellowlees, 2013)

To prevent results gained from cyber security risk analyses to become obsolete by the time they are implemented, something that often happens in the fast changing cyber environment nowadays, Pak & Cannady (2009) suggest asset prioritization, in which important assets are given prioritized attention and resources to assess.

3.11 Conclusion Systematic Literature Review

In the literature overview several presentations of cyber risks are presented. However, they all have some corresponding elements which includes assets which are targeted by a threat, a probability these are threats will occur and a certain impact when the threats occur. Some risk models include another dimension: the vulnerability of assets. Vulnerabilities can be both of technical kind and of organizational kind. Vulnerabilities exist on different abstraction levels, such as program bugs, back doors, naive employees or non-segregated networks. Several trends were identified that increased the vulnerability of an organization: bring your own device, internet of things, connected SCADA systems, the increased use of the cloud, networks used as stepping stone, hotspots and an extended data collection (Appendix B).

Concerning the cyber assets of hospitals little information was extracted from the literature research. Cyber assets generally consist of data, software and hardware. The types of cyber assets that were found can also be divided into several domain groups: financial assets, employee assets, medical devices, patient assets and infrastructure.

Threats consists of a threat actor, with a certain motivation to target a cyber asset by using a certain attack vector, of which the change of succeeding can be measured the type of access to the organization's cyber assets, the prior knowledge of the organization and its weaknesses, the skill level and the strength of the motivation. The skill level needed by threat actors to attack successfully is however decreasing due to services and tools on the internet that provide malware, DDoS attacks or other cyber crime services. There are a wide variety of different motivations, the most important differences between these motivations for the cyber security are whether their motivation to attack is persistent or whether the threat actor will try its luck elsewhere when the basic cyber security is of a certain level. The utilized threats can syntactic, semantic or

both attack vectors, in which the first utilizes vulnerabilities in software and infrastructure, the latter utilizes the human or organizational weakness. An overview of the connection between these elements in relation to a threat profile is provided in **Error! Reference source not found.** in the process delivery notation of Van de Weerd & Brinkkemper (2009).

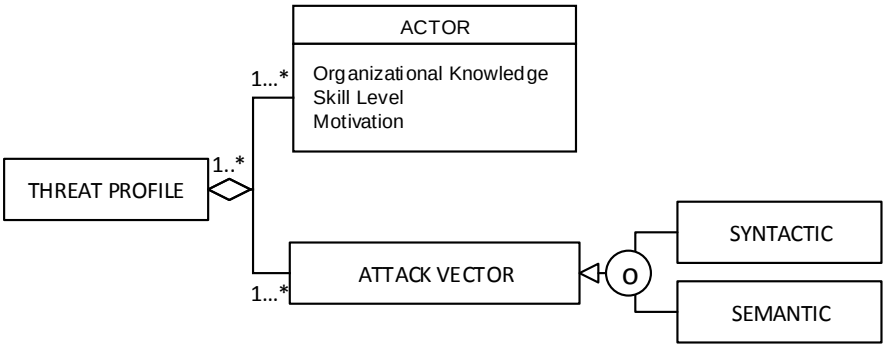


Figure 15: Cyber Threat Profile Structure

Little literature was found which gave an insight in the threats for hospitals specific, those who did focused on the American health-care sector. Most included literature described general cyber threats and mentioned hospitals as a possible target. A clear research gap is therefore identified considering the threat landscape for hospitals. Moreover considering information security risk assessment methods, only two articles were found which were focused specifically on the healthcare domain, of which one was focused on threat mapping of medical devices and one was focused on e-health applications. No research was found concerning the optimization of CSRA for hospitals, thus identifying another research gap.

In regard to CSRA based on the systematic literature research process and non-process elements are identified. The process elements are core elements of the CSRA process. These processes were identified as crucial and should return in each CSRA. These process elements were extracted by using the concept table (Appendix A), in which each of these elements were mentioned in most papers obtained in SLR 1 and often the papers in which certain process elements were mentioned had a scope more narrow than the whole risk assessment process. The identified process elements are:

- **Asset identification:** the identification of important cyber assets within the organization.
- **Asset valuation:** the ranking or differentiation between the important and less important assets.
- **Threat identification:** the identification of threat actors and associated threat vectors that pose a threat to the important assets of the organization.
- **Control identification:** the identification of taken en to be implemented security measures and policies.
- **Vulnerability identification:** the identification of weaknesses which can be abused in the people, processes or technology of the organization in order to let a threat attack an asset successfully.
- **Impact assessment:** an estimate of the impact a threat would have on the organization if it materializes.
- **Likelihood assessment:** an estimate of the likelihood a threat would materialize.
- **Risk evaluation:** The prioritization and discussion of the identified risks.

Finally during the literature research several other points were identified which were described as quality factors in CSRA. In literature these quality factors were the results of research in which was concluded those factors had positive influence on the quality of the risk assessment. This theory was explained elaborately in this chapter and some of the more general and important quality factors came up as well in the concept matrix (Appendix A) during the SLR (the first six listed) and rated most important as these were recurrent throughout the literature. Other quality factors were mentioned less often, but were included as the literature they were extracted from was rigid and provided valuable insight. The identified quality factors are:

- **Risk Model:** risk models largely decide the process as most sub-processes performed are in order to feed the risk model information. The risk model used will define how detailed the identified risks are and have large influence on the quality of the risks.
- **CIA triad:** confidentiality, integrity and accessibility (CIA) are important principles concerning information security. Therefore they are important for cyber security as well, since cybersecurity is described as a part of information security in which the assets are all electronically. The risk assessment method should incorporate these principles.
- **Use in networked environments:** in most organizations forms of hyperconnectivity occur, causing systems and devices to be connected to each other by networks. Therefore the method should be usable in networked environments.
- **Tools:** tools are able to simplify the process and provide support to the risk assessor on both administratively as well to support the analysis.
- **Validation:** the results of sub-processes and the final findings should be validated. Often this is done by interviewing stakeholders.
- **Quantification:** to gain a more nuanced and detailed insight in the severance of the risks, a form of quantification of the risks is advised. This also allows for more automation of the analysis by software based tools.
- **Different scope level abstraction:** the scope of the assessment should be on different abstraction levels, e.g. policy and technical.
- **Internal collaboration:** during the process collaboration with experts from different domains should be incorporated in the process, as important knowledge concerning the business processes lays with them.
- **Top management reporting:** To ensure optimal succession of the CSRA and improve the cyber security optimal the reporting of the results should be to the higher management level.
- **Government sharing:** In case the threats might have certain relevance for (parts of) the national security the threats should also be reported to the government.

Finally it can be concluded that the process elements are important parts of the CSRA as these are the building blocks of the process. The quality of these will make up the quality of the whole process. These will therefore be used as maturity dimensions in their form or a combined form. The quality factors are more complex to fit into this picture. These apply to all or some of the process elements, meaning that the right implementation of the quality factors improves the quality of a process element or elements. The maturity of the maturity dimensions will thus be build up based on the quality factors. In the next chapters a variety of methods will be used to expand the list of process elements and quality factors.

4 Cyber Security Risk Assessment Method Comparison Analysis

To gain extend the initial identified list of CSRA elements found in the SLR and increase insight in the way the initial elements are used in the CSRA a CSRA method comparison analysis is performed. In this analysis first an overview of CSRA as used in security standards for hospitals is provided to describe the minimal requirements of a CSRA method for hospitals and provide the inclusion requirement for the comparison. Then some methods are excluded from the analysis according to set exclusion criteria and finally the included methods will be compared on in advance set criteria, based on the elements found in the SLR.

4.1 Risk Assessment Standards for Hospitals

Internationally the ISO/IEC 27799 (BSI, 2008) is a widely accepted standard for information security. This standard is based on the ISO/IEC 27002 and translated to the health care domain. As cyber security is a section of information security and the ISO/IEC 27799 largely covers cyber security at hospitals. In the Netherlands the NEN 7510 standard exists, which is strongly based upon the ISO/IEC 27799. The Dutch healthcare inspection or in Dutch: Inspectie voor de Gezondheidszorg (IGZ) has taken this field standard in her oversight (IGZ, 2014), making the NEN 7510 the most important information security standard for Dutch hospitals to comply to. An important cornerstone of the ISO/IEC 27799 and the NEN 7510 is the use of a risk management approach. In the standards a high level overview of risk assessment elements ('detailed risk analysis') is provided as part of the risk management approach, as adopted from the ISO/IEC TR 13335-3. This process is given in yellow part of Figure 16: Risk Management Model ISO 27799 *(BSI, 2008)*Figure 16.

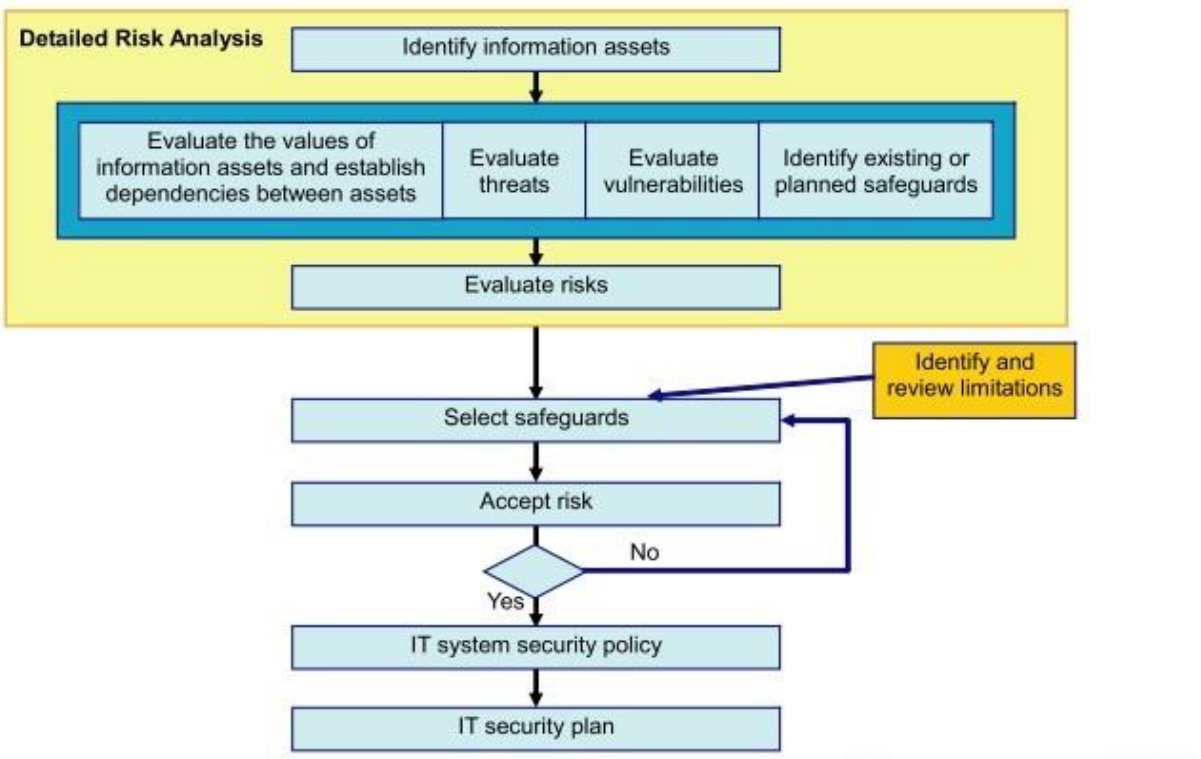


Figure 16: Risk Management Model ISO 27799 (BSI, 2008)

In Table 8 a mapping of the risk assessment process elements of the ISO 27799 against the earlier identified process elements from the SLR is provided. During the SLR a more detailed overview of the risk evaluation phase was found. Beside the risk evaluation phase the important process elements map fully.

Process Elements SLR	Process Elements ISO 27799
Asset identification	Identify information assets
Asset valuation	Evaluate the values of in information assets and establish dependencies between them
Threat identification	Evaluate threats
Control identification	Identify existing or planned safeguards
Vulnerability identification	Evaluate vulnerabilities
Impact assessment	Evaluate risks
Likelihood assessment	Evaluate risks
Risk evaluation	Evaluate risks

Table 8: Process Element Mapping from SLR with ISO 27799

4.1.1 Risk Management Model Structure

The risk assessment process overview described in the ISO/IEC 27799 (BSI, 2008) is merely a very high level one and cannot be viewed as a full methodology. The risk assessment process as viewed by the ISO/IEC 27799 is given in Figure 15. The part in yellow is described as the detailed risk analysis. This process identifies and weighs the risks an organization has to deal with. The risk analysis process consist of the following sub processes:

- **Identify information assets**: In this stage the assets that are important to and organization or the ones which will be analyzed in this RA cycle are identified.
- **Evaluate the values of in information assets and establish dependencies between them**: For this process it is of importance to identify the product owners, who have the resources and influence to decide on, and pay for, the needed security measures.
- **Evaluate threats:** The threats which the asset might face are identified to define the threat landscape of the asset.
- **Evaluate vulnerabilities:** The weaknesses in the assets that might be exploited need to be identified to determine where the security measures should focus on.
- **Identify existing and planned safeguards**: The existing and planned controls, which might mitigate possible risks need to be identified to get a clear view of the real threat and vulnerability of an asset.
- **Evaluate risks:** The risks are given a weight resembling their importance. Often this is done through estimating the impact a threat will have and the likelihood the threat will occur. Based on the risk analysis a list of risks is created, which are weighted for importance. In this sub process a decision is made which risks need to be mitigated and the order in which these will be addressed.

The second part of the risk management process consists of the development of a plan to mitigate the identified, analyzed and identified risks. Starting from the process: select safeguards, the sub-processes are out of the scope of this research. The sub-processes are explained as follows:

- **Select safeguards:** Mitigating measurements and techniques are decided upon.
- ***A*ccept risk:** The remaining risks which are too expensive to mitigate or do not need mitigation are accepted. This means that although management is aware of the risks, a clear reason was given not to implement mitigate these risks (further than already mitigated). When certain remaining risks are not accepted, new measures are decided upon for these risks.
- **IT system security policy:** The process has now led to a policy for the information security.
- **IT security plan:** Translated as information security plan. A planning is created to implement the information security policy, including it is decided upon measures.

To conclude, according to the ISO/IEC 27799 and the NEN 7510 risk assessments should at least include processes to identify information assets, evaluate the assets and dependencies, evaluate threats, evaluate vulnerabilities, identify existing safeguards and evaluate risks.

4.2 Selection Criteria

A long list of risk assessment methods for the comparison analysis is constructed first. These methods should at least contain the same building blocks as the risk assessment overview of the ISO 27799 in Figure 16, as this defines the minimum required risk assessment process for hospitals as set by the international standard (Inc-01). Furthermore the risk assessment methods should be able to assess cyber security risks specific or as a component of information security risk assessment (Inc-02) to comply with the research scope.

Inclusion criteria:

(Inc-01) The method is or contains core elements similar to the risk assessment overview of the detailed risk analysis (risk assessment) as presented in the ISO 27799 (Figure 16).
(Inc-02) The method is developed to be used to assess cyber security risks or at least supports this.

By combining the risk assessment method inventory list from ENISA (2014) together with RA methods found during the systematic literature review in the risk assessment method comparisons of Zambon et al. (2010) and Köster et al. (2009). The risk assessment methods from these sources are likely to cover a substantial part of all the internationally broadly used RA methods. All the found risk assessment methods who complied with the inclusion criteria were added in alphabetical order to the long list in Table 9.

Exclusion criteria were added to clearly state which methods from the long list are excluded from the comparison. When relevant documentation, explaining the method, was not available (for free), it was not possible to evaluate this method. The method needed to be either in Dutch or English to be readable to the researcher (Ex-01). To ensure that the methods included are rigid, the methods should be used in more than one country, i.e. a minimum of two countries (Ex-02). The Dutch A&K was omitted for this reason, since it is only used in the Netherlands. Furthermore, methods that do not take organizational contexts into account, but solely focus on the techniques of an information system or information system development are excluded, since a reason for the comparison analysis of the RA methods is to compare risk assessment methods on a management level (Ex-03). And finally, if the method has not been updated in the past 5 years it was excluded (Ex-04), to ensure the evaluated methods are up to date.

Exclusion criteria:

(Ex-01) The method lacks relevant, (freely) available documentation in English or Dutch.
(Ex-02) The method is not internationally used.
(Ex-03) The method does not take organizational context into consideration.
(Ex-04) The method has not been updated in the past 5 years or has been replaced.

Method	Reason of exclusion
AS/NZS 4360	(Ex-01), (Ex-04)
Austrian IT Security Handbook	(Ex-01)
CORAS	included
CRAMM	included
Dutch A&K	(Ex-02)
EBIOS 2010	included
ISAMM	(Ex-01)
ISF Methods	(Ex-01)
ISO/IEC 27005	included
IT-Grundschutz	(Ex-04)
Magerit	(Ex-01), (Ex-04)
Marion	(Ex-01), (Ex-04)
MEHARI 2010	included
Microsoft Threat Modeling Method	(Ex-01)
MIGRA	(Ex-01)
OCTAVE	included
RiskSafe Assessment	(Ex-01)
NIST SP800-30	(Ex-03)
Trike	included

Table 9: Long list of RA methods and their exclusion criteria

4.3 Comparison Analysis Approach

The CSRA method comparison analysis will compare the CSRA methods on several aspects to determine alternative approaches and deduct similar and strong concepts displayed in the methods, which will be used input for the maturity model. In this comparison analysis it will describe the background of each CSRA method, give an overview of the method structure, an overview of the risk models used and compare the methods on the support they give risk assessors in the execution of their task.

One of the findings of the SLR was the importance of the risk model for the risk assessment, since it largely define the structure of the risk assessment. Special attention will therefore be given at the risk model and analysis approaches, comparing the processes found in the SLR that are related to risk analysis and evaluation. First the overall risk model used in the method will be analyzed (R-1), since this model decides the structure that defines the method, providing an overview of the overall approach. The existence of other sub risk models depend on the overall risk model. These sub risk models are analyzed into more depth to obtain a better understanding of the overall risk model, based on important subjects mentioned in the literature research. Risk models may include models containing a decision process to define the asset importance (R-2), an impact assessment and dependency establishment to determine the damage for business processes if a threat attacks a system successfully (R-3), a likelihood assessment to determine what the changes are the impact will occur (R-4) and a risk evaluation approach to determine which risks which risks should be mitigated and whether some require prioritization (R-5).

Risk models:

(R-01) The overall risk model.
(R-02) The asset valuation.
(R-03) The impact assessment.
(R-04) The likelihood assessment.
(R-05) The evaluation of risks.

In the above analysis of the risk model a section of the important process elements discovered in the SLR are discussed. However some processes remain concerning the gathering of information for the risk assessment. Risk assessment methods provide different forms of methodological support to gather this information.

Therefor the support which is provided for threat identification (S-1) and vulnerability identification (S-2) are analyzed. Asset and control identification, also part of the information gathering process, were omitted in the comparison as these are more straight forward and less complex than threat and vulnerability discovering, thus providing no added value. Instead they will be discussed briefly during the general explanation of the risk assessments.

Next to process elements several quality factors were identified in the SLR. Of these quality factors Internal collaboration, top management reporting and government sharing are less methodical, more organizational factors, making them unfit for this comparison analysis. Concerning the others methods are able to support those quality factors in their method. Of these factors the quantification of risks and different scope abstraction will be included in an analysis considering the type of risk model used (S-3). Other quality factor is the inclusion of the CIA triad in the risk assessment method. The CSRA methods should include these, since all systems in hospitals are information based and the CIA triad is one of the cornerstones of information security and derived domains of it such as cyber security. Other concepts such as non-repudiation, accountability, authenticity and reliability are sometimes mentioned as well, however it can be argued that these are specified forms of the CIA triad (S-4). Medical devices and SCADA systems nowadays are often connected to networks, which makes assets more vulnerable to cyber-attacks due to interdependencies between the assets. Furthermore other systems within the hospital are increasingly connected to the main network. Being one of the identified quality factors the compared methods are therefore also analyzed on their possible use for networked environments (S-5). Furthermore, the risk assessment process requires cooperation between different actors and the result needs to be communicated to people with different backgrounds. Tools and a clear documentation of the process (S-6) help with this and aids a better internal process and as quality factor is included in the comparison. Finally, some sort of validation approach should be included to verify the results, resulting in the final quality factor for comparison (S-7).

Support comparison factors:

(S-01) Support for threat identification.
(S-02) Support for vulnerability identification.
(S-03) The type of risk models used in the method.
(S-04) The use of the confidentiality, integrity and principles in the method.
(S-05) The use of the method for networked environments.
(S-06) The tools and documentation help available.
(S-07) Validation approaches used by the method.

4.4 CORAS method

4.4.1 Background

CORAS is a model based security risk analysis method developed by SINTEF ICT for the EU-funded CORAS project IST-2000-25031. It provides a customized language for threat and risk modelling. It contains detailed guidelines to explain how the language should be used to model relevant information during the different stages of the security analysis. Often the Unified Modeling Language (UML) is used to model the analysis. For the documentation of intermediate results and the presentation of the conclusion special CORAS diagrams are used, based on UML. The CORAS method contains a computerized tool to support the documenting, maintaining and reporting of analysis results (SINTEF ICT, 2014). Figure 17 presents an overview of the basic building blocks of CORAS (Dahl, Hogganvik & Stolen, 2007).

Figure 17: CORAS Incident Scenario Building Blocks (Dahl, Hogganvik & Stolen, 2007)

4.4.2 Structure

The CORAS method contains a security risk analysis in eight steps (Figure 18), which are:

- **Step 1:** The initial preparations for the risk analysis. In this stage the main objective is to gain a basic idea of the size and target of the analysis, such that the necessary preparations for the actual risk analysis tasks.
- **Step 2:** The introductory meeting is held with the customer for which the analysis is conducted. In this meeting the overall goals and the target of the analysis are discussed with the customer. Furthermore the scope of the analysis is set and the analysis is planned.
- **Step 3:** A common understanding of the target of analysis, including the focus, scope and main assets is ensured in this step. The analysis team presents their understanding of what they learned of the given documentation and the first meeting. Based on interaction with the customer the main assets and a high-level analysis of the major threat scenarios, vulnerabilities and enterprise level risks are analyzed. The deliverable of this step is a detailed understanding of the target description and the objectives of the analysis.
- **Step 4:** The background documentation for the rest of the analysis is ensured, including the target, scope and focus. A more refined description of the target is analyzed. In this stage the analyst describes the target using a formal or semi-formal notation such as the UML. This step includes the risk evaluation criteria for each asset and concludes the context establishment.
- **Step 5:** The risks are identified using a structured brainstorm. This is a step-by-step walkthrough of the target of analysis and is carried out as a workshop. Participants with different backgrounds are included in this workshop to give enable different perspectives and identify more and other risk than a homogeneous group or individuals would have come up with. This step involves a systematic identification of threats, threat scenario's, unwanted incidents and vulnerabilities concerning the identified assets.
- **Step 6:** The risk level of the risks, represented by unwanted incidents, are determined. These unwanted incidents were documented in threat diagrams in step and are used as the basis for the risk estimation. This step is conducted as a brainstorm, involving personnel with different backgrounds and is used to estimate the likelihoods and consequences of the unwanted incidents. The combination of these values are the risk level of the risk.

- **Step 7:** An evaluation is performed to decide whether the identified risks are acceptable and which should be further evaluated. This includes the judgment whether a risk is acceptable and involves the estimation and evaluation of the risks for indirect assets.
- **Step 8:** The identification and analysis of treatments. Found risks that are labeled unacceptable are evaluated to find means to reduce them. The found treatment should contribute to reducing the likelihood and/or consequence of an unwanted incident. The cost-benefit aspect of this analysis is important.

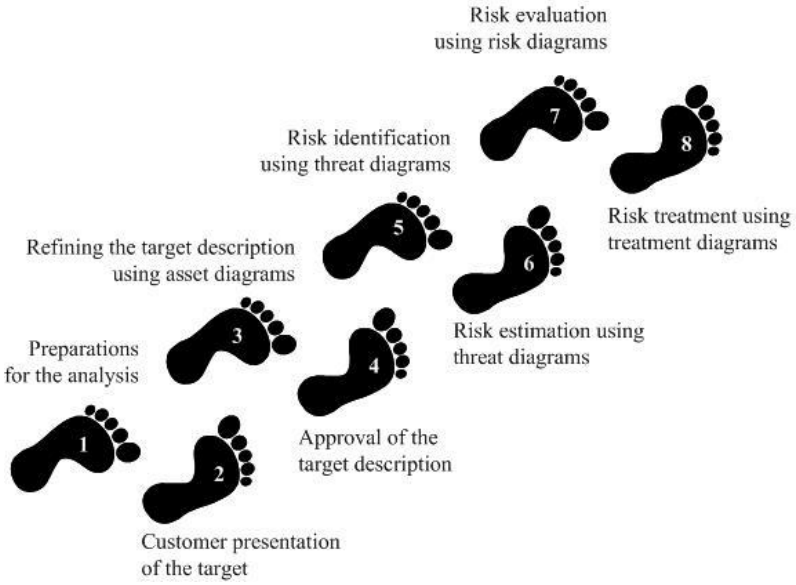


Figure 18: CORAS Method (SINTEF ICT, 2014)

4.4.3 Risk Models

(R-01) The CORAS method uses mainly qualitative models, which can be quantified. The risk model of the CORAS method is valued as the importance of a risk is based on the consequences which an incident can have on an asset and the likelihood this occurs.

(R-02) The asset valuation is done based on an ordinal scale ranking to determine which assets are most important and should be assessed first.

(R-03) The impact is modelled by an ordinal scale from 1-5, which are described as insignificant, minor, moderate, major and catastrophic. Quantitative values can be attached to the impact values, based on the domain (e.g. amount of health records compromised).

(R-04) The likelihood is modelled by an ordinal scale from 1-5 as well, with the values rare, unlikely, possible, likely, certain. Quantitative values can be attached to the likelihood as well, based on the needs in the domain (e.g. daily, weekly, yearly, etc.).

(R-05) The risk prioritization is done in the form of an impact x likelihood matrix. In this matrix all the low risks are accepted and all the moderate and high risks are evaluated in-depth.

4.4.4 Support

(S-01) The way in which threats are identified is based on the opinions of the people which are in the brainstorm sessions. The quality of the threats largely depends on the gathering of the right people and their knowledge.

(S-02) Similar as with the threats, vulnerabilities are identified is based on the opinions of the people which are in the brainstorm sessions. The quality of the vulnerabilities largely depends on the gathering of the right people and their knowledge.

(S-03) The quality of the risk models used start basic, but can be further developed in-depth, with quantification, which increases the accuracy of the model. It is however important to test the models that will

be used.

(S-04) The CORAS method does not specifically mentions the CIA principles. More emphasis on these principles could help in better identifying threats and classifying assets.

(S-05) Although in normal use the interaction between systems is not taken into account specifically, the documentation however provides options to use it in this way.

(S-06) The UML based modeling documentation is a very strong tool for communicating the threat scenarios and solutions. It provides a clear overview of the landscape and the mitigation approaches.

(S-07) Validation is done based on interviews and feedback towards the responsible people. The quality of this validation depends on the knowledge of the people informed in the RA process.

4.5 CRAMM

4.5.1 Background

CRAMM (CCTA Risk Analysis and Management Method), was developed by the British government organization the Central Communication and Telecommunication Agency (CCTA), which is renamed to the Office of Government Commerce (OGC). The method was first released in 1985 (ENISA, 2014) and although in its whole it is a risk management method, it contains a risk assessment method which is documented well. CRAMM is fully compliant with the ISO/IEC-27001.

4.5.2 Structure

CRAMM consists of three stages, which in turn contain several steps.

- **Stage 1:** Evaluate the scope of the security problem.
  - **Step 1:** Prepare the project framework and scope. And identify the assets which will be assessed.
  - **Step 2:** Assets are evaluated for their worth. Next to financial value, the impact of personal safety, political embarrassment, infringement of privacy, disruption of activities, failure to meet legal obligations and commercial confidentiality. These values are contained by interviews with the asset owners.
  - **Step 3:** Review the data results, to check if they correspondent to reality. When the wrong people have been interviewed the image might be skewed.
- **Stage 2:** The risk evaluation.
  - **Step 1:** The relationships between threats and assets are identified. The method contains 31 generic threats that cover all possible threats from accidents to malicious misconduct.
  - **Step 2:** The likelihood of threats occurring are calculated. This takes into account whether a threat has happened in the past and who is interested in the asset. For the vulnerability it is calculated if it makes the threat more likely to happen.
  - **Step 3:** The security requirement is calculated, taking into account the ratings of the threats, vulnerabilities and assets. The ratings have a value from one to five and give a security requirement for every dimension.
  - **Step 4:** The security requirement values are reviewed to prevent the measures of errors. Which might lead to unnecessary security measures or a lack of needed protection for assets.
- **Stage 3:** The selection of appropriate countermeasures.
  - **Step 1:** Countermeasures required by the analysis are identified from a list of 53 countermeasure groups. These are categorized according to strength (1-5), security aspect (hardware, software, communications, procedural, physical, personnel, environmental and cost).
  - **Step 2:** The required countermeasures are compared to the ones already in place, to find how many new countermeasures are needed.
  - **Step 3:** The countermeasures are confirmed with the management (SANS, 2002).

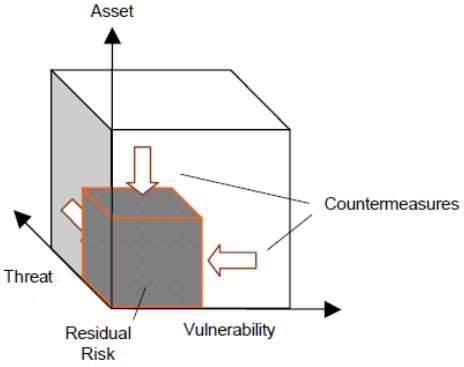


Figure 19: CRAMM Risk Model (SANS, 2002)

4.5.3 Risk Model

(R-01) CRAMM describes risk analysis as:*" the identification and assessment of the levels of risks calculated form the known values of assets and the levels of threats to, and vulnerabilities of, those assets*" (SANS, 2002). This defines risk as a product of threat, vulnerability and asset values: Risk = Impact of Threat on Asset x Likelihood of Threat x Vulnerability of Asset towards Threat. Countermeasures assigned to the parameters can reduce the risk levels, as is shown in Figure 19.

(R-02) Asset values are constructed based on CIA impacts on assets and the impacts derived from these. This can be in quantitative measures (often measured in money) or be recalculated to a scale from 1 to 10, 10 being the highest impact.

(R-03) The vulnerability can be calculated by presenting a percentage of succession that a certain threat will attack the asset successfully. These percentages can then be calculated back into a five level ordinal scale consisting of very low, low, moderate, high and very high.

(R-04) The threat occurrence likelihood is calculated qualitative on an ordinal scale from very low, low, moderate, high, very high. A tool is provided which can calculate these levels based on the answers of structured surveys, however for domain specific assessments this might not work well.

(R-05) The risk prioritization is done by ranking risk levels for every asset group against the threats it is vulnerable to. These values are divided into a scale from one to seven, in which seven represents the most important risk that needs immediate attention. The controls which will be selected are given a value, between one and five, in which they protect the assets and countering the likelihood of threats, the vulnerabilities and impact, as modelled in Figure 19.

4.5.4 Support

(S-01) The identification of threats is mainly based on the opinion of interviewees. The same counts for the impact valuation, of which the valuation model might also provide a bias as different actors might do different amounts of damage to systems and this viewpoint is not taken into account.

(S-02) The identification of vulnerabilities is mainly based on the opinion of interviewees as well. This makes the quality dependent on the interviewees their opinion.

(S-03) The risk models used in this method are based on a concept that in theory works well, but in practice needs an experienced risk assessor or improved domain specifics to work properly.

(S-04) The CIA principles are used to give a complete picture of possible impacts, thereby helping to refine these.

(S-05) The method could be used for networked environments, although interactions in the environment are not accounted for as the threat scenarios are done per asset.

(S-06) The documentation of the process and scenarios can be done in the tool, but is in essential basic and the quality will differ depending on the risk assessor.

(S-07) Validation is mainly opinion based. It is important in this process that the interviewees are chosen rightly and are skilled.

4.6 EBIOS 2010 Method

4.6.1 Background

The EBIOS (Expression of Needs and Identification of Security Objectives) method was founded in 1995 by the L'Agence nationale de la sécurité des systèmes d'information (ANSSI) and is since further developed. The method is developed to asses and treat risks related to information system security and form a tool to communicate with partners within the organization. The EBOIS method is modular and consistent with the international standers ISO/IEC-31000, ISO/IEC-27001 and ISO/IEC-27005 (ANSSI, 2014).

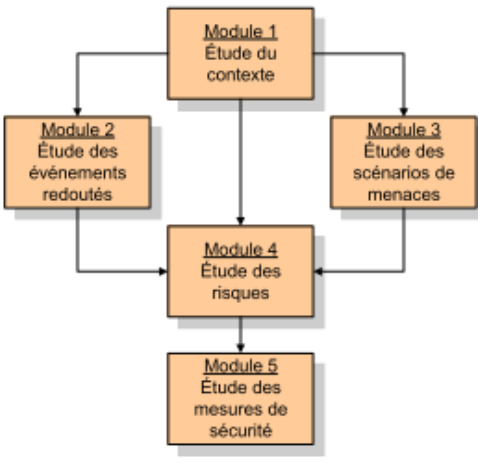


Figure 20: OBOIS Method Overview (ANSSI, 2014)

4.6.2 Structure

The OBIOS method consists of 5 modules, shown in Figure 20:

- **Module 1:** Define the context. This includes a definition of the scope, defining the metrics used in the risk assessment and defining the most important assets and the infrastructure they use.
- **Module 2:** Review undesirable events. In this module the security needs of the important assets are identified and assessed based on availability, integrity and confidentially. The impacts when these security needs are violated are assessed based on the impact they would have (e.g. on financial, legal and safety). Sources that form such a violation of the security needs are identified (e.g. human, environmental, internal, external, accidental and deliberate).
- **Module 3:** Study the threat scenarios. In this module threat scenarios are developed and weighted on the possibility of occurrence. For this possible threats are compared to usable vulnerabilities.
- **Module 4:** Risk evaluation. In this module the risks are evaluated and the most risks, based on probability of occurrence and impact (measured on qualitative scales) are ranked on importance.
- **Module 5:** Decide on the security measures. In this module the risks are treated. The needed security measures are specified and a validation plan for the treatment of risks and residual risks (ANSSI, 2010).

4.6.3 Risk Models

(R-01) The EBIOS method views risk as the product of the threat impact and vulnerability of the asset.
(R-02) The asset valuation is done by identifying the needed security for assets based on the CIA principles. The security gaps are identified, using the ISO/IEC-27002 as a baseline for optimal security, other baselines could be used as well.
(R-03) The impact is then measured on an ordinal scale from one to four standing for negligible, limited, important and critical.
(R-04) The likelihood of threat is measured on an ordinal scale with the values minimal, significant, strong and maximal.
(R-05) Risk prioritizing is done with an impact x likelihood matrix. The “important x strong” risks and higher are valued as intolerable. Other risks are either significant or negligible. The control prioritizing is done based on the risks that are valued intolerable and significant and the amount of money they cost.

4.6.4 Support

(S-01) The EBIOS method is strongly dependent on previously defined security measures. The threats are defined as a breach of confidentiality, integrity or accessibility of the data. This offers a very structured approach. Although this has large advantages over approaches which do not start from the CIA triad, the likelihood estimation gets more complicated in this approach, since no practical threat scenarios exist.
(S-02) The vulnerabilities are defined as the lack of certain controls, which are stated in the base line (e.g. the ISO/IEC 27002). This makes is easy to identify needed security controls, but depends heavily on the quality of the chosen security baseline.
(S-03) The quality of the risk model is as good as the standard chosen. The default standard is the ISO/IEC 27002. It might be preferable to have a domain specific standard although this might not exist, be too complex or too simple. Also some possible bias on the opinion on the impact size and likelihood of threats exist, although the amount of bias is lower compared to other methods. The quality of this assessment therefore stays dependent on the knowledge of the interviewees.
(S-04) The CIA principles are used to value the security needs of the assets, helping to complete the picture.
(S-05) The EBIOS method is also usable in networked environments. The strength of the method in these cases will depend on the used security baseline and the domain in which it is used.

(S-06) The documentation of the process and scenarios is very extensive and clear, with extensive lists of security needs and prioritizations of security control tables.
(S-07) The validation is partly included into the process as the chosen information security standard. The compliance to this standard gives a clear view on the quality of the assessment. The main bias exists in the choice for the standard and the likelihood and impact assessment. Although this method seems to have a more structured approach than most competitors and a relative low bias.

4.7 ISO/IEC-27005

4.7.1 Background

The ISO/IEC 27005 consists of guidelines for information security risk management, specifically supporting requirements for an information security management system as defined by the ISO/IEC 27001 (ISO, 2014).

The whole risk management process is given in Figure 21 starts with a context establishment. In this stage the basic criteria for information security risk management, the scope and boundaries are set. An appropriate organization operating the information security risk management is established.

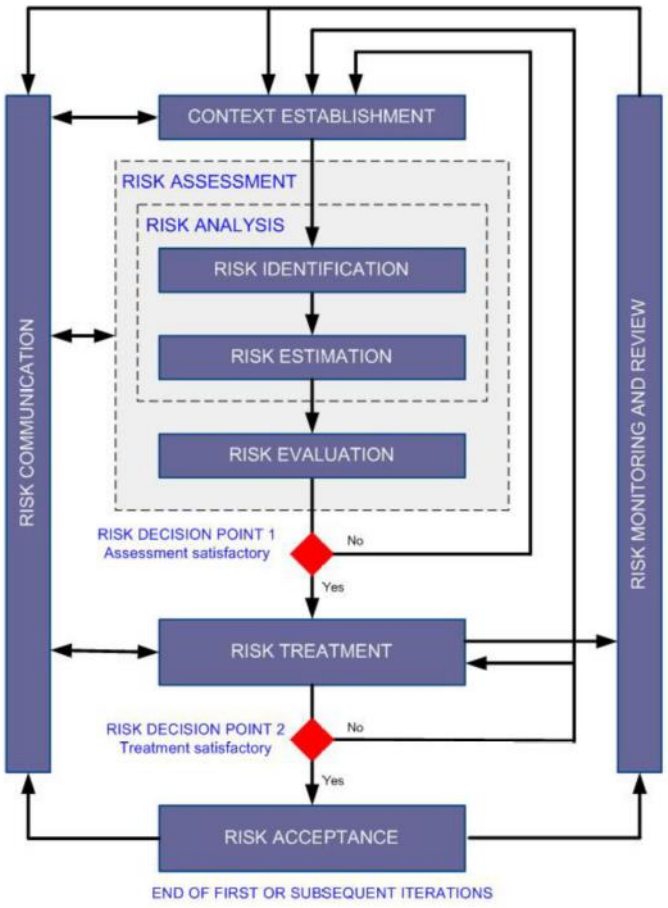


Figure 21: ISO/IEC 27005 Risk Management Method (ISO, 2014)

4.7.2 Structure

The ISO/IEC 27005 RA process, differs from the definition of the RA process as described for this comparison analysis. This comparison analysis also includes the setting of the context, which in case of the NEN 7510 is already done, i.e. the healthcare context. According to this standpoint the RA process of the ISO/IEC 27005 has four main phases: (1) context establishment (2) risk identification, (3) risk estimation and (4) risk evaluation.

- **Phase 1: Context establishment.**

  The risk identification process first sets the scope for the risk assessment. From this scope the assets of value of the company, which need to be protected, are identified. In the information security process these assets consist out of more than just software and hardware.
- **Phase 2: Risk identification.** The next process is the identification of threats. Information is gained through incident reviewing, asset owners, users and other sources, including external threat catalogues. Threats could be from natural or human sources and accidental or deliberate. Now existing and planned controls are identified to prevent duplicate controls. These controls are checked to see if they work properly. Based on the asset list, threat list and control list the vulnerabilities in information security are now determined. The last step in the identification is to develop a list of incident scenarios. In these scenarios the consequences of a threat exploiting a vulnerabilities are described based on confidentiality, integrity and availability.
- **Phase 3: Risk estimation.** The risk estimation process starts by selecting a proper risk estimation methodology. This methodology may either have qualitative estimation, quantitative estimation or both. The qualitative estimation uses an ordinal scale to describe the magnitude of potential consequences (e.g. high, medium, low) and the likelihood that these consequences occur. Quantitative estimations uses a scale with numerical values for both consequences and likelihood. The quality of this analysis depends on the accuracy and completeness of the numerical values and the validity of the models used. Then based on the chosen methodology the consequences and likelihood of these are assessed accordingly. This will produce a list with all indicated risks, valued by risk level.

- **Phase 4: Risk evaluation.** During the risk evaluation process the estimated risks are compared to their risk evaluation criteria defined during the context establishment. The risk evaluation criteria used to make decision should be consistent with their internal and external information security context and take into account the objectives of the organization and the stakeholder views. In this process an analysis is made to decide whether certain activities should be undertaken and which priorities for risk treatment exist, considering the estimated levels of risks.

4.7.3 Risk Models

(R-01) The ISO/IEC 27005 gives several risk models. In general these are all based on the principle that an assessment should be made on the distinction between important and less important assets, the ease of exploitation (vulnerability) and the likelihood of threat occurrence.
(R-02) No clear distinct asset assessment is done. The main assessment of this part is included in the impact assessment.
(R-03) The given models for impact assessment are based on ordinal scales representing values from low to high, often assessing the impact on business value.
(R-04) The given models to assess the likelihood are based on ordinal scales representing values from low to high.
(R-05) All the risk prioritization methods are based on matrices in which the impact on assets, vulnerabilities and threats are mapped against each other, resulting in an overview of more and lesser important risks.

4.7.4 Support

(S-01) The ISO/IEC 27005 method assists the risk assessor with large lists of possible threats and actors. These not extensive, but provide a strong start for the user or could help with the validation of the risks. Furthermore it states extra sources (e.g. threat landscapes and interviews) are still needed and provides methods to identify threats.
(S-02) The ISO/IEC 27005 method assists the risk assessor with large lists of possible vulnerabilities as well. Also here it states extra sources (e.g. penetration tests, interviews) are needed. Several options are presented for this.
(S-03) The risk models used are fully qualitative and do not assist the user with models to gain the values, making them strongly opinion based.
(S-04) The CIA principles are explicitly mentioned as important risk evaluation criteria. Implicitly they return in the vulnerability list.
(S-05) As the method is very general, it can also been used for networked environments, although the vulnerability list only partly supports this.
(S-06) The ISO/IEC 27005 provides several structures for the process and underlines the importance of documenting and communicating these. It does not provide a tool for this.
(S-07) Validation in the ISO/IEC is done with interviews and communication to stakeholders. The quality of the execution of this process and the knowledge of the stakeholders strongly defines the strength of this process.

4.8 MEHARI 2010

4.8.1 Background

MEHARI (MEthod for Harmonized Analysis of RIsk) is a French risk assessment method, which was first released in 1998 by the CLUSIF (Club de la Sécurité de l'Information Français). The method was last revised in 2010 and is complaint to the ISO/IEC 27005 (CLUSIF, 2014). MEHARI is a risk assessment and risk management method, which includes formulas for the direct assessment of risk and options to reduce these risks. The method uses knowledge bases to document and retrieve threats, vulnerabilities, assets and risks from (CLUSIF, 2011).

MEHARI 2010 is an RA and RM method that also includes, directly in the knowledge bases, the formulas for the direct assessment of the risks and selection of the ways to reduce them. The knowledge bases are available as a workbook (for Excel or Open Office) capable to conduct the qualification and quantification of all the elements of risk (CLUSIF, 2014).

4.8.2 Structure

The MEHARI 2010 consists of three main phases, as shown in Figure 22:

- **1: Preparatory phase.**
  - The strategic, technical and organizational context is studied.
  - The scope and boundaries are set on the technical and organizational perimeters and the oversight structure of the operation.
  - Finally in this phase the technical parameters of the risk analysis are established. These consist of the risk acceptability table, the natural exposure table and the risk evaluation tables.

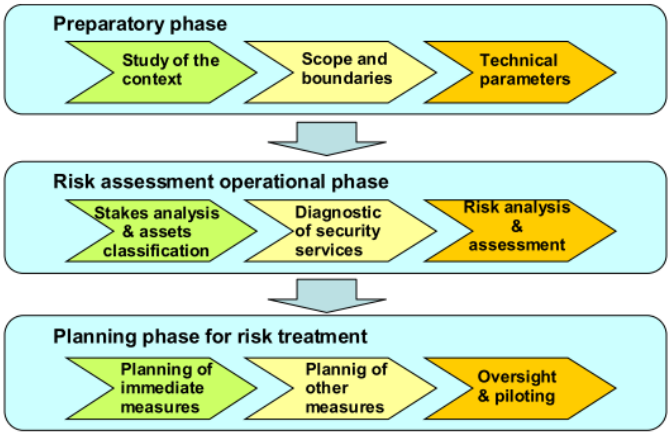


Figure 22: MEHARI 2010 Method Overview (CLUSIF, 2014)

- **2: Risk assessment operational phase.**
  - The assets are identified and classified on importance with an ordinal scale from one to four, four being the most important. Possible malfunctions for the assets are identified and the consequences of these. Based on the CIA principles of the assets and the efficiency of management processes, tables are constructed with an overview of the impact per asset.
  - The security controls already in place are mapped. This is usually done by an audit.
  - Risk scenarios are developed in order to focus analysis to possible critical situations. The total likelihood of the occurrence of the threats is measured, as well as the total impact based on the importance of the assets. The mitigating effect on the likelihood and impact of the security controls in place is calculated and subtracted from the intrinsic likelihood and impact, resulting in the residual risk seriousness.
- **3: Planning phase for risk treatment**
  - A planning is created for the implementation of security measures that can be taken directly.
  - A planning is created for more context specific measures and long term measures.
  - And finally a planning is made to develop indicators, a dash board and trend charts to monitor the treatment process.

4.8.3 Risk Models

(R-01) The MEHARI 2010 calculates the risk with the following model: Risk Seriousness = (the intrinsic likelihood of threat – reduction of likelihood of threat caused by existing security measures) x (the intrinsic impact of a threat – the reduction of impact caused by existing security measures) (Figure 23).

(R-02) Assets are rated in MEHARI as primary asset or secondary asset, based on its importance to the organization.

(R-03a) The intrinsic Impact is valuated by creating intrinsic impact tables. In these tables all assets are listed and for each asset for the availability, integrity or confidentiality a value on an ordinal scale from zero to four is given, i.e. no impact, low impact, medium impact, high impact and catastrophic impact. For standard intrinsic impacts a guideline of values is presented.

(R-04a) The intrinsic likelihood of existing threats are valued on an ordinal scale from one to four, i.e. unlikely, fairly unlikely, fairly likely and very likely.

(R-03b & R-04b) The reduction factor of impact is measured by the protective and palliative measures in place. The reduction of the likelihood is calculated by the dissuasive and preventive measures in place. If only one measure is in place the calculated value for this measure is the used value. If more measures are in place, a calculation is made how effective these are together. The final score is recalculated to an ordinal scale from

zero to four, four being the strongest reduction.

(R-05) The residual likelihood of the risk is measured with P-tables. These tables show for each risk group (i.e. natural disaster, error, malicious intent) the residual risk after subtraction of the dissuasive and preventive measures. The residual impact of the risk is measured with I-tables. These tables show for each scenario criterion (i.e. confidentiality, integrity, availability and limitability), the residual risk after subtraction of the protective and palliative measures. The sum of these residual likelihood and impact values is the risk seriousness. These values can then be ranked and evaluated.

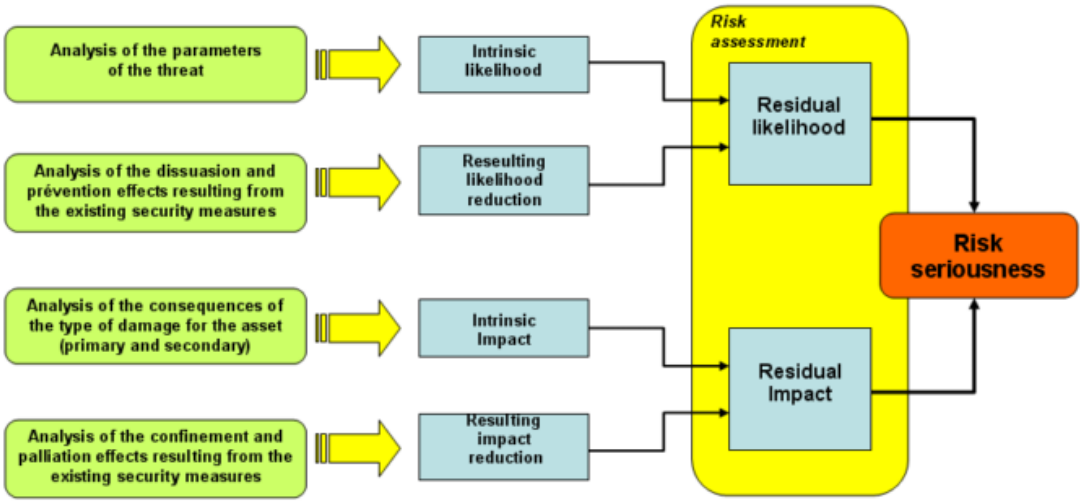


Figure 23: MEHARI 2010 Risk Model (CLUSIF 2010)

4.8.4 Support

(S-01 & S-02) MEHARI 2010 reasons from the main assets and all the malfunctions which might occur to these, instead of the often used threat, vulnerability driven approach. It has standard values for standard types of risk. For more domain specific risks more quantified measure scales, which apply to the domain, can be made. These will later be translated to the standard ordinal scale of MEHARI. The method supports this approach fully.

(S-03) The risk model provides a sophisticated, clear and structured way of assessing the risks. The main downside of MEHARI 2010 is the basic approach in which the asset valuation is done. These are only divided in primary and secondary assets. A more specific dividing process might improve the method.

(S-04) MEHARI 2010 uses an extended form of the CIA principles to map important possible threats towards an organization. This method gives a strong overview of the main impact possibilities.

(S-05) MEHARI 2010 is strongly asset directed. Possibilities for interactive environment evaluation in networks can be done in a more abstract way if it is viewed as an asset on its own, but this approach would be devious.

(S-06) The documentation of the process and scenarios in MEHARI 2010 is very structured and good manageable because of the knowledge base approach used.

(S-07) The sub process is validated on several occasions in the process by giving feedback to the stakeholders and interviewing them about the results. Their knowledge and especially the skills of the risk assessor are important in the process.

4.9 OCTAVE Method

4.9.1 Background

OCTAVE stands for Operationally Critical Threat, Asset and Vulnerability Evaluation. This method, developed by the CERT software engineering institute of Carnegie Mellon University, was developed for large organizations with 300 employees or more. The original OCTAVE method uses an approach to examine organizational technology issues in three stages: (1) organizational view, (2) technological view and (3) strategy and plan. It assembles a comprehensive view of the organization's information security needs. The method consists of a

series of workshops, facilitated or conducted by interdisciplinary analysis teams of three to five employees of the organization (CERT, 2014) .

4.9.2 Structure

The method applies the following processes:

- **Process 1:** Identify the senior management knowledge of the critical assets, areas of concern, security requirements, current protection strategy practices and organizational vulnerabilities.
- **Process 2:** Identify the operational area management knowledge of the critical assets, areas of concern, security requirements, current protection strategy practices and organizational vulnerabilities.
- **Process 3:** Identify the staff knowledge of the critical assets, areas of concern, security requirements, current protection strategy practices and organizational vulnerabilities.
- **Process 4:** Create threat profiles. These are created based on a picture of the critical assets and threats.
- **Process 5:** Identify key components of the computing infrastructure so that they can be examined for vulnerabilities.
- **Process 6:** Evaluate the selected components. In this process a search for technological vulnerabilities is done in the existing infrastructure.
- **Process 7:** Identify and prioritize the risks of the organization. A priority list of risks based on the impact to the organization is delivered in this stage.
- **Process 8:** Develop a protection strategy. In this process a strategy is developed to mitigate the prioritized risks.

In Figure 24 process 1 till 4 are executed in stage 1, process 5 and 6 are executed in phase 2 and process 7 and 8 are executed in phase 3.

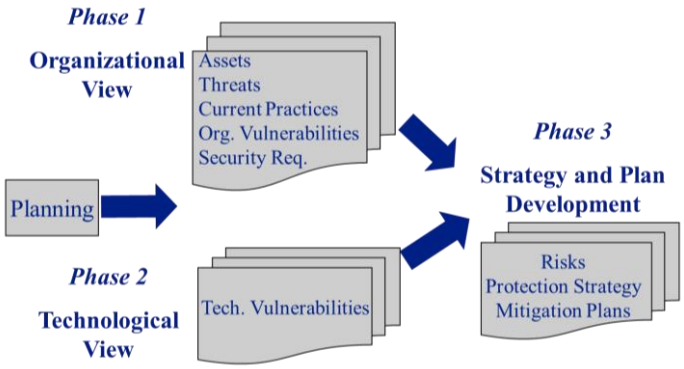


Figure 24: OCTAVE Method Overview (SEI, 2001)

4.10 OCTAVE-S

4.10.1 Background

For smaller organizations up till 100 people, the OCTAVE-S method was developed. This method meets the same criteria as OCTAVE, but uses a more streamlined process and different worksheets. It however produces the same results (SEI, 2005).

4.10.2 Structure

The two main differences with OCTAVE are:

1. For the OCTAVE-S method a small team of 3-5 people who understand the company is enough. The method does not begin with formal knowledge elicitation workshops to gather information. It is assumed that that team can provide all the necessary knowledge.
2. And for the OCTAVE-S method only a limited exploration of the infrastructure is done. Vulnerability tools are not used, since the tools might be difficult to interpret and their IT if often outsourced (SEI, 2005).

4.11 OCTAVE Allegro Method

4.11.1 Background

This is a streamlined variant of the OCTAVE method, which focusses on information assets. Similar to the OCTAVE method, it can be performed in a workshop setting. It is however also possible to use for individuals that want to perform a risk assessment without extensive organizational involvement, input or expertise. In this method the important assets of the organization are identified and assessed based on their information assets to eliminate potential confusion about scope (CERT, 2014).

4.11.2 Structure

The OCTAVE Allegro method consists of 8 steps:

- **Step 1:** Establish risk measurement criteria. This are the drivers that will be used to evaluate the effect of a risk to the organization. This includes the defining of impact areas and the ranking in importance of these.
- **Step 2:** Develop an information asset profile. For this al information assets that should be included are listed and rated on importance. From this list the most important assets are chosen and of these IT assets a more information is gathered.
- **Step 3:** Identify information asset containers. This identifies the place where the asset is stored, how it is transported and how it is processed.
- **Step 4:** Identify areas of concern. This is done by starting to develop information asset risk profiles. In this case a risk is defined as the combination of a threat (a condition) and an impact (consequence).
- **Step 5:** Identify threat scenarios. Such a threat scenario is a situation in which information assets can be compromised. It contains properties such as assets, an access or means, an actor, a motive when the actor is human and an outcome.
- **Step 6:** Identify risks from the threat scenarios. In this step the impact of the threat scenarios are determined quantitatively.
- **Step 7:** Analyze risks. In this step the risks are qualitatively valued based on the impact scores. This is then used to rank the risks based on importance.
- **Step 8:** Select Mitigation Approach. In this step it is considered which risks should be mitigated and how. In practice this usually means that the high impact risks are the most important to mitigate (SEI, 2007).

4.11.3 Risk Model

Since the risk models are the same in all OCTAVE methods, they will be given once:

(R-01) A risk is defined as the possibility of suffering harm or loss and a certain impact it has on the asset. The total impact score is given as the product of the rankings of the impact areas times their impact value. The total impact score of the impact assessment is then multiplied with the likelihood a threat occurs.
(R-02) The assets are assessed on their importance to the organization. Only the critical assets are assessed.
(R-03) The impact assessment is done by developing domain specific quantitative models that assess the impact on reputation, financial, productivity, safety and legal penalty impacts. These impact areas are ranked on importance. Per impact area the ranking is multiplied with the impact value, which is scored on 1 (low), 2 (moderate) or 3 (high).
(R-04) A threat likelihood assessment is done on an ordinal scale with the values: low, medium and high.
(R-05) The risk prioritizing is done by using risk matrixes. The score calculated for the impact is plotted against the threat likelihood. Based on the position in the matrix the risks are either in pool 1, 2, 3 or 4. Pool 1 risks needs to be mitigated, pool 2 risks needs to be mitigated or deferred, pool 3 risks needs to be deferred or accepted and pool 4 risks can be accepted.

4.11.4 Support

If major differences in the support criteria are found, they are specified individually. However mostly the three methods are supported with the same principles.

(S-01) Support for threat discovering is given by threat trees. These identify threats based on four categories: human actors using technical means, human actors using physical access, technical problems, and other problems. This provides a framework to identify threats and is supported with questionnaires.
(S-02) Vulnerabilities in this method are identified based on historical failures, accidents and concerns that came up. The OCTAVE and OCTAVE Allegro method can use the help of a vulnerability assessment tool.
(S-03) As the method has no clear likelihood of threat occurrence imbedded in the risk model the high impact, low likelihood threats might become too important and decrease the quality of the risk assessment. Also the ranking of the impact areas is done rigidly, which might skew the results score.
(S-04) The CIA principles are embedded in the security requirement analysis, which define the current gap in the security measures.

(S-05) Networked environments can be assessed with the use of information asset containers, although a broad definition of this concept might be used.
(S-06) For the documentation of the process some structure is provided, although little specific attention is given to this.
(S-07) Little support is given concerning the validation of the process. It seems to be the responsibility of the risk assessor itself to validate its results.

4.12 Trike Method

4.12.1 Background

Trike is an open source threat modeling tool and methodology. The project started in 2006 as an attempt to improve the effectiveness and efficiency of existing threat modeling methodologies and is continuously in further development (octotrike, 2014).

For the threat modeling process it uses a risk management perspective. It is meant for security auditing teams to accurately and completely describe the security characteristics of a system, both in high-level architecture and low-level details. The threat modeling tool can be used to automatically generate threats.

4.12.2 Structure

The process of the Trike method goes as following:

- **Step 1:** Develop a model of the requirements and the implementation of the application. This includes a list with all possible actions in which the system can be used. Identify the assets which are important for the company and give them a dollar value, based on the opinion of employees of the organization.
- **Step 2:** Generate a list of possible threats. These threats are either a denial of service or an elevation of privilege. With elevation of privilege is meant that an actor performs an action it should not be able onto an asset, that an actor performs an action on an asset despite the rules for that action or it means that the actor uses the system to perform an action on another system's asset. These threats are all generated for all identified actions.
- **Step 3:** Develop attack trees. An attack tree consists of a threat as root node and attack options in its connected nodes. In normal cases a complete attack tree will not need to be generated for every threat, but should be expanded till it is possible to decide whether the risk is reduced to an acceptable level.
- **Step 4:** Combine the attack trees in an attack graph. Since an attack can be used in realizing multiple threats, a directed graph can be constructed which contains all attacks against the system.
- **Step 5:** Define the impact. Chose a value from one to five, five being the most undesirable, for the level of undesirability that this action occurs to the asset.
- **Step 6:** Define the risk level of actors, with (possible) access to an asset. Each actor is given a risk level from one (trusted) to five (untrusted).
- **Step 5:** Weaknesses in the system are defined and added to the attack graph. Each weakness is ranked in tree scales from one to five. The first rates the ease in which the weakness can be reproduced, the second rates the exploitability of the weakness and the third rates the risk value attached to the least trusted actor able to technically effect this weakness. The overall probability of the weakness consists of these three values multiplied.
- **Step 6:** Define which weaknesses are mitigated and till what extend. Weaknesses that are not mitigated fully can be defined as vulnerabilities. The exposure for a vulnerability is now set as the sum of exposures of the threat this vulnerability makes possible.
- **Step 7:** Calculate the threat risk value by multiplying the threat exposure by the largest applicable vulnerability risk. This is then related to the impact, giving an overview of the most important risks (Saitta, Larcom, & Eddington, 2005)

4.12.3 Risk Model

(R-01) The overall risk model is given by multiplying the asset score times the impact score times the likelihood score.
(R-02) The asset are given a monetary value based on their inherent business value to the organization. This is

not their market worth, but the value as is estimated for the organization.
(R-03) The impact is assessed by considering all actions that can be taken on an asset and choosing relative values for the undesirability for them based on an ordinal scale from 1 to 5, 5 being the most undesirable. This rating occurs twice, first based on the actions that can occur while following the rules, if possible, and then when the actions are completed by an attacker who breaks the system rules. Now the actors are rated from 1 to 5, 5 being an actor with the most malicious motivation. The multiplied score of the ratings are now calculated and give an indicator of risk seriousness.
(R-04) The likelihood of the threats is measured based on the ease of use of the exploitation of a vulnerability times the reproducibility of the vulnerability, both measured on a scale from 1 to 5, five being respectively the easiest and most reproducible.
(R-05) The risk prioritizing is done by putting the risk with the highest score the highest in the list. Mitigating controls can then be chosen accordingly.

4.12.4 Support

(S-01) Support for threat discovering is given through a basic protocol, including denial of service, possible harmful actions which might occur following the rules, possible harmful action which might occur while breaking the actions and the possibility of taking one system and using it against another system.
(S-02) Support for vulnerability discovering is not explicitly provided. It is advised to sweep the code for exploitable weaknesses, which might be exploited from the threats.
(S-03) The quality and type of risk models used in the method are strongly dependent of the quality of the process and the skills of the risk assessor. This method desires at least a highly skilled tester or programmer to test the code of the programs.
(S-04) The use of the CIA triad are not explicitly included, however an alternative related set of information security points is included.
(S-05) Attention in the method for networked environments is covered mainly in the threat identification in the aspect which views possible actions of taking one system and using it against another.
(S-06) About the documentation of the process and scenarios it is mentioned that it should be included, however no guidelines are given.
(S-07) Validation approaches used by the method are not mentioned explicitly.

4.13 Conclusion Cyber Security Risk Assessment Method Comparison

4.13.1 Risk Models

The risks models determine the sub-processes needed to gather information, which can then be analyzed and evaluated. Different methods utilize different risk models. A distinction can be made between closed and open risk models. Closed risk models use a control standard as baseline. The risks are derived from the lack of controls implemented. Open risk models on the other side allow the risk assessor to develop an unlimited amount of risks based on the threats, vulnerabilities, assets and controls. Hybrid models exist as well. Most risk models may include an asset valuation, business impact assessment and a threat likelihood assessment. Some methods work with gross risks (risk value without the decreasing ability of implemented controls) and net risks (remaining risks with the effects of implemented controls subtracted) others only have a single analysis process. Finally all methods have some form of risk evaluation based on their severity and form some sort of ranking. The processes are all aided by tools and standardization for documentation. Simple risk models often use risk matrixes in which they map risk likelihood against the risk impact. In these risk matrixes a distinction is made between high, medium and acceptable risks. The more complex risk models try to provide insight in the gap between the amount of acceptable risks and current risk, stating which risks should be addressed to obtain a level in which all remaining risks are acceptable.

Concerning the different types of risk models the open risk models allow for more nuance and are better adjustable to the introduction of new threats than closed risk models. Also open risk models align better with the concept or risk assessment as described in the ISO 27799. One advantage of a closed risk model is that it has a more clear approach to ensure the basic controls are implemented and obtain an overview of which controls still need implementation.

Regarding the use of more complex models, which include asset valuation and net-gross risk differentiation, this may help with gaining better insight in differences between risks, obtaining a more detailed view. However to use these more complex models successfully the use of a method seems required, since they require a detailed approach which would benefit of pre-developed threat lists, vulnerability lists and all kind of supportive tools.

4.13.2 Support Points

Considering the support points which were evaluated some general conclusions could be taken.

Threat identification: Most methods use interviews or brainstorm sessions to identify threats. Other methods include lists of standard threats, or even standard risks. Often the identification use frameworks and threat catalogues to ensure the list of threats is complete.

Vulnerability identification: As with threat identification this is largely interview or brainstorm based in most methods. Vulnerability lists and catalogues are used to complete the risk assessment. Further sophistication can be obtained by analyzing historical incidents, both internal and at other organizations, and on a more technical level test the systems for vulnerabilities. Closed risk model based methods rely heavily on control gap analysis to identify vulnerabilities.

Risk model: As described at paragraph 4.13.2 different risk model types exist. As most risk assessment methods are domain neutral the most important question is whether they support domain specification. Most risk models enable this. However closed risk models seem less fit for this as domain specific control standards are often based on ideas of open risk models.

CIA triad: The methods who use the CIA triad often use this to develop different scenarios or to explore the consequences of potential incidents. This approach seems to be solid and often adopted.

Networked environments: Only Trike specifically motions this as an important component. However almost all methods allow for use in networked environments.

Tools and documentation: The sophistication of the tools used differs from risk matrixes and standardized forms to software based tools that support the whole risk assessment process. Some methods include the use of knowledge bases as well, stressing the importance for the storage and recycling of previous done work.

Validation: All methods based on open risk models do validation of their (sub) results at important stakeholders. Even if the stakeholders would not be able to provide added value, they are still involved as the stakeholders are often the ones responsible for the budget for the controls, the implementation of the controls or are the ones who have to comply with the controls.

In Table 10 an overview is given of the compared support points that were described at the beginning of this chapter per individual method.

	CORAS	CRAMM	EBIOS 2010	ISO/IEC 27005	MEHARI 2010	OCTAVE	Trike
Threat identification	From brainstorm sessions	Interview based	Identified from the loss of CIA per asset	Large list of threats and actors provided. Advice given over other sources.	Standard values for standard risks. Possibilities for domains specific quantification	Threat trees used with interviews	Basic protocol is given to identify threats
Vulnerability identification	From brainstorm sessions	Interview based	Based on control gap analysis	Large list of vulnerabilities provided. Advice given over other sources	Standard values for standard risks. Possibilities for domains specific quantification	Based on historical failures, accidents and concerns	Not explicitly given, code sweep is advised
Risk model	Basic, but open to more domain specification	Advanced, but needs to be made domain specific	Advanced, quality depends on the chosen security baseline	Different options given, all of moderate sophistication	Advanced	Basic, but open to more domain specification	Advanced, but needs to be made domain specific
CIA triad	Not mentioned	Used to create impact overview	Used to identify the security needs for assets	Used for risk evaluation. Implicit used in the vulnerability list	Used to map important possible threats	Embedded in security requirement analysis	Not explicitly included
Networked Environ-ments	Not specifically, but possible	Not specifically, but possible	Possible, depends on security baseline	Possible, but only partly explicitly supported	Possible, but only partly explicitly supported	Possible, but only partly explicitly supported	Covered in threat identificati on
Tools & Documen-tation	Strong scenario modeling tool & language	Tool supported	Extensive amount of stencils provided	Several stencils provided, no tool provided	Supported with a knowledge base	Structure is partly provided	No guidelines given
Validation	Based on interviews	Based on interviews	Compliance to base standard	Based on interviews	Based on interviews	Based on interviews	Not explicitly mentioned

Table 10: Overview of Risk Assessment Comparison on Support Points

4.13.3 Advice for Hospitals

From this comparison analysis an advice can be provided for hospitals. First of all the EBOIS 2010 method has a closed risk model which differs from the advised open risk model described in the ISO 27799 and the NEN 7510. The problem with this risk model, although it has a high ease of use, is that is does not discriminate enough between the different needs and risk levels of different types and sizes of hospitals. Therefore it is advised not to use this model. The risk assessment methods CORAS and TRIKE are both still in development and do not yet provide all the support and resources other methods do. And although they both seem to have

promising elements, for now it is advised not to use these methods until they have reached a more mature level. OCTAVE, although provided with a large amount of stencils, mainly focuses on the strategic and policy level of the organization, thereby lacking the right depth into technical threats and vulnerabilities, making it less fit for a hospitals in which due to patient safety the stakes are high and the room for error is small. The ISO 27005 provides a good basis for risk assessments. For hospitals which do not yet have a structure the use of this method could help to get the basics right. However for hospitals with a high risk profile this will likely not suffice. The remaining two methods, CRAMM and MEHARI 2010, could both be used within hospitals and would be able to obtain an accurate and precise assessment of the cyber risks. A side note however needs to be made that CRAMM is a very intense method which requires a lot of resources and effort. Therefore MEHARI 2010may provide to be the better option for most hospitals. And finally other useful methods may be out there which were not found or included in this comparison for the stated reasons. For example a country specific method may be the best option for hospitals in that country. CRAMM and MEHARI 2010 are merely the best fitting included international option for hospitals.

4.13.4 Input for the Maturity Model

In general all methods contain several core elements. All methods start with the definition of the scope and the context in which the risk assessment should take place. The stakeholders are identified and in most cases consulted during the process. Then an information gathering process starts in which information is gathered about assets, threats, vulnerabilities and in most methods also controls. This is followed by an analysis and an evaluation process. Next to the affirmation of the already identified process elements, several new process elements were identified:

- **Context identification:** Identify factors that define the organization were the risk assessment is performed.
- **Stakeholder identification:** Identify the stakeholders of the risk assessment and involve them in the process.
- **Scenario development:** Combine the identified information concerning the assets, threats, vulnerabilities and controls in develop incident scenarios. Often these are the aspects that are analyzed.

Next to process elements a common element seems to be very important during most processes, as most information is gathered during interviews or sessions in which certain interview techniques are used, often together with stakeholders. These interview techniques differ in sophistication, from simple interviews, to workshops which include voting devices. Interesting in this whole is that threat identification, vulnerability identification and asset identification use a lot of similar processes, as they all gather information from similar sources, often including personnel.

Since most CSRA methods work with open risk models and as the ISO 27799 prescribes such the maturity model will focus on an open risk model. The use of the confidentiality, integrity and accessibility principles will hereby be taken into account as these were deemed important and used in almost all methods. The use of the method in networked environments did not provide much specific information, in the design this subject will therefore be attended as a more abstract subject. Furthermore the tools, which some methods provided seem indeed to provide a lot of support to the risk assessor and are therefore taken into account as well. Hereby specific attention will be aimed at the use of a knowledge base, which allows for incremental improvement of the risk assessment process. And finally the validation of the CSRA seems to be strongly dependent on the stakeholders and will be connected to them in such a manner.

5 Maturity Model Planning

According to the chosen method for maturity model the maturity model development should start by a comparison study in which according to a set of inclusion and exclusion criteria subject related maturity models are identified and compared to obtain useful content and design architectures. The maturity model comparison is followed by the development strategy and approach, which explains how the maturity model will be designed and which principles underlie this process. After these sections the context in which the maturity model is situated (chapter 6) and the results of the maturity model development (chapter 7) are described. The context consists of the hospital culture related to cyber security, the threat landscape and the methods used by the hospitals for their CSRAs.

5.1 Maturity Model Comparison Study

The maturity model comparison study identifies and compares existing maturity models to give an overview of useful architectural practices and content. The identification is done through a web search and a search on Google Scholar. An identified maturity model is included if it defines different steps who define different maturities in certain capabilities or processes (Inc-01). Furthermore the domains in which the model is used should be information or cyber security, risks, IT in healthcare a combination of before mentioned or the maturity model is recognized as a general framework on which other maturity models are build (Inc-02).

Inclusion Criteria

(Inc-01) The model defines some sort of steps towards the improvement in maturity of certain capabilities or processes.
(Inc-02) The model is related to Information or cyber security, risk, IT in healthcare, a combination of the before mentioned or the maturity model is recognized as a general framework on which other maturity models are build.

Based on the inclusion criteria a search statement is formulated:

("Maturity Model" AND (((Information OR Cyber) AND Security) OR Risk OR "Risk Assessment" OR (Healthcare AND "Information Technology"))

Two maturity models were added outside of these inclusion criteria. The Capability Maturity Model Integration for Service Organizations was added as it is often used as a standard framework for the architecture of new maturity models. On an abstract level the information security management system can been seen as a quality process for a service organization, i.e. a healthcare provider. The second maturity model the T is added since this model was used to test the level of information security at Dutch hospitals and thus contains a direct link to the sector (Dutch hospitals) and the subject (CSRA).

From the search results a long list of maturity models was constructed (Table 11), showing the year of the latest documentation release and the domain or domains to which they appertain. To ensure all models used in the comparison comply with high standards, i.e. they are not just put together as a concept or idea of someone, but embedded in well-structured theory. Therefore several exclusion criteria are set, of which the first two demand a certain level of scientific research to be in place and the latter one demanding a clear explanation of the model in its final form. Therefore the model should contain information concerning the theory and problem statement which are used to trigger the development design and describe any models on which the architecture or content is based (Ex-01). As well the design process, i.e. the description of the method used and the steps taken to come to the end result, and the method and processes used to validate and evaluate the maturity model should be clearly described (Ex-02). Finally it should be clear how the model should be used and the content should be explained (Ex-03). In the long list in Table 11 an overview is provided of the exclusion criteria that applied to certain maturity models or in case none applied whether the maturity model was included in the comparison. Excluded models where at most used for inspiration.

Exclusion Criteria

(Ex-01) The model lacks information concerning the models and theory it is based upon.
(Ex-02) The model lacks documentation concerning the design and evaluation processes used during the development of the model.
(Ex-03) The model lacks information concerning the documentation of the use or content of the model.

Reference	Name	Organization	Source Date	Domain					Exclusion Criteria
				IT	S	R	H	G	
01	The Community Cyber Security Maturity Model	CIAS	2011	✓	✓				Included
02	Electric Subsector Cybersecurity Capability Maturity Model	USA, The Department of Energy	2014	✓	✓				Included
03	Open Information Security Management Maturity Model	The Open Group	2011	✓	✓				Included
04	Capability Maturity Model Integration	SEI	2003	✓				✓	Included
05	Toetsingskader Informatiebeveiliging Maturity Model	NIAZ/NOREA	2012		✓	✓	✓		Included
06	Cyber Security Maturity Model	Harris Corporation	2010	✓	✓				(Ex-01)
07	Information Security Competence Maturity Model	Port Elizabeth Technikon	2006	✓	✓				(Ex-02)
08	Hyper Connectivity Readiness Curve	World Economic Forum	2012	✓	✓				(Ex-01), (Ex-03)
09	Cyber Security Capability Maturity Model	Deloitte Belgium	2012	✓	✓				(Ex-01), (Ex-02), (Ex-03)
10	Deloitte Cyber Security Maturity Model	Deloitte Nederland	2014	✓	✓		✓		(Ex-01), (Ex-02), (Ex-03)
11	Cyber Security Maturity Model	Cyber Security Strategies LLC	2010	✓	✓	✓			(Ex-01), (Ex-02), (Ex-03)
12	United States EMR Adoption Model	HIMSS Analytics	2012	✓			✓		(Ex-01), (Ex-02), (Ex-03)
13	A New IT Maturity Model (Value-based)	Oracle	2012	✓					(Ex-01), (Ex-02), (Ex-03)
14	NIMM - NHS Infrastructure Maturity Level Summary	Atos Healthcare	2009	✓			✓		(Ex-01), (Ex-02), (Ex-03)
15	Security Awareness Maturity Model	SANS	2012	✓	✓				(Ex-01), (Ex-02), (Ex-03)
16	Aon Global Maturity Model	Aon	2010			✓			(Ex-01), (Ex-02), (Ex-03)
17	Risk Management Maturity	Riskpoint	2012			✓			(Ex-01), (Ex-02), (Ex-03)

Table 11: Longlist Maturity Models

5.1.1 Comparison Criteria

The maturity models included in the comparison are compared on several criteria. The comparison criteria serve two goals: to identify useful architectural frameworks and identify useful content. Per included maturity model a short description about the model, the organization that developed the model and its use in its domain will be given. Then the maturity models will be compared on the type of theory or models the maturity model is based upon (C-01). The used maturity levels in the maturity models are compared to identify useful maturity structures (C-02). As well as the maturity levels, the sub-domains that can obtain the levels of maturity are compared (C-03). And finally the main useful content for the maturity model is identified (C-04).

Comparison criteria:

(C-01) Used theory or models.
(C-02) Maturity levels architecture.
(C-03) Sub-domain architecture.
(C-04) Content useful for the maturity model.

5.1.2 CCSMM

The Community Cyber Security Maturity Model (CCSMM), shown in Figure 25, was published in 2011 at the University of Texas. As a trend concerning threats and attacks on computer systems and networks was found and since communities, states and nations rely in increasingly amount on such systems a need was identified to develop a measurement instrument and a roadmap to depict the level of cyber security within countries and give options to improve this (White, 2011).

(C-01) The CCSMM is based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) (SEI, 1999)and the Capability Maturity Model for Software (SW-CMM) (Jung & Goldenson, 2003).

(C-02) Five maturity stages are identified in the CCSMM, i.e. initial, advanced, self-assessed, integrated and vanguard. In level 1: initial the communities have little to no cyber security awareness, analysis and assessments. In level 2: advanced the communities are aware of cyber threats and issues and informal sharing occurs. In level 3: self-assessed leaders within communities actively promote cyber security awareness, training and cooperation with others. In level 4: integrated cyber security becomes part of the foundation of the community and is a part of the planning process. And finally in level 5: Vanguard cyber security has become business imperative (UTSA, 2014).

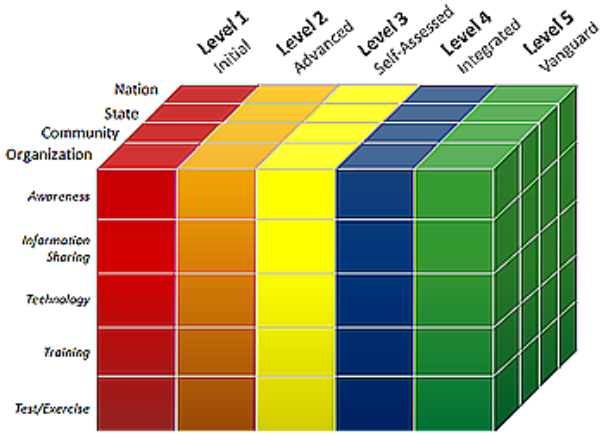


Figure 25: The Community Cyber Security Maturity Model

(C-03) The CCSMM is depicted in three dimensions. One of these dimensions consists of the maturity levels as described in (C-02). The second dimension consists of the different domains of cyber security, i.e. awareness, information sharing, technology, training and test/exercise. The other dimension depicts the scope of the maturity model in nation, state, community and organization. As a nation clearly other measures and policies are needed than on organizational level. This maturity model integrates them into one model.

(C-04) The CCSMM gives a structured high level overview of important practices in cyber security. Practical for the HCRAMM it provides an overview of the capabilities organizations should have at certain maturities and thus what information the organization would poses and be able to provide in the CSRA process. Especially information sharing, technology and testing and exercises are sub-domains in which information is generated, that might prove useful for the CSRA process. Training and awareness provide conditions that improve the information generation from interviews, workshops and other methods using human resources. Aspects that should be at least taken into account are (White, 2011):

- Information should be shared with and gained from security communities, organizations from similar nature and governmental security organizations.
- The cyber security of an organization should be tested and exercises should be held, the information gained from this can then be used for the risk assessment.
- Ways to measure the quality of an organization's security should be available. The HCRAMM will provide a specific solution for the risk assessment.

5.1.3 ES-C2M2

The Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was published in 2014. It is developed as White House initiative (United States of America government), led by the Department of Energy. The ES-C2M2 was developed to support the development of cyber security capabilities in the electricity subsector (DOE, 2014).

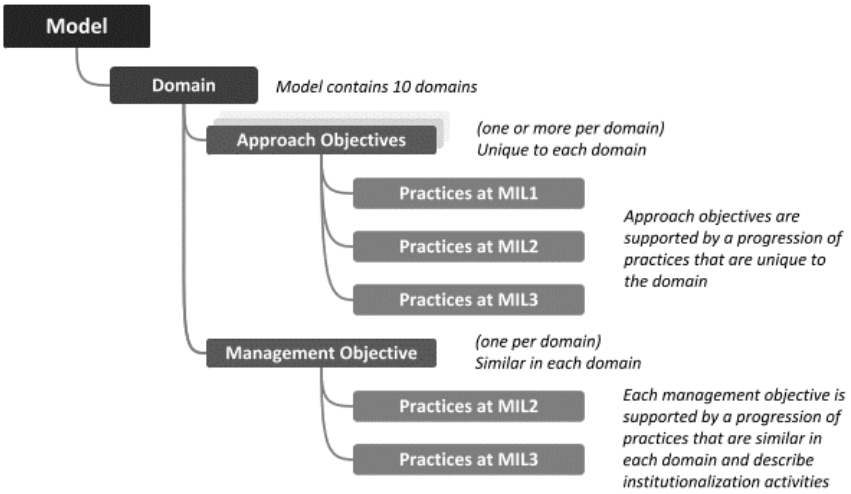


Figure 26: The Electric Subsector Cybersecurity Capability Maturity Model

(C-01) The ES-C2M2 is based on the Maturity Indicator Level Scale for cyber resilience developed by the Software Engineering Institute of Carnegie Mellon University (Butkovic & Caralli, 2013).
(C-02) The ES-C2M2 consists out of ten domains, which all have a similar architecture as shown in Figure 26. Each domain consists of one or more approach objectives that are unique for the domain, each containing fore maturity levels named maturity indicator levels (MIL), ranging from MIL 0 to MIL 3. Also each domain has a management objective which consists of practices similar for each domain, describing institutionalization activities, each containing two maturity levels MIL 2 and MIL 3. At MIL 0 and MIL 1 no management objectives are implemented.
(C-03) The subdomains used in the ES-C2M2 are risk management; asset, change and configuration management; identity and access management; threat and vulnerability management; situational awareness; information sharing and communications; event and incident response, continuity of operations; supply chain and external dependencies management; workforce management; and cybersecurity program management.
(C-04) The ES-C2M2 provides a quite extensive overview of different cyber security domains and the activities partaken in these. Concerning risk assessment however, the activities remain high level, but provide a basis which might be used as input for the HCRAMM. Concerning risk assessment the ES-C2M2 believes the following aspects are of importance (DOE, 2014):

- Risks should be documented, preferably within a risk register.
- Risk identification and analyses should be done according to a method.
- Information for the risk analysis should be extracted from the cyber security architecture.
- Stakeholders are identified.
- Standards and guidelines have been identified to inform risk assessment activities.
- The risk assessment is periodically reviewed.
- Authority and responsibility for the performance of the risk assessment is assigned to personnel.
- Personnel performing risk assessment has the right skills and knowledge needed for their task.

The other domains and their identified activities are useful to identify information generated during the ISMS cycle, which is useful as input for the CSRA process.

5.1.4 O-ISM3

The Open Information Security Management Maturity Model (O-ISM3), as shown in Figure 27, was published in 2011 by The Open Group. It is developed to ensure that security processes are aligned with organization's business requirements. It is made compatible with the ISO/IEC 27000:2009, COBIT and ITIL standards (The Open Group, 2011).

Capability Level		Initial	Managed	Defined			Controlled	Optimized
Management Practices Enabled		Audit, Certify	Test	Monitor	Planning	Benefits Realization	Assessment	Optimization
Documentation		*	*	*	*	*	*	*
Metric Type	Activity		*	*	*	*	*	*
	Scope		*	*	*	*	*	*
	Unavailability[1]		*	*	*	*	*	*
	Effectiveness		*	*	*	*	*	*
	Load			*	*	*	*	*
	Quality						*	*
	Efficiency							*

Figure 27: The Open Information Security Management Maturity Model

(C-01) The O-ISM3 was based on ISO/IEC 27000:2009, COBIT and ITIL standards and was additionally complemented with the TOGAF model. The main development was done in work groups in the Open Group forum.
(C-02) The O-ISM3 consists of five maturity levels: initial, managed, defined, controlled and optimized. These maturity levels represent the combination of processes practiced at a certain level and the capabilities needed for these processes.
(C-03) The sub-domains consist of capabilities needed for processes to manage successfully. The capability achieved by the process depend on the metrics used to manage it and the documentation of the process.
(C-04) The O-ISM3 gives an overview of important processes in information security mapped against the metrics needed for these processes. It gives a clear map on which activities to improve to obtain better information security management, it however does not go into detail about risk assessment. The most important related points are (The Open Group, 2011):

- Stakeholders should be involved.
- Knowledge should be stored and managed.
- The processes should be part of an Information Security Management design and evolution.

5.1.5 CMMI

The Capability Maturity Model Integration (CMMI), as shown in Figure 28, is a framework for the improvement of organizational processes used to develop, deliver and maintain products and services. It is published in 2002 by the Software Engineering Institute of Carnegie Mellon University (Herndon et al., 2003)

(C-01) The CMMI is based on the three Capability Maturity Models (CMM), the SW-CMM, the SA-CMM and the SE-CMM. The maturity model was originally developed for the U.S. Department of Defense to test de maturity of software companies with which they might give software development assignments (Jung & Goldenson, 2003).

(C-02) The CMMI contains two maturity level architectures. A 'continuous representation' in capabilities for a single process area and a 'staged representation' in maturity levels for multiple processes areas. An mapping of the capability levels against the maturity levels is given in Figure 29. The five maturity levels of staged representation: 1 Intitial, 2 Managed, 3 Defined, 4 Quantitatively Managed and 5 Optimizing. When using the capability levels, level 0 Incomplete is added, depicting a situation in which the process if not fully executed. Also the highest level in this case is level 3 Defined, since level four and five are processes that integrate an optimize multiple processes (SEI, 2010).

(C-03) The sub-domains consist of the different processes in system engineering. In level 1 system engineering is done ad hoc and thus not depicted in Figure 28. For the higher level a mapping is made in which is depicted which processes represent a certain maturity in the system engineering process.

(C-04) The usefulness of this maturity model lays mainly in the architectural structure which is developed to high extent and forms a useful framework to map the CSRA process in. Furthermore it gives a basic framework for risk management, one of the sub-domains, and the use of it.

Name	*Abbr.*	*ML*	*CL1*	*CL2*	*CL3*
Configuration Management	CM	2			
Measurement and Analysis	MA	2		Target Profile 2	
Process and Product Quality Assurance	PPQA	2			
Requirements Management	REQM	2			
Supplier Agreement Management	SAM	2			
Service Delivery	SD	2			
Work Monitoring and Control	WMC	2			
Work Planning	WP	2			
Capacity and Availability Management	CAM	3			
Decision Analysis and Resolution	DAR	3			
Incident Resolution and Prevention	IRP	3		Target Profile 3	
Integrated Work Management	IWM	3			
Organizational Process Definition	OPD	3			
Organizational Process Focus	OPF	3			
Organizational Training	OT	3			
Risk Management	RSKM	3			
Service Continuity	SCON	3			
Service System Development[12]	SSD	3			
Service System Transition	SST	3			
Strategic Service Management	STSM	3			
Organizational Process Performance	OPP	4			
Quantitative Work Management	QWM	4		Target Profile 4	
Causal Analysis and Resolution	CAR	5			
Organizational Performance Management	OPM	5		Target Profile 5	

Figure 28: Capability Maturity Model Integration

Level	*Continuous Representation Capability Levels*	*Staged Representation Maturity Levels*
Level 0	Incomplete	
Level 1	Performed	Initial
Level 2	Managed	Managed
Level 3	Defined	Defined
Level 4		Quantitatively Managed
Level 5		Optimizing

Figure 29: Capability Level to Maturity Level Mapping

5.1.6 TIMM

In 2010 hospitals in the Netherlands had to show, through an external NEN 7510 audit, to the Dutch healthcare inspection that they were structurally improving their information security. The Dutch association of hospitals (Nederlandse Vereniging van Ziekenhuizen or NVZ in short) decided these standards were too burdensome at the time and therefore created their own NVZ standard based on the NEN 7510. This NVZ standard was an ad hoc norm and was not meant as a regulation for certification audits to assess compliance with the full NEN 7510 standard. The regulation included the integral risk analysis and a selection of 33 elements from the old NEN 7510 (Nederlands Normalisatie-instituut, 2014). To test the information security in hospitals the NVZ standard was depicted in a Toetsingskader Informatieveiligheid Maturity Model (TIMM) (Figure 30) to which the maturity level of the hospital could be represented. The NIAZ, the Dutch healthcare

accreditation institute, and NOREA, the Dutch EDP auditor order, further developed the test criteria and published the results in 2012 (NIAZ, 2014).

score	PDCA cyclus	CMM volwassenheidsniveau	EDP-auditing
n.v.t.	Het onderwerp is niet van toepassing (gemotiveerd / onderbouwd).	n.v.t.	
1	Plan: Er zijn afspraken maar deze zijn (nog) niet vastgelegd of afspraken zijn vastgelegd maar de implementatie ervan is slechts beperkt uitgevoerd.	Ontkennend (initial) Problemen worden pas opgelost als ze zich stellen (ad-hoc). Het niveau dat iedere organisatie aankan.	Opzet
2	Do: Afspraken zijn vastgelegd en de implementatie ervan is grotendeels uitgevoerd.	Reactief (repeatable) Het niveau waarbij de organisatie zover is geprofessionaliseerd (bijvoorbeeld door het invoeren van projectmanagement) dat bij het ontwikkelproces gebruik wordt gemaakt van de kennis die eerder is opgedaan. Beslissingen worden genomen op basis van ervaring.	Bestaan
3	Check & Act: Uitvoering en naleving van de vastgelegde afspraken zijn eenmalig geëvalueerd en waar nodig zijn de plannen bijgesteld.	Bureaucratisch (defined) Het niveau waarbij de belangrijkste processen zijn gestandaardiseerd.	Werking
4	Control: Uitvoering en naleving van de vastgelegde afspraken zijn periodiek geëvalueerd, doeltreffend gebleken, geborgd en worden indien nog nodig bijgesteld	Proactief (managed) Het niveau waarbij de kwaliteit van het ontwikkelproces wordt gemeten zodat het kan worden bijgestuurd.	Doeltreffendheid

Figure 30: Toetsingskader Informatieveiligheid Maturity Model

(C-01) The content of the maturity model is based on the NEN 7510, the standard for information security in Dutch healthcare. The architecture of the maturity model is based upon the Deming cycle and the CMM model (Informatieveiligheid, 2012).
(C-02) The TIMM contains five maturity levels. 0 the subject is inapplicable. 1 Opzet (Initial): there is a plan, however the implementation is only partly or not completed. 2 Bestaan (Repeatable): appointments are made and the implementation of these are mostly completed. 3 Werking (Defined): implementation and compliance are evaluated once and if needed plans are adjusted. 4 Doeltreffendheid (Managed): implementation and compliance are evaluated regularly, have a proven effectiveness, are secured and if needed adjusted.
(C-03) The sub-domains of the maturity model consist of a selection of norms chosen by the NVZ from the NEN 7510. These include subjects such as defining the ISMS, information security policies, organization of information security, management of information sources, the personnel, physical security, communication and operating processes, access control, maintenance of the information systems, business continuity and compliance.
(C-04) The TIMM gives an example how the NEN 7510 norms can be mapped in maturity levels. As risk assessment is a part of the NEN 7510 as deducted from the ISO 27799, which can be used for its architectural frame.

5.1.7 Conclusion Maturity Model Comparison

The main conclusion from this maturity model comparison is that no CSRA related maturity model yet exists, let alone for hospitals. Some maturity models contain CSRA, however they mostly view processes from such a high level that the cyber risk assessment process is mentioned briefly at most. However a section of the CCSMM stresses metrics or to clarify, it stresses the need for cyber security measurement methods (White, 2011). As CSRA is a part of this, the HCRAMM will provide a needed measurement tool for this subsection.

Some use of the compared models lays in their maturity level architecture, which can be used to build a structure for the HCRAMM. Especially the architecture of TIMM, based on the CMMI structure, seems to be of great use as this is already used and proven effective in the field of information security within Dutch hospitals. Therefore the HCRAMM architecture, specifically the maturity level construction will be build up from the TIMM and CMMI concepts. An overview of the comparison is given in Table 12.

	CCSMM	ES-C2M2	O-ISM3	CMMI	TIMM
(C-01) Models and theory used	SSE-CMM, SW-CMM	Maturity indicator level scales for cyber resilience	ISO/IEC 27000:2009, COBIT, ITIL and TOGAF	SW-CMM, SE-CMM, SA-CMM	NEN 7510, Deming cycle, CMM
(C-02) Maturity level architecture	Initial, Advanced, Self-Assessed, Integrated and Vanguard	Approach objectives MIL 0/3 and management objectives MIL 2/3	Initial, Managed, Defined, Controlled, Optimized	Initial, Managed, Defined, Quantitatively Managed, Optimized	Inapplicable, Initial, Repeatable, Defined, Managed
(C-03) Sub-domain architecture	Cyber security domains and community scope	Cyber security subdomains	Information security metrics	System engineering processes	NEN 7510 test criteria
(C-04) Main usefulness of content	High level overview of cyber security	High level overview of cyber security	High level overview of Information security	Strong architectural framework	Example of NEN 7510 standards mapping in a maturity model

Table 12: Overview of Maturity Model Comparison

Next to the architectural frames which is useful some content can be used. Although not all models provide useful content for CSRA, some useful content is deducted from the maturity models:

- Information should be shared with and gained from security communities, organizations from similar nature and governmental security organizations.
- The cyber security of an organization should be tested and exercises should be held, the information gained from this can then be used for the risk assessment.
- Information for the risk analysis should be extracted from the cyber security architecture.
- Risks should be documented, preferably within a risk register, which should be managed, possibly as part of a knowledge management process.
- Stakeholders need to be identified, involved in the process and reported to.
- Risk identification and analyses needs to be done according to a method.
- Standards and guidelines need to be identified to inform risk assessment activities.
- The risk assessment needs to be reviewed periodically.
- Authority and responsibility for the performance of the risk assessment needs to be assigned to personnel.
- Personnel performing risk assessment needs the right skills and knowledge required for their task.
- The CSRA processes should be part of an Information Security Management design and evolution.

5.2 Protocol of Determination

5.2.1 Development Strategy

As is concluded from the results of the comparison of related maturity models, no maturity model concerning information security or CSRA was already build on the needed abstraction level so that it could potentially be used as a framework for the HCRAMM. This excludes an enhancement or combination design as no appropriate maturity models exist to enhance or combine. The maturity model will partly be newly developed and partly transfer useful architectures and content of the compared models. A matrix structure is chosen in which maturity domains (rows) are compared against maturity levels (columns). The cells will be filled with content compliant to this structure.

The maturity levels are based on the maturity levels of the TIMM as these have a proven fit for information security maturity for Dutch hospitals, of which CSRA is an important process. The fifth maturity stage (managed), will be replaced by the fifth maturity stage of the CMMI model as the label optimized better represents iterative improvement, quantitative measurement and steering. In the level optimized the whole CSRA process is optimized as a whole, continuously adjusting to the organization's needs.

The maturity dimensions are newly designed based upon the results of the literature study, the comparison analysis and expert interviews, supplemented by information security, cyber security and risk related content from the compared maturity models.

5.2.2 Maturity Model Development Approach

In Figure 31 an overview of the maturity model development process is provided. The development of the context description follows the same path. The development starts with the theoretical background including the SLR, the comparison analysis and the maturity model comparison. A framework as described in the development strategy is elaborated and the first theory is inserted. The first 13 interviews the information to this framework is added (iteration 0), until an initial maturity model could be formed. Next interviews were used to evaluate the initial context and maturity model, adjust it and evaluate it again. This process was performed four times. An interview protocol (Appendix C) was developed, however this was not used in interviews when specific subjects are discussed with some cyber security expert (e.g. medical devices) and in the validation process. Also during the exploratory interviews already some subject discussed in other interviews were added to the questions. After the evaluation interviews a maturity model version 1 was developed. This was translated into a survey, which in turn was distributed among hospitals. Among the maturity model questions, the survey asked for feedback, which was analyzed and based on the feedback a final version (2) was developed.

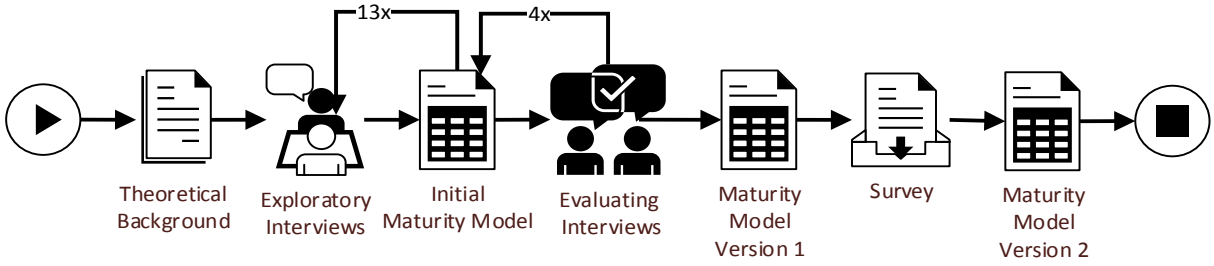


Figure 31: Overview of the Maturity Model Development

The interviews were recorded and fully transcribed, except for interview 6 and 17 as they did not allow recording of the interview. In those cases notes were taken during the interviews. The transcribed text and the notes were coded in NVivo.

To provide a balanced view interviews were conducted with two main groups of stakeholders: the hospital cyber security managers (HCSM) and cyber security experts (CSE). The hospital cyber security mangers are selected based on the criteria that they should be (partly) responsible for the CSRA in a Dutch hospital. This

group provides domain specific information on how CSRAs are conducted within hospitals and in which context these assessments take place. The cyber security experts are selected based on the criteria that they are an expert in the field of hospital CSRA. Depending on their background they focus more on a certain subject, e.g. medical devices.

In total 17 interviews were conducted, of which 11 hospital cyber security managers and 6 cyber security experts. Hospital cyber security managers consisted mainly of information security officers or security officers. One interview was conducted with an ICT managers and one with a head IT auditor. A broad demographic spread is chosen between the hospitals, both in size, type (i.e. academic, top clinic or general) and location (i.e. hospitals in the north, south, middle, east and west of the Netherlands). The cyber security experts were drafted as well from different backgrounds (i.e. government organizations, branch organizations and commercial organizations) and with different specialties varying from cyber security at a technical level to policy level. The interviewee's reference, the interviewee's type of organization, the interviewee's function, the iteration and type of information gathered from the interview for the research and whether the interview protocol is followed are shown in Table 13.

Since most hospital cyber security managers and cyber security experts were not allowed or did not want to be referred to by name and organization name, as provided information may be sensitive, all functions and organizations are generalized. Quotes who are directly traceable to certain organizations are not used or partly censored (names of people or organizations are removed) to protect the main source. The full name, details and transcript however were made available to the supervisors of this thesis.

Nr	Reference	Organization Type	Function	MM Iteration	Protocol Followed
1	HCSM:01	Academic Hospital	Security Officer	0: General Input	Yes
2	HCSM:02	Academic Hospital	Head IT Audit	0: General Input	Yes
3	CSE:01	Security Advisory Firm	Medical Technology Security Expert	0: Specific Input	No
4	HCSM:03	General Hospital	Information Security Officer	0: General Input	Yes
5	CSE:02	Branch Organization	IT Policy Advisor	0: General Input	Yes
6	CSE:03	Government	Cyber Security Expert	0: Specific Input	No
7	HCSM:04	General Hospital	Information Security Officer	0: General Input	Yes
8	HCSM:05	General Hospital	Security Officer	0: General Input	Yes
9	CSE:04	Security Advisory Firm	Cyber Security Expert	0: General Input	Yes
10	HCSM:06	Top Clinical Hospital	Security Officer	0: General Input	Yes
11	HCSM:07	Top Clinical Hospital	Security Officer	0: General Input	Yes
12	HCSM:08	General Hospital	Manager ICT	0: General Input	Yes
13	CSE:05	Security Advisory Firm	Cyber Security Expert	0: Specific Input	No
14	CSE:06	Government	Medical Technology Security Expert	1: MM evaluation	No
15	HCSM:09	Top Clinical Hospital	Information Security Officer	2: MM evaluation	No
16	HCSM:10	Academic Hospital	Security Officer	3: MM evaluation	No
17	HCSM:11	Academic Hospital	Information Security Officer	4: MM evaluation	No

Table 13: Overview of Anonymized Interviewees

During the interviews the main focus was on questions regarding the CSRA process, divided into several main topics, including: general method, assets identification, threat identification, vulnerability identification, analysis and evaluation. Questions about the context in which these CSRA processes occurred such as the hospital (security) culture are added. Finally questions about the context, mainly focused on the threat landscape in which the CSRAs takes place are included. These mainly consist of questions concerning threat, vulnerability and asset types relevant to hospitals.

6 Context Determination

The comparison analysis confirmed that the context determination is an important aspect in CSRA. Since the specific hospital focused scope of this research this chapter will provide a description of the context in which the CSRAs occur in hospitals. As the SLR provided very little information concerning hospital, the expert interviews are used to expand the knowledge of the hospital cyber security risk context, which will be build op from the cyber security risk culture at hospitals, the CSRA methods used at hospitals and the threat landscape of hospitals. This description is needed to understand how the specific context for hospitals is build up.

The expert interviews used to obtain context consist of the first 15 interviews of Table 13, in the last two interviews the focus was fully on the maturity model itself. The interviewees consisted thus out of nine hospital security managers, two medical device security experts (one commercial, one in service of a government organization) and four cyber security experts (two commercial, two none commercial). During these interviews the interviewees were asked among other questions what assets, threats and vulnerabilities ware specific and important to their business and what methods they used to assess their cyber security risks. Next to this many interviewees discussed certain important aspects of the hospital culture relevant for the cyber security and CSRA context. The interviews were recorded and transcribed, from which a qualitative synthesis was extracted considering the culture, assets, threats, vulnerabilities and used methods, leading to a final conclusion considering the context.

6.1 Hospital Culture

The hospital culture is a complex one as many subgroups exist within the hospital all containing a certain form of authority over their own work. They have a large influence in the decisions made by the hospitals. The ICT department or people responsible for information security obtain less status in hospitals and even though hospitals nowadays are becoming more and more digitalized organizations and are becoming heavily dependent on ICT, they still have less influence.

[HCSM:03] "A hospital has a lot of kingdoms. Neurology is historically viewed a kingdom, the laboratory is a kingdom, medical devices is a kingdom and so you have got others as well. ICT is historically viewed not a club with a lot of status in a hospital."

[HCSM:03] "Yes, I believe you could say that in hospitals ICT is viewed easily as a chance to make everything nice, sexy and better, but it is not viewed as a risk area and something that requires serious investments in quality. Because the risks and dependencies are so big. That is a slowly growing process and is often left to the manger ICT."

More specific about information security, health care personnel wants to provide care and do what they believe is the most important, curing people. Secondary processes, which do not seem to contribute to this goal directly, may become overshadowed. Especially if these are of a more abstract nature.

[HCSM:07] "Well look, the subject is off course not something that people are interested in. Let's be fair. People come here to work, to nurse, to doctor, or what else. Not to handle information secure."

[HCSM:07] "Risk is an abstract and complex subject, while the hospital mainly works pragmatic. That is difficult to combine."

And although accessibility and integrity of information are often found important by health care personnel, as this touches the care for their patients directly, the confidentiality of information is less prioritized and viewed as less important especially if it seems to conflict with their direct priority of providing the right care to patients.

[HCSM:03] "When you talk about the impact side of the scenario, you will mainly look at accessibility and integrity and privacy, but privacy is not popular in the healthcare. You could say that everybody thinks it is important, but the care is more important. Thus when a choice needs to be made in the healthcare, are we

healing the patient or do we respect his privacy, then we always heal the patient. And that mindset is really strong, thus we look with high priority at availability and integrity of information. The confusion to privacy as priority is constant and everywhere."

[HCSM:05] "Well, privacy is thought to be annoying in the care. A familiar story in the care is: more people died of too much privacy then a lack of it. Thus if I am allergic for a medicine and you provide them that medicine, because you do not know, than that is worse than if I would know by accident that you are allergic for that and I do provide you with the right medication. Thus in the care, and that is the case here as well, we understand the necessity to deal with that, but we see that it has cons and dangers as well. Aside from the fact that we have all those regulations and how to implement them. That is very difficult."

For non-care personnel this seems to be less the case and they seem to put more priority towards full information security.

[CSE:04] "We did NEN 7510 assessments. As well as complete NEN 7510 activities, thus every chapter, but more like we should be compliant with the NEN 7510. We got the instruction of the IGZ, so we should comply. But not from an intrinsic motivation to become more secure. That is my general view. It is more an obligation. And I have been on the administrational side as well as on the care side. And you notice that the administrative side wants everything in order, the human resource system, the financial system. All the processes behind it. That is often done fine. Within the care side it is more like we need to deliver care and the security is second. You need to mainly help patients fast. They do not worry that much about the confidentiality of information. They believe they settled it with their code of profession and all. Considering the digitalization of hospitals they are worried about the integrity of information."

The priority that the board of directors of hospitals attribute to information security seems to differ strongly per hospital. However with the new European privacy regulations coming up an increased amount of priority seems to come up as the liability of the board of directors is strongly increasing.

[HCSM:04] "Yes and it has certainly woke up the directors. They are terrified, because suddenly they have become severally liable. Well, back to the commercial sector. There it was already the case. En we saw that several top directors were fired for that reason. Mismanagement was suddenly punished hard."

6.2 Methods Used

The interviewees were asked what kind of cyber (or information) security risk assessment method they used to identify their risks. In Figure 32 an overview is given of the used methods.

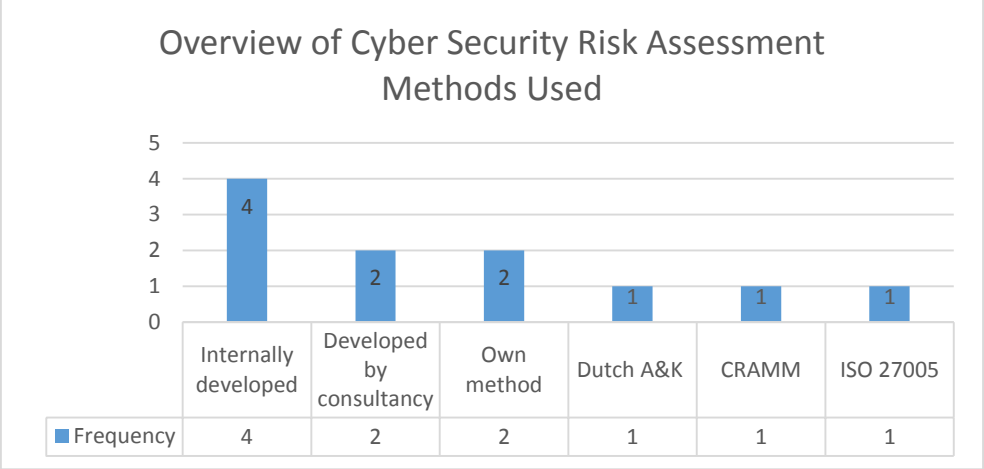


Figure 32: Frequency of CSRA Method Used

In the hospital sector there seems to be no standard method used. Only three of the eleven hospitals use a wide spread proven method (i.e. Dutch A&K, CRAMM, ISO 27005), although even the ISO 27005 could be viewed more as a framework, as it does not provide a wide variety of detailed stencils and other tools to

support the risk assessment process. Also the hospital who used CRAMM indicated that they stopped using CRAMM as the organization was not ready for it yet:

[HCSM:09] "It was, how shall I say this, a little too much for us. For us from information security, because we are certainly convinced and we are certain… But the organization just is not ready yet."

Two methods were developed by a consultancy, which did a risk assessment once, and the hospital continued to use the methods. Four methods were developed internally often based on other methods, which were not necessarily related to the information or cyber security domain. And two methods were methods developed by the risk assessor themselves, based on past experience and methods used in the past. And even though some methods may be more sophisticated than others, they all are conform the NEN 7510 guidelines. The most often named reasons why the used methods were chosen was because the risk assessor or hospital already had experience with the method or the method was already in place before they came.

6.3 Threat Landscape

During the semi-structured interviews the interviewees were asked what they saw as important assets, important threats towards these assets and hospital (domain) specific vulnerabilities, which in this case can best be described as common problems in the hospital sector. The assets, threats and vulnerabilities together form a domain specific threat landscape.

6.3.1 Cyber Asset Groups

Hospitals can have hundreds of different cyber assets. For the scope of this research it is not relevant to identify them all and thus they are grouped in the most relevant cyber asset groups. Viewed from a high level perspective hospitals have three tasks: healthcare, education of new care professionals (mostly conducted at academic and top clinical hospitals) and research (mostly conducted at academic hospitals). The important cyber assets come forth from these processes or support these processes. In Figure 33 an overview is given of the sources and references that mention the assets.

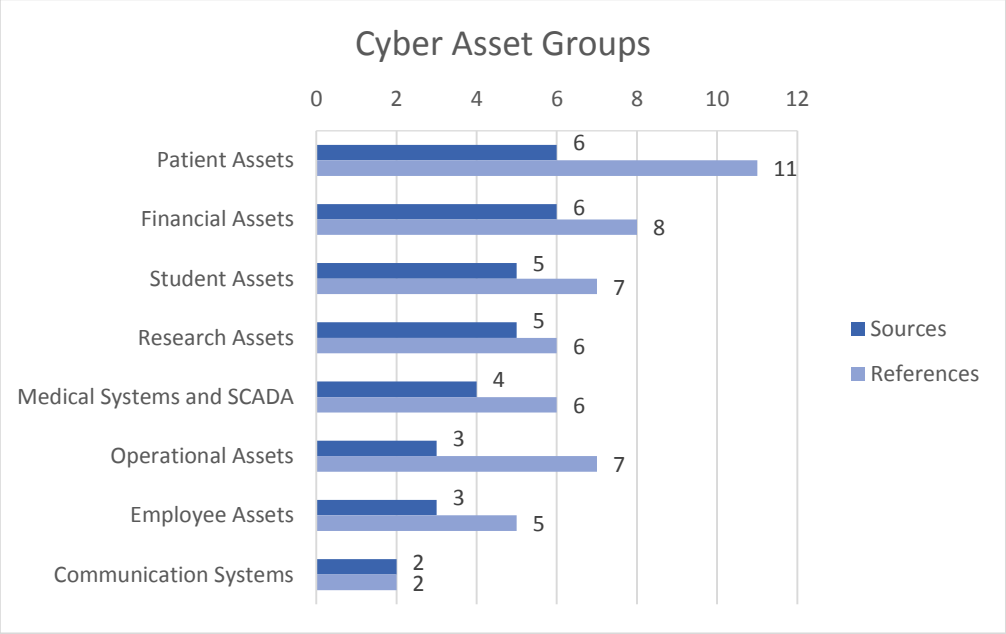


Figure 33: Cyber Asset Groups

In Table 14 a mapping is provided how the initial cyber asset groups, identified in the literature research, evolved to the final groups. In the third column it is specified whether in this chapter the asset group during the interviews is identified, extended, rated as a non-relevant asset or added to other asset groups. For infrastructure this is the case as all the other asset groups have specific infrastructure they use.

Initial Asset Groups	Final Asset Groups	Specification
Financial Assets	Financial Assets	Extended
Medical devices	Medical Systems and SCADA	Extended
Patient Assets	Patient Assets	Extended
Employee Assets	Employee Assets	Extended
Infrastructure	-	Included in all other assets
	Student Assets	Rated non-relevant
	Research Assets	Identified
	Operational Assets	Identified
	Communication Systems	Identified

Table: 14 Cyber Asset Groups Specification

Patient Assets

Hospitals contain large amount of patient data consisting of details about the patient and his medical records and history, as well as software and hardware to process these. There seems to be consensus that this asset is the most important as this is the backbone of the main process of hospitals and cannot be missed for a long time. The accessibility, integrity and confidentiality of these are all of high importance:

[HCSM:07] "Patient data is the most important."

[CSE:02] "Well, the most important processes are healing the patients. And in those cases you have acute cases and less acute cases. Ehm, acute is when the intensive care, but also the in the operation rooms. So you need to act fast there. Patients on the IC that, and you suspect something and you take some blood for testing, in those cases we are almost fully dependent of ICT. A little is still possible, we can remain a little while without ICT, but after a while the whole system will collapse."

[HCSM:05] "…If we think about the protection of data, the primary focus lays on patient data, because I would dislike it very much if my personal data are in the open, what I earn, but actually that does not bother me at all personally. For a patient however it can be very bothersome that his illnesses… So we do not want that. And especially not if the data is altered with consequences. If the salaries are altered by a nice hacker, well, after a month we will have it corrected."

[HCSM:01] "Healthcare contains as asset care data of all patients, that are somewhere near the one million I suppose. And that data is stored in our vaults. That is not showed in a window. That is done because of the confidentiality, because healthcare, is based on trust. The moment that you feel like what you tell your doctor does not remain between you and the doctor, and in this case you need to view the doctor as the system the doctor is using, in that case you will not tell everything anymore to the doctor. And at that point the doctors will complain that they are unable to do their job."

Financial Assets

A core asset of every organization, financial assets consists of all invoices, payments and financial administration data, systems and the hardware containing it. This asset is especially sensitive to fraud by insiders. Although for cyber criminals it is interesting as well to gain access to financial data and systems. The altering of payments in financial systems is a direct way to obtain money from fraud and hacking activities. As most healthcare systems contain some sort of financial aspect, de financial systems are often linked to these [HCSM:05]. But although financial systems may seem very interesting for threats, they are one of the most protected systems as well concerning cyber security. This includes mandatory yearly IT audits. These IT audits often include the most important IT systems they are connected to, as is illustrated by the following:

[HCSM:09] "We have an IT audit from <…>, they do the finance, but they also look at the finance that are running on IT systems and they distinguish your most important IT systems and do an audit on them."

Student Assets

Student assets, mainly the student grading data may seem important for hospitals with a teaching task, which is the case for academic hospitals, top clinical hospitals and to a lesser extend general hospitals. However all

hospitals, including the academic hospitals, indicate that they are not the main responsible for the student data. Marks and such are stored at the educational institutes the students are affiliated with and often not or possibly not stored in the hospital, which means they are not directly responsible for the protection of this asset type.

[HCSM:05] "I do not know where, but they are not saved in our systems. They are saved in educational systems."

[HCSM:02] "There is one educational system and that is stored at the university."

[HCSM:07] "I would not know, I suppose so. <…> I am not sure about that process. Interns will be rated en they will get a mark and if it is stored here or there, the latter one of course, and if it is stored her, I do not know."

Other personal data concerning interns, e.g. name and address, is marked as employee data.

Research Assets

As research is mainly conducted at academic hospitals, in a lesser extend in clinical and barely in general hospitals the importance of this asset is viewed as such. In general hospitals they often do not possess research data and systems, when research is conducted it is usually in collaboration with an academic hospital and in most cases the important data is stored there. Top clinical hospitals might conduct some research, but especially academic hospitals have research data which might prove interesting from an economic or scientific point of view. This is illustrated with the following quotes:

General hospital: *[HCSM:08] "No there is no research done at us."*

General hospital: *[HCSM:05] "No we are a general small hospital, so relatively few. We work together with the <…> hospital, so we have those people here. But our hospital is not fit for research."*

Top clinical hospital: *[HCSM:07] "It depends what you define as research of course. We are not an academic hospital, we are a top clinical hospital. We have a lot of doctors in training here, they perform some research, but that is different than in an academic hospital."*

Academic hospital: *[HCSM:01] "Private organizations could be, since we have a lot of material, which is very interesting for the pharmaceutical industry. It takes a lot of time and investments to develop a new cure, when you can get that partly by stealing the data, it would save you a lot of money. They could for example hire a Brazilian to steal the data and who diverts the data through Middle America and sells it. Then they can say they gained it in a fair way. "*

Operational Assets

Operational assets is an umbrella term for all remaining data, system and hardware types needed for hospital operations. This kind of asset is not often targeted as the economic value of it is low. However if the data is not available anymore or altered the hospital might face problems. Also some operational data should remain confidential for safety reasons. The main identified types of operational assets were schedule data and chemical, biological, radiological and nuclear data (CBRN). Without schedule assets and related systems it might become difficult to maintain operations and a switch has to be made to old fashion scheduling. CBRN data may especially be interesting for hacktivists as they might want to attack such for ideological reasons. This kind of data is especially found at academic and top clinical hospitals.

[HCSM:06] "The CBRN, chemical, biological, radiological and nuclear safety <…> We have permits for quite some stuff, that does not say it is all around here, but we have a permit. And we have some of that stuff as well, isotopes, we do enrichment and that kind of activities."

[HCSM:02] "A farm or as we call it a laboratory animal center. A nuclear power plant, we have our own nuclear power plant, because we make radio-isotopes for research."

Medical Devices and SCADA

Although the main asset of medical devices consists of patient data, their control software are identified separately since altering this might harm people or objects in the physical world or could deny people to medical treatment. Supervisory control and data acquisition (SCADA) systems fall in the same category of systems that have a direct link with the physical environment and failure or unwanted change of functions could potentially harm people and the environment. An example of such was given by a security manager:

[HCSM:08] "We have those (SCADA) mainly for medication, for example were the temperature could be important. That is in a device and that medication should be used under certain conditions. Or when it should be stored, then it is monitored, so it is measured. Equipment, it should work well, such as air-conditioning, but you talked about air pressure as well in isolation rooms, etcetera. That is possible if someone has a nasty infection…"

Awareness of possible impacts of medical devices and SCADA systems is increasing. Especially since the impact might be very high on patient and general human safety, one of the most important impact aspects, penetration tests are needed [CSE:03]. However the amount of awareness for this kind of assets is still small. As illustrated by the following security manager:

[HCSM:05] "We see it, we deem the change small, or we do not look at it at all."

Employee Assets

Even small hospitals are organizations with a lot of employees. Of those employees personal data is stored for all kinds of reasons. Often mandatory by the government. This kind of personal data could be used for all kinds of identity theft:

[HCSM:06] "Identity theft is for me probably one of the largest threats, because we have quite some here. Complete citizen service numbers, name, address, gender, etcetera. And we have almost complete all bank accounts somewhere, so we are pretty complete concerning that. And of employees, if you ask what we have of those, we have copies of their passports, etcetera."

Also some employees might hold functions that are resented by certain types of activists. Especially in academic hospitals where experimental research is done:

[HCSM:02] "And for example healthcare employees have functions here, that the outside world should not know about, since it is threatening. Lab animal caretakers, against activism. Those people who create radio-isotopes, well you have to keep that secret as well, they may have a risk of activism as well."

Communication Systems

Communication systems include websites, internet portals, e-mails, internal communication systems, etcetera. Depending on the type of system the healthcare could become reliant on it. In increasing amount hospitals are trying to unburden or automate communication with for example patients. Some hospitals stay away from it for now, others are increasing their capacity:

[HCSM:02] "One thing that is nice add to that, we use a DigiD driven communication portal for the communication with patients for one department. And this year more will be added."

Although containing many advantages for both customer ease and more planning efficiency at hospitals, a risk considering the implementation of such communication systems is the dependency on them. If they are down because of for example malfunctions or DDoS attacks, a back-up plan should be available. This is also the case for internal communication system that have become more and more IT related as is illustrated by the following quote:

[HCSM:08] "And telecommunication, since that is IT as well nowadays, 9 of the 10 times. And with us if we miss or are not reachable by phone, that is of course a different cup of tea than here at the <…> office. But reachable by phone at a nursery department or a specialist, or the reachability of a reanimation team, that are all cases you should put extra effort in to make sure it works."

6.3.2 Threat Profiles

Interviewees were asked what they viewed as the main threats concerning the electronic assets in hospitals. In almost all cases they seemed to reason from the treat actor, which is why the threat is depicted as such in Figure 34. However threat actors contain a certain motivation linked to preferred asset types, preferred methods to approach the asset and a skill level, which describes a full threat profile. Not all possible threats are included, threat profiles are created from the most important ones and depicted in this sub-chapter.

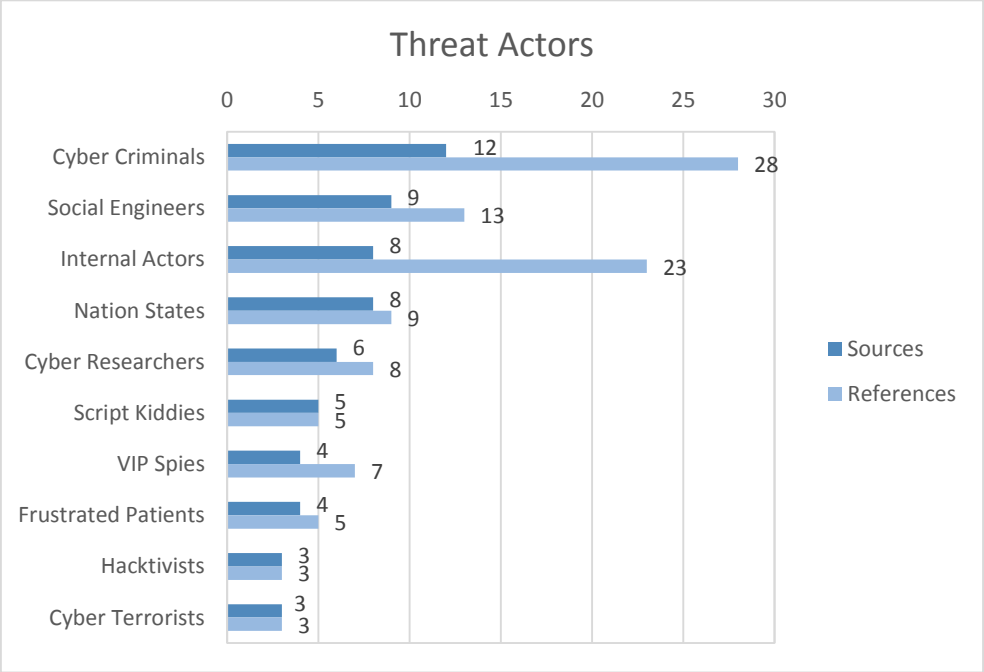


Figure 34: Threat Actors

Most actors from the literature research were recognized or came up as threat actor during the interviews. A mapping is made in Table 15. Private organizations however were not recognized as a direct threat. This may still prove to be a threat for hospitals, but they will most likely hire other threat actors, such as cyber criminals or social engineers, making the need to identify them as separate threat obsolete. Cyber terrorists were identified, but all experts who mentioned this threat actor agreed it did not posed a threat for hospitals at the moment of research. The no actor was out of scope as mentioned before. Two new actors were introduced: VIP Spies and Frustrated Patients. For all the in the interviews mentioned threat actors, their whole threat perspective is described in detail, based on the previous literature and information gathered in the interviews.

Initial Threat Profiles	Final Threat Profiles	Specification
Nation States	Nation States	Specified
Cyber Terrorists	Cyber Terrorists	Non relevant threat
Cyber Criminals	Cyber Criminals	Specified
Script Kiddies & Cyber Vandals	Script Kiddies	Specified
Hacktivists	Hacktivists	Specified
Cyber Researchers	Cyber Researchers	Specified
Private organization	-	Not identified as separate threat entity
Social Engineers	Social Engineers	Specified
Internal Actors	Internal Actors	Specified
No actor		Out of scope
-	VIP Spies	Domain specific
-	Frustrated Patients	Domain specific

Table 15: Threat Profile Specification

Cyber Criminals

Cyber criminals are often technically well skilled and have financial motives. Since their motives are financial they often have business models such as taking data or systems hostage, selling data and adding clients to a botnet which can then be exploited. There methods to achieve their goals are roughly divided in malware distribution and hacking. Often this malware might not be targeted directly at the hospitals specific, but targeted in general or spread from other sources [CSE:03, HCSM:03]. Or as is demonstrated by an example:

[HCSM:04] "Well, last year we had that large outbreak at municipalities as well, I don't even remember its name. Well that has crashed a lot of administrative systems. Well the healthcare was sucked into that as well."

Two examples of malware in hospitals with easily identifiable financial gains are given in the following quotes:

[HCSM:07] "By the way, last year with the Dorifel virus, they reported us properly that we were infected…"

[CSE:02] "Yes, we just had a nice example of such, that is, another warning went out. At a certain moment your computer would be locked."

The Dorifel virus was used to steal bank details among others. The second quote explains a form of ransomware, malware in which your data or systems would be taken hostage by encryption and a ransom would be demanded. This action can also take place through hacking:

[HCSM:07] Well, you could imagine that if an important person is threated here, you might want to blackmail that person or something. <…> Or you might want to blackmail the hospital. Hey hospital, your data is confident, but I still have it, I would like a half million for it and then I will return it."

[HCSM:05]: Of course you have criminals that hack a database and don't release it until you pay an x amount <…> We think that is very inconvenient. And we looked at that, but we assessed the likelihood of something like this happening reasonably low."

Increasingly malware is detected on medical equipment as well:

[CSE:01] "Yes I did a couple of assignments in the area of medical devices. Like MRI scanners, echo scanners and that kind of equipment. <…> A few doctors complained that those things were infected with computer viruses."

[HCSM:03] "Last year they did some research and they found a lot. If you look at virus outbreaks in hospitals in the recent history they were mostly almost connected to medical devices. The persons responsible for the medical devices do not have knowledge about operating systems."

Medical devices seem to be quite vulnerable to malware attacks. A large part of the problem can be found in the recent connection of medical devices to the hospital network. These networks are not always aggregated enough [CSE:05] and often the contract with the suppliers prohibits the use of virus scanners on the medical devices [CSE:01]. The reason behind malware attacks on medical equipment is demonstrated by the following:

[CSE:04] "You see, a hospital contains a lot of equipment. If you take these over, you will gain large amounts of computer capacities. Which you could use for DDoS attacks. <…> Hospitals are usually not the most secure environment and it is relatively easy to enter them and create a botnet."

[CSE:04] "I know of a hospital, some time ago, that indeed was part of a botnet."

The connected and not well secured medical equipment provides an interesting target in this case. The change to be part of a botnet might differ from hospital to hospital, depending on their security. As the impact is not necessary high the risk of such is not seen as large:

[HCSM:09] "If we are part of a botnet, I would not know that, but I do not think that is the case. Because I saw too few symptoms of such. <…> I do not few that as a large risk.

In general the experts seem more wary for hackers as is demonstrated by the following quotes:

[HCSM:08] "…I think at us it is mostly the opportunity hacker. They are scanning for vulnerabilities and we are found, I mean hospitals."

[HCSM:09] "Especially that openness itself, that story at the moment, the IRS in America that was plagued, that a part of their server, some space, was misused for hacking purposes, well, then you are able to commit all kind of tricks, so to speak. And that already happened in 2012 and they just came with that and we as well are just starting to act. So you just do not know everything."

[HCSM:08] "The hacker and concerns about privacy. That are the largest threats for me."

[CSE:02] I think if I worry about something and if I take a week to immerse myself in hacking then I should get quite far. And as an organization you should arm yourself against that."

[CSE:02] "I, look, it is tried. Take for example the national switching point. I was closely involved in that, I don't have numbers, but there were dozens of people that have tried to hack that thing and went there on purpose. They think that is interesting. For hackers that is a big prize."

Threat profile Cyber Criminal	
Motive:	A cyber criminal is motivated by financial gains and will mainly target assets enabling him to turn into an economical benefit.
Methods used:	Often used methods of cyber criminals are the distribution of malware and hacking into systems and databases connected to the internet. They may be situated close to the target or on the other side of the globe.
Skill level:	Depending on the background cyber criminals might have medium to highly technical skills. In some cases the skills of other threat actors might be bought.

Social Engineers

The social hacker is a form of cyber criminal that uses the vulnerabilities in human psychology rather than technical vulnerabilities. As hospital employees often are not fully aware of social engineering methods they provide a convenient entry towards the hospital's assets.

[HCSM:08] "That happens a lot <…> That is where you see the human aspect, that humans should be aware of that.

[CSE:04] "They are not aware that a large part of the danger lays at the user itself and not within the technique. So awareness is an important issue at hospitals."

Method may vary from direct methods in which the social hacker tries to bluff its way into the organization in order to gain access towards assets, specified online methods in which specific targets are approached through online channels and diffuse online methods where large mass e-mail messages asking for credentials are send to unspecified users. Some examples of methods used where given:

[CSE:02] "Social engineering. Somebody with a laptop enters and says I am here for the maintenance of this machine. He just connects and there you go. The awareness of employees is very important. Today they receive training in customer friendliness and helping people in a fast pace and tomorrow they receive training in customer unfriendliness. Someone says I am here for my mother to collect her patient files. And you just receive them…"

[HCSM:02] "That is that all kind of different companies on technical servicing, in name of telecom providers, want to visit you and inspect your equipment. And that happens at the <…> as well that unknown companies present themselves, that thus come to check your telecommunication equipment."

[CSE:04] "If you look at spear phishing and all the possibilities to seduce people to click on links, that has become increasingly easier."

[CSE:04] "When you send an e-mail for a meeting with the minutes, where people can easily click on it. Click on the link to download the minutes and, well, sometimes you can try to find out there username and password in the background."

Threat profile Social Hacker	
Motive:	Social Hackers are financially driven. Their main business models are to gain access to valuable hospital data such as patient data and employee data and sell these, gain access to financial systems and redirect financial flows or collect passwords to communication systems such as e-mail and use them for spamming purposes.
Methods used:	Social Hackers use social engineering methods both online and offline to gain access cyber assets. For this they use access to publicly available information about organizations and its employees, such as social media, to build a trust relationship.
Skill level:	Social Hackers possess a low to medium technical skill level, but a medium to high skill level in social engineering.

Internal Actor

The internal actor is by most of the interviewees seen as one of the biggest threats. Often the internal threat actor is an employee and by most interviewees it was viewed as a large threat as is demonstrated by these quotes:

[HCSM:05] "The largest threat so far is still our employee. He leaves things open, or mails them outside. All that kind of behavior."

[HCSM:06] "That is the largest threat. That is really the largest threat. And when you take a USB stick and you start extracting a database or a research report then it is lost and I could say that it is not allowed, well…"

Since he is already past the first line of cyber defense the impact of this threat might prove to be large:

[HCSM:04] "Intern we have incidents as well. Somebody that inserts an USB stick in the system and half the hospital is shut down, that is a realistic incident."

The threat of an internal actor may emanate from several causes, such as the lack of awareness :

[HCSM:08] At the employee. The awareness of people in the domain of security, how should you handle information and patient information."

[HCSM:09] "The sharing of information with external organizations, the exchange of information. And at one hand that is work related, thus the doctor who asks for a second opinion from a doctor at a different hospital and he does that through e-mail."

The lack of compliance to security standards or lack of security standards itself:

[HCSM:01] Well, such a threat I have here, is for example employees who do not comply with procedures, guidelines and standards, is something that often comes up. Or even the lack of guidelines and standards. So for example I would like to set up a server the right way, but there are no rules for this. And I just do it as I think is best."

[HCSM:02b] "If they buy a hard disk at the Mediamarkt and save the data on it, that is possible of course, and we do not see that. Maybe we advised them to save the data on the central disk, but if they buy something themselves and save it on that, that is possible of course."

[HCSM:04] "Well as you probably heard often, from the inside the most mistakes are made. These are mostly in attitude and behavior. The culture in the care is still one that thinks lightly about risks that in occur in practice and the people involved with the core task care are not able to think of threats outside their care task or the hospital. That is some ignorance, naivety even."

[HCSM:02] "Somebody who secretly takes a file with user IDs and passwords, because he wants to take another look at them, if the structure is well set. En then on accident he leaves them in the train. Well, that happens with us as well, all these kind of simple accidents."

Although in most of the above mentioned cased the internal actor is more a vulnerability of the organization. From a more threat like perspective, the internal actor might contain malicious purposes such as revenge:

[HCSM:08] "I think, that when you talk about frustrated people then mainly the ex-employees are a big risk. Sometimes you need to say goodbye to someone in a less pleasant way. We are careful in that, that they should hand in their keys immediately, while accounts are blocked. We already do that when they walk out the door."

Also financial fraud is a cyber risk hospitals should be aware of [HCSM:03] as well as selling valuable research data [HCSM:01]. Often Employees do not have high IT skills, except for the IT department, they however know the systems and structures in the organization very well and can use that in their advantage if they mean to do harm [CSE:02].

Threat profile Internal Actor	
Motive:	Internal actors often could be seen as a vulnerability, having a lack of motivation or awareness. However intended threats coming from an internal actor are mainly revenge and financial gain.
Methods used:	Internal actors have internal access towards assets, which enables them to get around primary defenses. From the inside miscellaneous attack methods are used.
Skill level:	Low IT skills, but highly knowledgeable of internal systems and structures.

Nation States

Nation states deploy state sponsored hackers and malware developers to either obtain political advantage, obtain economical advantage or propagate an ideological mindsets. They use a variety of methods including sophisticated malware using zero-day attacks, which are malware that exploit still widely unknown vulnerabilities in software. There is often no answer to this kind of malware, making them very dangerous [HCSM:04]. Furthermore they seem very persistent once interesting targets are locked, leading to the term Advanced Persistent Threat (APT).

Obtaining political advantage can be done by espionage activities such as are carried out by the American NSA. Specifically for this type of threat most experts either believe that organizations with political motive such as the NSA are not a problem for Dutch hospitals and they are too technological advanced to protect yourselves against them. Also the assets of hospitals might not be interesting enough.

[HCSM:03] "You should wonder if the NSA is a problem. What kind of problem is the NSA for medical information in the Netherlands. Tell me."

[CSE:02] You know that if you are connected to the internet you have certain risks. And the NSA can always enter. Do not fool yourself."

Nation states that would like to carry out ideological mindsets by for example defacing websites or shutting down important infrastructure mainly seem to focus on sectors with high visibilities such as journalistic websites, banks and telecom [CSE:03]. Hospitals do not seem to be a direct target of these hackers.

The main risk for hospitals is the economic motive. Considering hospitals mainly Chinese state sponsored hackers are active. Their aim is on information and intellectual property possessed by academic hospitals and research done by hospitals. But they will also target information about medical equipment [CSE:03]. This seems to lead to a distinction in threat profile between general, top clinical and academic hospitals. The general hospitals contain little interesting information for this type of threat. Top clinical hospitals are more advanced, use new and experimental procedures and equipment and sometimes participate in research. Academic hospitals invent new procedures and equipment and have a lot of research and intellectual property. During the interviews these kind of reactions were typical:

General hospital: *[HCSM:08] "I do think it is a risk, but not for us, we are not an academic hospital."*

Top clinical hospital: *[HCSM:05] "Nah, states are not, I do not think that."*

Academic hospital: *[HCSM:01] "That is a concrete threat we have as knowledge institute."*

One hospital security manger of a top clinical hospital tells about an incident he encountered:

[HCSM:06] "We had one issue here and we solved it. Something witch was new and what indeed contained intellectual property. And that was solved with patents and those kind of things."

Threat profile State Sponsored Actor	
Motive:	Concerning Dutch hospitals a threat is active from an economical or political motivated state sponsored actors, which may be very persistent.
Methods used:	A combination of methods to enter hospital systems and often use zero-day attacks to install forms of spyware to obtain research data or intellectual property.
Skill level:	State sponsored hackers are often well educated, organized and financed.

Cyber researcher

Cyber researchers are often highly skilled people affiliated with cyber security research centers, universities, media or commercial cyber security. They mainly want to test systems for security, for ethical or scientific reasons, but sometimes possess an economic motive as well. Examples of cyber researcher activities are given with the following quotes:

[CSE:01] "A German researcher Florian Grun, Grunwel… I do not know his name exactly. He showed that it is very ease to hack a heart monitor. And he programmed that heart monitor in such a way that it would not alarm the doctor until you had a heart rate of 30.000."

[HCSM:09] "We just had a journalist once who found a hole and then it became front page news."

Opinions whether or not they are specifically targeted by cyber researchers vary:

[HCSM:01] "The same counts for cyber researchers." (We are not a specific target for them).

[HCSM:02] "Yes, of course what would you expect with a faculty in beta science were people are educated in IT, yes we have those. And just this week we had a discussion how to handle those cases. So we are busy writing policy to coop with that. What should you do with people who say that they try to hack your system for ethical reasons?"

[HCSM:06] "From information security perspective, from the market privacy is an issue that is in the newspapers every day with all kind of examples. When something happens, you will be in the newspapers tomorrow."

Of the different types of cyber researchers, journalist seem to have to most impact as they often expose the vulnerabilities or incidents to the largest group of people. Journalists often are less skilled then other types of cyber researchers, but make up for that by involving more skilled cyber researchers in their research.

Threat profile Cyber Researcher	
Motive:	For ethical and scientific reasons sometimes intertwined with an economical motive.
Methods used:	Cyber researchers develop own malware and use creative hacking methods to find vulnerabilities in systems.
Skill level:	Cyber researchers are medium to highly skilled depending on their background.

Script kiddies:

Script kiddies are individuals that try to attack systems to see whether they are able to. They gain satisfaction when they successfully break in or shut down a system. Opinions about them are very divers. As their skills are relatively low the hospital will be, depending on their basis level of security, relatively well protected against them:

[HCSM:09] "Well, if you look at the layers in our network it is difficult to break into it, you will need to be top notch. Script kiddies have a high copy past grade. The analytical abilities of that kind, of that group, I am not that impressed by that."

On the other side, not all hacking methods and malware on the internet are simple. For example more advanced malware can be bought and thus hospitals should be wary of that:

[CSE:04] "Yes, script kiddies, as in botnets. Hospitals are more and more aware that you do not need a high level of expertise to do a lot of damage."

Also not all hospitals might be that well protected. In a hospital it was possible for script kiddies to hack a radiation device and remotely control the device [CSE:03]. And finally hospitals might not be the most interesting target for script kiddies, who might be more interested in targets that they believe are unethical or highly visible.

[HCSM:01] "We do not encounter cyber vandals and script kiddies often, because hospitals are not really interesting to them."

Threat profile Script Kiddy	
Motive:	For fun and as demonstration of their skills.
Methods used:	They often use online available methods, scripts, malware or simple DDoS attacks which they tweak to use for their purposes.
Skill level:	Relatively low, containing a high copy paste level.

VIP Spies

VIP spies are people interested in the health status or whereabouts of specific people. VIP spies can be divided into two main groups: tabloid journalists and criminals. The first group is mainly interested in publishing information about celebrities for economic purposes:

[CSE:04] "…An example of a famous Dutch person or a famous person who is in the hospital, to obtain some information about him, like, okay, what is the matter with him."

The second group is motivated by revenge or fear and wants to use the information to liquidate a certain person:

[HCSM:06] "Yes, we have protocols for that. Those people are anonymized. We regularly have to deal with those cases since a prison is in our region and people that are in that prison that mostly more famous criminals, they visit this hospital from time to time. <…> We had incidents that people were shot and they survived and people came to visit them to literally pull the plug to finish the job. And that is more easy when you know in which room you have to be."

Since these VIP spies usually do not have high cyber skill levels and the do not form a large threat to basic cyber security of hospitals their main aim are vulnerabilities in employees, which they exploit by using social engineering methods:

[HCSM:09] "Ehm, they will not find out through our system, because our system, and at more hospitals, we anonymized it well. It went wrong one time, when data was leaked, but we learned of our mistakes. And it was in the news then as well when a so called physiotherapist of the football club <…> who was able to obtain personal data of a famous football player."

Threat profile VIP Spy	
Motive:	VIP spies are depending on their target motivated by either economical or revenge and fear motives.
Methods used:	VIP spies use social engineering methods both online and offline to gain access to personal data of VIPs.
Skill level:	Often they possess medium social engineering skills and low cyber skills.

Frustrated patients

Patients or family members of patients that feel that they are not treated well or feel they are let down in some way could get frustrated with the hospital and become motivated to harm the hospital. This is illustrated by the following example:

[CSE:04] "The frustrated patient and family members and those want personal data from doctors, that kind of things. <...> I had one hospital that was in <…>, they gave that example. And I do not know what happened, but there was a frustrated patient. And there was a gypsy family behind it, or at least a criminal family. And those wanted to complain to the doctors. And those are, it was not really a break-in, they just went in a room and sat down behind a working space that was unlocked. To obtain that kind of data."

However at most hospitals they do not believe the threat is large for cyber assets, since it can either be mitigated or is not targeted primarily at cyber assets:

[HCSM:09] "If I look at a patient I do not see any significant remaining risk. No. Not, no. You know we also use Linked-In, or what am I saying, Twitter I mean. As hospital and patients let off steam there and how bad the

hospital is and those are all taken care off by the department of communication and those contact the patients, so that is canalized well. So we are well prepared for those cases."

[HCSM:08] "I do not think so. If it happens, with patients, what you often see is aggression of patients that need to wait long or those that are not satisfied with the treatment. Ehm, those, that, the aggression or the anger is often manifested in a more primitive way than a sophisticated attack against the hospital, it is more against the first person wearing a white suit and then verbal or physical abuse. We put a lot of effort in that, so how to deal with aggression, we have courses for that. But there is no found relation between this kind of attacks and information security as far as we know"

However it should be taken into account that destructive methods such as DDoS attacks are easily bought on the internet, providing a more patient and persistent frustrated patient with possibilities to unleash their frustration.

Threat profile Frustrated Patient	
Motive:	Frustrated by hospital related let downs considering them or their family and friends.
Methods used:	Frustrated patients often use locally at the hospital present possibilities to attack, such as unlocked computers or even stealing computers. More patiently attackers could buy easily available attack capabilities on the internet, such as DDoS-as-a-Service.
Skill level:	Frustrated patients often possess low skills.

Hacktivists

Hacktivists are activist hackers, motivated ideological against ideas such as animal testing and nuclear research. A clear distinction can be made in the threat level between academic hospitals and other hospitals, as often only academic hospitals contain such research facilities and are targeted by hacktivists:

Top clinical hospital: *[HCSM:06] "I see that as a very low risk. I rate that as hacker. And there are no indications, or they are not in the news. But indeed if we had really sensitive business like animal testing, but no we do not."*

Academic hospital: *[HCSM:01] "Hacktivists are a mediate threat for us. And if it is a threat it is because we do animal testing on a small scale."*

Academic hospital: *[HCSM:02] "We do not perceive a lot of attacks. You might say they do not stand out. But it happens a couple times a year that it happens. I just had some reports from the university side, I will get the hospital side next week. Well in those cases you talk about 4, 5 signaled incidents. That does not say it was only tried 4 or 5 times, because if you do not see it, you do not register it."*

A typical method is to disrupt the research facilities by hacking systems and deleting research data or publishing it. Especially when research might be ethically sensitive this could harm the image of hospitals.

Threat profile Hacktivist	
Motive:	Ideologically opposed to activities such as animal testing and research and production involving biological or nuclear activities.
Methods used:	Methods used by hacktivists are usually disruptive. They try to hack into systems and delete data or enable denial of services. Also publication of ethical sensitive research data are used methods.
Skill level:	Often they possess low or medium hacking skills.

Cyber Terrorist

Cyber terrorist are ideological driven threat actors focused on destruction for their cause or obtaining attention for their cause. They are terrorists that specialized into hacking and malware development methods instead of physical violence. And even though this actor was mentioned several times, all actors agreed that is was not an important actor considering hospitals.

Threat profile Cyber Terrorist	
Motive:	Ideologically driven against certain states or cultural aspects.
Methods used:	Methods used by cyber terrorist are often focused on the disruption of systems or obtaining attention for their cause by methods such as the defacement of websites.
Skill level:	Often they possess low or medium hacking skills.

6.3.3 Vulnerability Trends

The interviewees were asked what they viewed as important vulnerabilities specifically for hospitals. These vulnerabilities are not on the detail level as are used in CSRA methods, but rather describe, from a more high level perspective, the security problems that hospitals deal with concerning their cyber security, which lead to vulnerabilities on a more detailed level. Therefore they are referred to as *vulnerability trends.* Hospitals should check whether effects of these vulnerability trends are present at their organization and whether they are mitigated properly. An overview of the vulnerability trends is given in Figure 35.

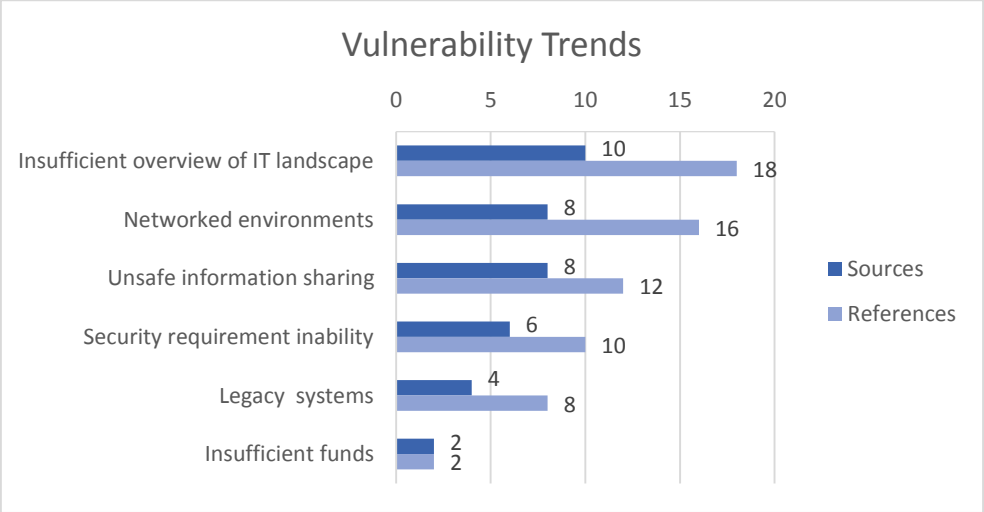


Figure 35: Vulnerability Trends

In Table 16 a mapping is made showing how the final vulnerability trends evolved from the initial ones. The initial vulnerability trends appeared to be very basic and focused on general trends. In the final vulnerability trends it is clarified how it affects hospitals and what the effects of these were, specifying it towards a lower abstraction level. In the third column of Table 16 a statement is made about the type of change the vulnerabilities underwent. They were either identified, specified towards the hospital domain or extended, which means the initial trend was elaborated upon.

Initial Identified Vulnerability Trends	Final Vulnerability Trends	Specification
BYOD, Control Systems, IoT	Insufficient overview of IT landscape	Specified
Stepping Stone, IoT	Networked environments	Specified
Cloud, Extended data collection	Unsafe information sharing	Extended and specified
Extended data collection	Security requirement inability	Extended and specified
Extended data collection	Legacy systems	Extended and specified
-	Insufficient funds	Identified

Table 16: Vulnerability Trend Specification

Insufficient overview of IT landscape

Often when looked at cyber security at hospitals a large focus is on the connections to the internet. Hospitals who mainly focus on that aspect may miss a large part of the threat vectors when you do not take into account all the possible entries and applications a hospital has. A large amount of experts warned for this narrow focus:

[CSE:04] "One of the eye openers for me was, we held a session and we identified data profiles and the crown jewels there. And we thought, how could cybercriminals enter and how could they move on to the crown jewels. And what we concluded was that everybody seemed to focus on the internet connection, the firewall, double firewall, intrusion detection. Everything is focused on that. There is little attention for different entries. Intern in the building, I just plug in an USB somewhere. A hospital is an open organization. Or IFU connections, camera connections, cash register systems. All kinds of openings. And if you organize a workshop and you enter the network you will often see more entries. And you will find out that security measures are not optimally taken to defend against that. And even worse is that when you are able to get at an unsecured working station through phishing or a camera, almost no barriers remain before the crown jewels."

[CSE:02] "And by the way, I worry a lot about that, that there are all kind of nice, let's call it CDs, which are entered somewhere where the hospital does not know off."

[HCSM:03] "And that threat does not necessarily originates from the internet, but it may originate from a random introduced laptop or USB stick or whatever. There are a lot of vectors through which viruses and other threats are able to enter the hospital. Thus the internet threat is not the most relevant issue or just one of the relevant issues."

And the vulnerability of unseen entries in the IT landscape do not necessarily only occur on neglected entries, but could as well occur when changing something in the IT landscape:

[HCSM:08] "The largest risk is around changes. Often when you are performing changes considering the infrastructure you need to pay attention that you do not already open a device and leave it open, because you will continue working with it later on."

This problem does not only occur with threats originating from the outside, but it may prove a problem as well when something malfunctions:

[HCSM:02] "When a disturbance occurs in the technical infrastructure, when a server malfunctions, it proved to be very difficult to find the reason. And what I conclude to be a vulnerability is the lack of documentation of the landscape. Do you know where you are talking about? Well we as two IT auditors have quite some trouble with that at the <…> to find out what kind of infrastructure is there and which applications run where? You might imagine, if something goes wrong, where do you start searching for the problem…"

Also hospitals are relatively open organizations containing large areas of public space, which enables threat actors to walk around and discover all kinds of entries.

[HCSM:07] "The hospital is of course a relatively open organization, you can just walk in. It is relatively easy to find a monitor which contains a running program that provides you with access to certain information. When you go to a bank you will need to walk through 10 doors so to speak. That is not the case here."

[HCSM:06] "You can walk in here the whole day. And that happens, you see people, downstairs at the coffee corners, who are working with their laptop, they are not here because they have an appointment. They are just sitting here the whole day. Maybe they do have an appointment with someone. What they say, go ahead, it is at the edge of <…> a parking lot near, parking for 2 euro and we can sit warm and dry. You can have something to drink and to eat, and that, yes, that hospital is open. Till a certain degree."

[HCSM:02] "If it is the main risk I am not sure, but the fact that it is a public space makes it a breeding ground for large risks."

[CSE:05] "The, my best trick to obtain data from a hospital would not use the internet, but I would walk in and search with my laptop for an unpatched portal and enter it and you can just literally plug a network cable in it and you will be able to monitor what happens on the network, so the question is, it are all just electronic packages that fly by and such. What did they do to prevent someone using this approach to obtain parts of the EMR, are the connections between the EMR systems encrypted at the bottom. Is the access of doctors to the EMR through their mobile or tablet encrypted, so it cannot be the case that someone that is, sniffing they call it, sees packages flying by on the network… And that is the way I would attack a hospital, just walk in and sit."

Networked environments

Since a couple of years hospitals are increasingly connecting systems and devices to each other and the outside world:

[CSE:02] "Up until a few years ago, 80% of the devices was stand alone."

[CSE:06] "There is a trend that more and more products are bought and need to communicate and an interface is build and connections are implemented, but it does not always happen in a responsible manner. There is not enough testing in all cases, the input from device A, if that goes to device B do you obtain the correct output. That is an interoperability point. Everything communicates with each other and just trusts everything goes well. But especially in chains of three systems and one of those is updated and in those cases not het whole chain is tested, yes of course it costs a lot of time. Certainly with all those patches of those devices and systems, it is not easy, but the problem remains and hospitals are discussing it. <…> Yes, we have seen incidents concerning devices that are connected in a network in which devices did thing which were unknown to the supplier and to the hospital as well."

Incidents were thus reported concerning networked environments. This seems to be a large problem especially with intelligent devices that are linked to each other and indirect to the internet. It is therefore not recommended to connect medical devices to the main network or at least create strong segmentation and access control to protect the devices [CSE:03]. This however is not always the case:

[CSE:01] "A considerable amount of MRI scanners just have a hard disk in them. Which contains patient data of course. More worrisome I found it to hear that a couple of hospitals do not fully realize that. Some of them are doing it right, so that is nice as well. I wonder if medical device security should be a part of enterprise security, whether the IT department should be responsible for that. It adds quite some extra requirements. You cannot rely on your normal IT infrastructure. And that is why sometimes you should not connect it directly to your administration network. And that happens sometimes. And in some of those cases you are talking about a virus outbreak. If you start working with segmentation, so when you create a separate subnet for your medical devices that would already improve the situation. <…> I know at least one case where everything was directly connected"

[HCSM:06] "On the other side, we are quite a flat network, little segmentation, because that is not possible. And a lot of hospitals are in that situation. You can only create a few security layers in your network. That has its disadvantages, when you are in, you are really in."

A lack of segmentation thus causes the network to be vulnerable when primary defense mechanisms are bypassed or breached. Another part of the trend in networked environments is the increase in outward

connections. Portals providing access to sensitive data such as patient data are more and more installed. These portals should be protected and tested well to ensure their security.

[CSE:04] "What you often see is that every hospital has its own data center. That is all neatly accessible through the internet. All kind of partners and homeworkers are connected through it."

Unsafe information sharing

Under unsafe information sharing methods and technologies are identified that enable sharing of confidential information in an unsafe manner. This differs from hyperconnectivity as hyperconnectivity is about all extra connections the hospitals develop, while unsafe information sharing is about the sharing of information with external sources outside the hospital through unsafe channels, often unofficially. Often this consists of information containing patient data or research data which is shared through cloud-like or unsafe e-mail solutions, mostly because safe options are not available at that hospital.

[HCSM:07] "Large amounts of information in the hospital goes outside, to general practitioners, to scientific professional groups, to other hospitals, that is quite a lot, there is a concern whether that always happens secure."

[CSE:04] "What more and more happens, and we saw this at a research club, that applications are stored in the cloud."

[HCSM:01] "The lack of alternatives, so one of the risks is someone starts using cloud like solutions like Dropbox, since we tell them it is not allowed."

[HCSM:01] "The lack of alternatives, so one of the risks is someone starts using cloud like solutions like Dropbox, since we tell them it is not allowed. <…> Well there is no good alternative. You want to share something with your college in Harvard, but you are not able to do this through the Sharepoint system. No outsiders are allowed on it. And you still want to share that file, well in those cases it is shared through Dropbox-like activities. Even though we say you should not do that. That is dangerous and still it happens. I do not have a save alternative. The hospital policy dictates that no confident files are allowed in e-mail. And still it happens, because there is no secure e-mail solution."

Some hospitals try to mitigate these risks by providing safe or at least safer solutions. Such as dedicated cloud and encryption solutions.

[CSE:02] "They would not dare that, well almost not. That only happens sparsely and mostly with older files, back-ups and alike. Somewhere on a dedicated cloud, we are not renting space at Amazone…"

[HCSM:09] "We are currently looking into the access to information, interviewing with the doctor, even doctors sometimes ask whether is secure. In some cases it is safe to mail, because throughout <…>, that is a kind of service condition, we have a tunnel and that is reasonably safe, well some hospitals are not connected to it. In those cases it is not always safe and you would prefer that, because you do not want your end user to break its head over such things, but I certainly want, look nowadays those mobile phones are super useful, coincidentally we had a discussion about that this morning, the doctor, or whatever care specialist maybe a different function, a person in the hospital does not shy from taking a photo. And that will remain on the device. Whether that is texted through Whatsapp, then we ask what do you think about such actions? Where does the information go, patriot act and such. People who use Dropbox, because we do not have the facilities, we are really looking into the best options for people to share information and how we can control it. But in a more facilitating approach, it just went so fast with the technological development, certainly as a hospital you are not always leader in innovations, you are always a little behind."

However the core of the problem seems to be that development on sharing enabling technologies went so fast the last couple of years that people who use such solutions started using them in their professional functions as well, not thinking or not aware of the risks such technology has. Next to internet based ways to share the data also unofficial storage of data on hard disks or laptops is possible. This is often done by (temporarily) employees.

[HCSM:06] "You cannot escape that, you do not have that control." Concerning employees who safe research data on external hard disks.

[HCSM:02] "A: Yes and employment contracts that become shorter, more external employees, who are in service temporary for specific projects. B: That is one of the vulnerabilities as well, the information is taken by external employees"

Security requirement inability

Security requirement inability refers to a part of the suppliers of mostly medical equipment which does not seem to be able to deliver secure enough software and do not make the needed investments to up the security to a higher level and on the other side of the buyer-seller relation especially smaller hospitals seem to have an inability to demand the right security levels.

[HCSM:04] "Yes, at this point there is increase in standardization. That is the law, the covenant on medical technology. At that point there is a trend that is the past 10 years all the static devices that people use, like a MRI, that is mainly the case with printers, they contain intelligence. And the easier it is to remotely control that device and link that device immediately to the internet as well, because than he can be automatically updated as well. And that is where you identify that suppliers are behind when it comes to the security of the devices. And the buyers are not able to formulate the right demands concerning that kind of technology. So yeah a MRI scan, but it might as well be an insulin pump or whatever, those devices are all becoming intelligent, the software they contain is just inferior."

[HCSM:01] "Today in the LA Times a report was published about 300 American hospitals that, well what if you take a look there, what do you see. They set default values on firewalls, as they are delivered by the factory, which is not recommended. They have simple passwords for very critical systems, also on the management side."

[CSE:02] "As an ITer you were never allowed to touch the medical devices. Those medical devices that would always, those ITers were always annoying. And the suppliers of medical devices were always like, do not sweat it, we will deliver it. That was there business case. It was even the case that, things went wrong, especially concerning medical devices linked to the network, of which the supplier did not allow you to alter, because in those cases the warranty for reliability expired. This caused one hospital to shut down."

The reasons behind this vulnerability were explained by the strong supplier power, who made it illegal to improve the software of the medical devices and a lack of in-house IT knowledge concerning the medical devices due to outsourcing of large parts of their IT.

[CSE:02] "There is a risk with viruses. Because the supplier say, we do not guaranty the reliability of our equipment if you install a virus scanner. And then that same supplier comes with an USB stick to do some maintenance. That are tedious risks. And some risks you should just… You could protect it, isolate it. I can try to segment your network as much as possible. There are all kinds of technical procedures for that. Those are mostly taken. But measures cost money. And those are not small amounts."

[HCSM:04] "We outsourced almost everything. <…> Knowledge concerning IT is outsourced as well. We buy it. <…> Because you outsource knowledge and if you outsource the knowledge to specify something you will not be able to specify something well and you will obtain junk. In management, in the management of risks, the mistake that usually is made concerning outsourcing is the outsourcing of responsibility. That is not possible. That is where things go wrong."

Legacy systems

Legacy systems refers to software that is outdated security wise, but cannot or very difficultly be mitigated or replaced without large costs or high risks. In most cases this concerns intelligent medical equipment that when it was bought probably was secure and is budgeted and able to run for years more before replacement of the device is needed, however the software is security wise strongly outdated, while in combination with other

vulnerabilities such as hyperconnectivity create a very dangerous situation. An often named example was medical devices containing XP, which is no longer supported:

[HCSM:03] "Ow yeah, I believe 60% of our devices still runs on XP or another old system. Parties like Siemens and Philips chose to, what is the name? To use some sort of host intrusion prevention and host lock down. They are not mitigatable to XP in the short run. They annotated that too late, so they have a plan, but it still has to be executed. Some of them still have an embedded XP of which the support is not finished yet, those will be updated one or two years longer. So there are more realities than just XP."

[CSE:04] "No, that, look, a while ago I had a hospital that, okay, all the medical devices, they run on Windows XP. With all kinds of cards and those things. You cannot upgrade those, well. But okay it is connected to the EMR. Fine right? But if it is connected to the EMR than it is connected to the network as well."

[HCSM:04] "There are a lot of outdated devices, in which no logging is possible, since they do not have the option. And that cannot be implemented ad hoc and even when that would happen it would not satisfy the current demands."

However the problem with legacy systems is not just related to medical devices. Other core systems used in the hospital might be needing replacement as well, something that is not always easy and since these systems might have an important role in the core business of the hospital mistakes made during the replacement could have large impacts.

[CSE:06] "Another risk is about the EMR, that was in an ICT tabloid as well, those are sometimes in need for replacement. In those cases a hospital is buying a new EMR. Well that transition stage is kind of difficult, because at a certain moment you will undergo some sort of end of support from one system since you are transitioning to another. And often that does not happen by letting one department start, but a big bang approach is used. And at the same time you will often hear that the EMR consisted of different little systems and that is replaced by one system and of course all kind of things can fail during this process."

Insufficient funds

Finally a vulnerability was mentioned concerning a lack of resources. As most hospitals have relatively little resources compared to other sectors such as oil & gas, finance and technology and try to invest most of their resources in good healthcare they may be a relatively easy target as their cyber security is relatively low. One hospital security manager when asked whether the recruitment of skilled IT employees would be a problem:

[HCSM:03] "There is a threat in that, although I cannot judge whether that is a core problem. Hospitals pay less and they are not the most profound, but it is not whether we need those people. That is a challenge, but it is more about whether you have the resources to do everything and still keep security in mind."

6.3.4 Conclusions threat landscape

The relevant assets groups and threat profiles, represented by the threat actors, are mapped in a target matrix in Table 17. This table provides a summary of the threats and assets above and how these are linked. Per combination it is given whether the threat actor is primary focused on the target group, focused on a part of the target group or non-specifically focused on a target group. When the threat actor has a primary focus on an asset group, extra protective measures should be taken against the threat actor and the used measures. When an asset group is a partly target, some specific targets of that asset group are interesting, others fall in the category non-specific. For communication systems considering cyber criminals mainly the internet portals are interesting and social engineers the focus is mainly on e-mail systems. Hacktivists are mostly interested in CBRN data and the employees handling these considering research, operation and employee data. These specific assets need extra protection to prevent these threat actors becoming successful. When an asset group is a non-specific target it means that either the threat actor is not directly interested in this asset group, e.g. only as a possibility to reach other targets through them, or the threat actor will mainly target assets that are not well protected or serve as collateral damage. A strong base security would often be sufficient in those cases against those threat actors. Threat actors and asset groups which are typically only in the risk profile of

academic and in lesser extend top clinical hospital, but barely for general hospitals, are marked with an asterisk.

Legend: p = primary target pa = partly target ns = non-specific target * = Academic/Top Clinical hospital specific		Cyber Asset Groups						
		Patient Assets	Financial Assets	Research Assets*	Medical Systems and SCADA	Operational Assets	Employee Assets	Communication Systems
Threat Actors	Cyber Criminals	p	p	p	ns	ns	p	pa
	Social Engineers	p	p	p	ns	ns	p	pa
	Internal Actors	ns	p	p	ns	ns	ns	ns
	Nation States*	ns	ns	p	ns	ns	ns	ns
	Cyber Researchers	ns	ns	ns	ns	ns	ns	ns
	Script Kiddies	ns	ns	ns	ns	ns	ns	ns
	VIP Spies	p	ns	ns	ns	ns	ns	ns
	Frustrated Patients	ns	ns	ns	ns	ns	ns	ns
	Hacktivists*	ns	ns	pa	ns	pa	pa	ns

Table 17: Target Matrix

The presence of certain types of research data is a large influencer on the presence of threats that emanate from nation states or hacktivists. Nation states, especially state sponsored hackers from China, seem to have a strong focus on research assets from a political-economical perspective, which are mainly held by academic and in lesser extend top clinical hospitals. Hacktivists seem to have a strong focus on, in their eyes, unethical research, e.g. research executed on lab animals. This type of research is often only done at academic hospitals.

Interesting considering threat emanating from nation states is that this threat is often underestimated by hospitals. For general hospitals this threat is only of moderate to none importance. However considering top clinical and academic hospitals a strong segregation in opinion was observed between hospitals who had no incidents, deeming it an unlikely threat and hospitals who did had incidents, backed-up by the government experts that nation states indeed posed a serious threat. It is most likely in this case that the former group (no incident yet) is mostly unaware of the most actual developments in the threat landscape. Although all hospital security manager were aware of the threat actor, the problem considering this aspect seems to be caused by an unawareness considering the interest of the threat actor in the assets of hospitals. This example stresses the importance for hospitals to gather information considering threats, vulnerabilities and incidents continuously and from a broad variety of sources.

High level vulnerabilities in the hospital sector that increase the likelihood and impact of threats were identified and grouped into six categories: insufficient overview of IT landscape, networked environments, unsafe information sharing, security requirement inability, legacy systems and insufficient funds. Although they might not be a problem for all hospitals, hospitals should look into them and ensure themselves they are mitigated properly. The first three vulnerabilities all have to do with increasing forms of hyperconnectivity. Hospitals should try to mitigate the risks of hyperconnectivity by investing in good documentation of the IT landscape, segregating their systems with implemented extra security measures between sub-networks and providing safe communication systems that satisfy the business need. Security requirement inability is often a problem at smaller hospitals who have less funds to invest in IT and the security of it. Often a large part of the IT systems they possess is outsourced, which as side effect results in the outsourcing of skilled IT personnel as well, causing a drain of IT knowledge. More problematic is the outsourcing of security, although the outsourcing itself may have many benefits, often the responsibility is outsourced as well. It would be better for hospitals to invest in in-house cyber security proficient employees to at least keep control over the development of security policies and keep the security responsibility in-house. At this point the security requirement inability intersects with the problem of insufficient funds, as these should be present to invest in such measures. The problem of insufficient funds is a difficult one as one would like to invest as much funds directly into health care. This stresses the need for good CSRA as it not only helps to clarify funds needed for

security measures, but can be used as well to increase the awareness and priorities of budget responsible management concerning the cyber security of assets.

7 Maturity Model Development

In this chapter the development process of the maturity model and the results, before the survey feedback will be clarified. It will start with a summary of the relevant theoretical background from the SLR (chapter 3), the comparison analysis (chapter 4) and the maturity model comparison (chapter 5). Then the development strategy and approach described in chapter 5 is elaborated upon and finally the results are presented of the maturity levels and maturity dimensions, leading to maturity model version 1.

7.1 Maturity Model Development Process

From the SLR, the comparison analysis and the maturity model comparison some interesting requirements were extracted, identifying important processes and quality factors within CSRA. As some processes and quality factors were identified in several of the theoretical background sections an overview of these requirements are presented with a unique identifier, with doubles excluded, in Table 18. Process 3 to 7 and 9 to 11 were identified in the SLR and confirmed later in the method comparison, where process 1,2 and 8 were added based on the findings. These sub-processes make up CSRA and should somehow be measured in the maturity model. The quality factors were results from research which are important for the quality of some or all of the sub-processes. Of these quality factors 12 to 21 were identified during the SLR. In the method comparison quality factors 12 to 21 were discussed more extensive and quality factor 31 was added. In the maturity model comparison quality factors 22 to 30 were added based on the theory and content of the compared maturity models.

Identifier	Process	Identifier	Quality Factors
1	Context identification	12	Risk Model Sophistication
2	Stakeholder identification	13	CIA triad
3	Asset identification	14	Use in networked environments
4	Asset valuation	15	Tools and documentation
5	Threat identification	16	Validation
6	Control identification	17	Quantification
7	Vulnerability identification	18	Different scope abstraction
8	Scenario development	19	Internal collaboration
9	Impact assessment	20	Top management reporting
10	Likelihood assessment	21	Government information sharing
11	Risk evaluation	22	Security community information sharing
		23	Cyber security testing and exercises
		24	Data extraction from the cyber security architecture
		25	Use of a rigorous method
		26	Use of standards and guidelines
		27	Periodically review of risk assessments
		28	Risk assessor authority
		29	Skilled personnel
		30	Risk assessment needs to be part of ISMS design and evolution
		31	Interview technique sophistication

Table 18: Requirements Identified in Theoretical Background

Based on the identified requirements from Table 18 the first framework for the maturity model was constructed. This included the maturity levels and maturity dimensions, which are developed according to the described strategy and approach in chapter 5. Requirements 16 (validation), 25 (use of a method) and 30 (ISMS design and evolution) are used in the development of the final maturity levels. All the other requirements were used, together with the exploratory expert interviews (ID: 1 to 13, Table 13) to identify the maturity dimensions and fill in separate cells. The maturity dimensions of version 0.9 are shown in Table 19, mapped against the requirements from the theoretical background. The requirements related to scope and context (1, 18 and 27) were excluded in the first version, as at the moment these were set out of scope. During the interviews a new maturity factor was identified: supplier collaboration. Supplier collaboration is a form of collaboration with suppliers of software and devices in the hospital. Due to collaboration with the supplier information concerning vulnerabilities (e.g. software bugs) and threats (e.g. malware) can be gathered, improving the threat and vulnerability awareness of the hospital. During the exploratory expert interviews the cells of the maturity dimensions were identified, resulting in HCRAMM version 0.9 (Appendix C). The

summarized framework and mapping is presented in Figure 36. Maturity dimensions without mapped process elements and quality factors are retrieved from the interviews and explained later on in this chapter.

Maturity Dimension		Level 0	Level 1	Level 2	Level 3	Level 4
CSMS Configuration[24]						
Asset Awareness						
	Asset Identification[3]	Identification of cyber assets				
Threat Awareness[5]						
	Brand Monitoring	Monitoring for threats directed at your hospital				
	External Threat monitoring	Monitoring of attacks comming from the outside				
	Internal threat monitoring[14]	Monitoring of internal data streams				
	Incident reporting	Collecting and reporting cyber security incidents				
Vulnerablity awareness[7]						
	Penetration Tests[23]	Simulating attacks in order to look for vulnerabilities				
	System Testing[23]	Testing the input and output of systems within the hospital				
	Cyber Security Exercises[23]	Hold exercises to test the responsiveness power of the hospital				
	Control Overview[6]	Obtaining an overview of all the implemented and planned controls				
	IT Security Audits[23]	Perform IT audits on the systems				
Analysis						
	Asset Valuation[4, 12, 13]	Valuate the importance of assets and their relations				
	Scenario Sophistication[8, 13]	Develop incident scenarios				
	Impact Sophistication[9, 12, 17]	Assess the impact of an possible incident				
	Likelihood of Occurence Sophistication[10, 12, 17]	Assess the likelihood of an possible incident				
	Risk Leveling[11, 12]	Decide upon the importance of the risks and their priority				
Structure						
	Interviewing[31]	Use interview methods to obtain information				
	Tools[15]	Use tools to aid the risk assessment process				
	Security Requirements[26]	Use security frameworks, with defined requirements				
	Documentation[15]	The process is well documented				
People						
	Top Managment Support[20]	Top management support the risk assessment process				
	Stakeholder[2, 28]	Stakeholders from different categories are involved				
	Quality of Risk Assessor[28, 29]	The risk assessor is experienced and well trained				
Collaboration						
	Internal Collaboration[19]	Their is collaboration between different devisions for the risk assessment				
	Supplier Collaboration	The suppliers of systems provide useful information for the risk assessment				
	Sector wide Collaboration[22, 23]	Different forms of sector wide collaboration are implementd				
	World Wide Input and Collaboration[22]	Input is obtained from threat landscapes and security communities worldwide				

Figure 36: HCRAMM V 0.9 Framework

The translation of the maturity dimensions from HCRAMM version 0.9 to HCRAMM version 1, following from the evaluation phase using expert interviews with ID 14 to 17 (Table 13), is depicted in Table 19. Most elements from maturity dimensions from HCRAMM version 0.9 are transferred directly to maturity dimensions of HCRAMM version 1. Two dimensions were split and the elements were divided over two new maturity dimensions. The elements depicted in documentation considering information storage are included into risk registration. Elements considering documentation providing structured tools, such as questionnaires or templates are included in tools. Internal collaboration was split as well resulting in certain elements being

transferred to risk assessor authority, these include the elements that aid the collaboration with the risk assessor. Remaining elements were transferred to stakeholder involvement, as collaboration with the stakeholders should be done in several domains instead of being directed from for example the IT department. Finally a new maturity dimension, scope and frequency, was added, previously set out of scope, although during the interviews and especially as [HCSM:11] stressed the importance of it, it was decided to add this process to the maturity model which in retrospect should have been included from the start.

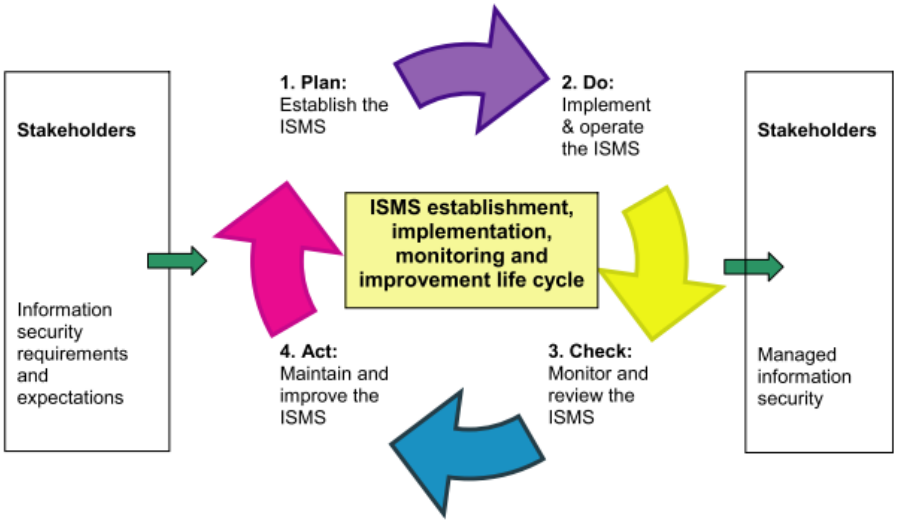


Figure 37: Plan, Do, Check, Act Cycle in Information Security (ISO 27799)

Feedback considering version 0.9 of the HCRAMM, with the highest change impact was considering the ISMS positioning aspects. As cyber security is a component of information security, important theories in the information security apply mostly. An important theory is the Plan, Do, Check, Act (PDCA) cycle (Figure 37) to improve information systems. This is used throughout information security related standards such as the NEN and ISO. This PDCA cycle starts with the plan phase in which inter alia the risk assessment is performed. Most requirements identified for the cells concerning the asset identification, threat identification and vulnerability identification part of the HCRAMM v0.9 were not related to plan-phase, but rather performed in other phases of the PDCA cycle, mainly the do-phase. The input of requirements however is important for the risk assessment, but as they are not performed in the plan phase, and thus during the risk assessment, it is merely the gathering of this information which is of importance for the risk assessment. As is demonstrated by the following quote:

[HCSM:10] "On itself, I agree to what you say. Those are important inputs of information. The question is however, do you perform them in the risk assessment itself or is it input of information from other trajectories. And I believe it is information that is gained from other trajectories and not directly is done in the risk assessment, but in the ISMS in total."

The asset identification, threat identification and vulnerability identification are therefore rewritten to information gathering dimensions rather than awareness dimensions on themselves. To bring other maturity dimensions to the same level of abstraction some maturity dimensions were merged. Asset valuation and impact sophistication were merged as depending on the risk model used these may not occur both, but they do serve the same goal, to indicate the damage of a possible incident. Furthermore some names have changed and some requirements have been divided over other maturity dimensions, shown in Table 19. All in all no elements were excluded, some extra were included, but most changes provided merely an allocation of identified elements. Finally feedback was provided, which suggested to align maturity cells more to their maturity levels and focus less on requirements and more on structures or processes. The maturity levels were still basic in this stage. No clear structure was presented in the maturity levels yet. Level 0 till 4 were installed as this architecture seemed to fit the solution. Interviewees were then asked if they agreed and were they

would map individual elements they described. Starting from HCRAMM version 1, based on the obtained information important information throughout the dimensions at certain levels was extracted and mapped against the TIMM and CMMI maturity levels during the evaluation phase, the results are explained in chapter 7.2.

Requirements	Maturity Dimensions v0.9	New Maturity Dimensions v1
3	Asset Identification	Information Gathering from Internal Sources
5	Brand Monitoring	Information Gathering from External Sources
5	External Threat Monitoring	Information Gathering from External Sources
5	Internal Threat Monitoring	Information Gathering from Internal Sources
5	Incident Reporting	Information Gathering from Internal Sources
7, 23	Penetration Tests	Information Gathering from Internal Sources
7, 23	System Testing	Information Gathering from Internal Sources
7, 23	Cyber Security Exercises	Information Gathering from Internal Sources
6, 23	Control Overview	Information Gathering from Internal Sources
7, 23	IT Security Audits	Information Gathering from Internal Sources
4, 12	Asset Valuation	Assessment of Consequences
9, 12	Impact Sophistication	Assessment of Consequences
8, 13, 14	Scenario Sophistication	Identification of Consequences
10, 12	Likelihood of Occurrence Sophistication	Assessment of Incident Likelihood
11, 12	Risk Leveling	Risk Evaluation
31	Interviewing	Information Gathering from Internal Sources
26	Security Requirement Standards	Information Gathering from External Sources
15	Tooling	Tooling
15	Documentation	*Partly in Risk Registration, partly in Tooling*
20	Top Management Support	Risk assessor authority
2, 28	Stakeholder	Stakeholder involvement
28, 29	Quality of Risk Assessor	Risk assessor authority
19	Internal Collaboration	*Partly in Risk Assessor Authority, partly in Stakeholder Involvement*
	Supplier Collaboration	Information Gathering from External Sources
21, 22	Sector Wide Collaboration	Information Gathering from External Sources
22	Worldwide Input and Collaboration	Information Gathering from External Sources
1, 18, 27		*Scope and Frequency*

Table 19: Mapping Hospital Cybersecurity Risk Assessment Maturity Model Version 0.9 to Version 1

The HCRAMM version 1, based on the given feedback is presented in Appendix D. The explicit definition of the maturity levels and dimensions is provided in the next two sub-chapters.

7.2 Maturity Levels

The final maturity levels and their description are discussed below. The maturity model levels are based on the used maturity levels in the test framework for information security developed by the NIAZ/NOREA (2012), as this was the only similar maturity model structure used both in the information and cyber security as well as in the health care sector. Furthermore the maturity levels seem to have a good fit for the purpose of the HCRAMM. The used levels are based on the CMM (Jung & Goldenson, 2003) and are respectively: incomplete, initial, repeatable, defined and managed. The last maturity level label is changed for optimized, as adopted from the highest CMMI level, the successor of the CMM (SEI, 2010), as this better represents the goal of the maturity level to optimize CSRA.

0: Incomplete

At the incomplete level, the maturity dimension is none-existent and does not meet the requirements for CSRA .

1: Initial

At the initial level risk assessment is performed in an ad-hoc manner. There are no structured approaches and little documentation is done.

2: Repeatable

Quality factor 25 (table 19) required that risk assessment was performed by a clear method. At the level repeatable this quality factor is satisfied. The processes follow a clearly defined structure and are documented. All the basis requirements of risks assessment are satisfied and repeatable in each risk assessment following this one.

3: Defined

At the level defined quality factor 16 (validation) and 17 (quantification, table 19) are included. More quantified information and analysis is used to support the risk assessment. And clear validation processes are included. Furthermore the sub-processes are streamlined with each other and work well together.

4: Optimized

At the level optimized processes are strongly streamlined and improve iteratively, strong quantified information and analysis is used support the risk assessment and concerning quality factor 30 (ISM design and evolution, table 19) a clear process is in place which iteratively improves the quality of the maturity dimension.

7.3 Maturity Model Dimensions

As was discussed earlier the maturity dimensions were first formed based on the process elements and quality factors extracted from the SLR, the method comparison and the maturity model comparison. The individual elements describe how those important aspects are filled in at the hospitals. Often several forms of these elements occur at different maturity levels. As the individual elements rely heavy on the interviewees depicted in table 13, the quotes relating to these elements are depicted per maturity dimension. In these 17 interviews the first 13 used a more open approach and the latter four were used to verify results.

The identified maturity dimensions of the maturity model are portrayed in Figure 38, including the times elements related to these were referred to in interviews. Herby a difference is made in the amount of interviewees (sources) that mentioned the aspect in the interview and the amount of references the interviewee made concerning this subject. More often mentioned maturities are not necessarily more important, but are often more complex and contain more elements.

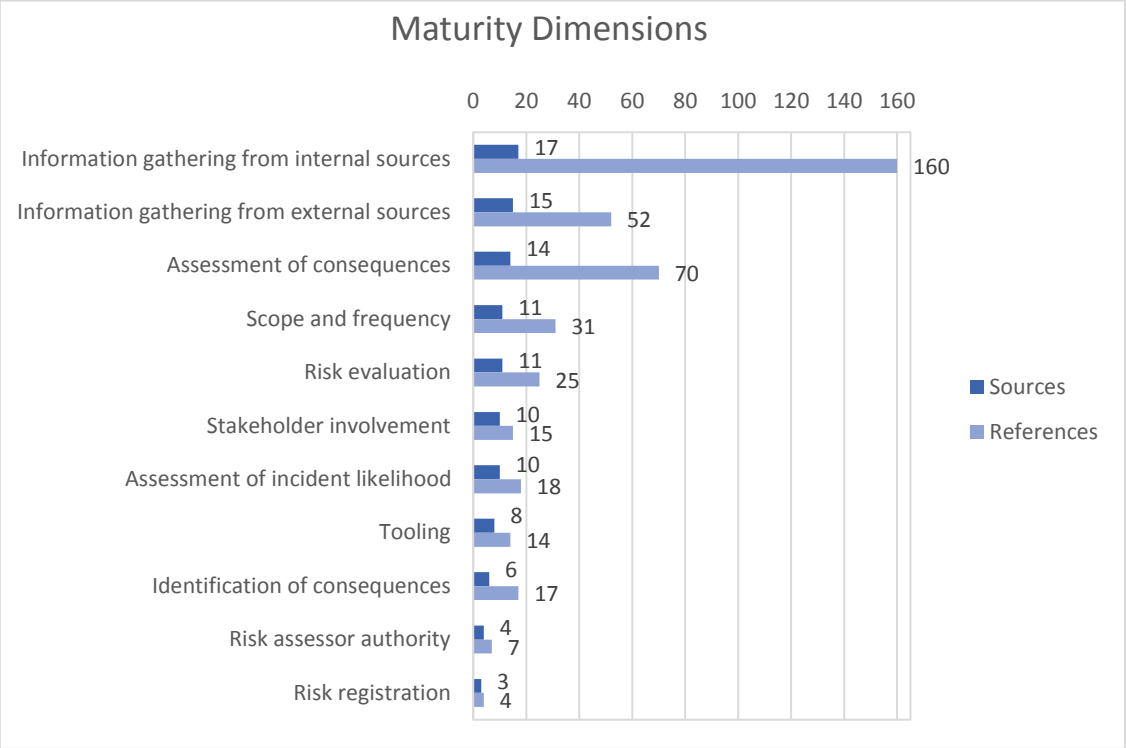


Figure 38: Maturity Dimensions

It should be noted that the HCRAMM is build based on an open risk model principle rather than a closed risk model principle. Even though an open risk model may be more complex to use it allows hospitals better to adapt to their specific situation. The maturity dimensions are explained in the order of their placement in the maturity model. References to the input from the theoretical background are provided together with the input from expert interviews, which together form maturity dimension and its cells. The maturity dimension result will be provided at the end of each sub-chapter. The order of the capabilities in the individual cells at the maturity levels is the result of the alignment of elements with the maturity level principles and information from expert interviews. The individual elements will be numbered as these are important for the scoring mechanism in chapter 8.

7.3.1 Scope and Frequency

From the theoretical background it became imminent that context identification (requirement 1) is an important sub-process of risk assessment. This process is partly taken care of as the maturity model is already domain specific. An important remaining aspect of context identification is the scope.

Element 1.1: The scope should be on different levels of abstraction (requirement 18). This should clearly defined in the scope, preferably on both policy and technical level, including both aspects such as societal

trends and technical vulnerabilities in IT systems and medical devices, which on other levels might affect the hospital.

Element 1.2: Furthermore almost all experts agreed that a cyber or information security risk assessment is best performed from a process perspective, as it are the main processes of the hospital that should be mitigated from risks and the assets are there to support these processes. Even the experts currently using an asset perspective agreed a process perspective would be better.

Element 1.3: Finally it should be clear when risk assessments are performed and in which frequency (requirement 27). Frequency of risk assessment differed between experts from once every four or five years to with every architectural change. Also the depth needed with those periods might change from a total hospital wide till risk assessment till an update of the current risk assessment. It seems however profitable for the hospital when a clear structure is present to ensure that risk assessments are performed on a regular basis. The results are provided in Figure 39.

[CSE:02] "Yes, you should think from your processes."

[CSE:04] "A hospital started a collaboration with another hospital and those exchanged anonymized information, well not anonymized, but they exchanged confidential information between each other. That is done through a certain system. And they asked us to review, audit their system. Well the level that they have, compare it with the NEN 7510, but that is only one aspect. I think that the NEN 7510 is something global, it is more on a tactical level. Tick of, did you implement it or not. But that does not tell you anything about your level of security, not everything. So we did a technical vulnerability assessment. Which vulnerabilities does the infrastructure contain. And which attack vectors and which scenario are they vulnerable to."

[HCSM:08] "Yes, well, you should do it on process level, what is your critical process and what are the risks when I do not have access to the system and what is the impact when information and information systems are not available. We are not strong yet in process thinking, we mainly limit ourselves to the most critical systems. Thus in such a case it you might take a look at the hospital information system, for example the EMR, how long can we abstain from access to it, what is the risk of unauthorized access or mutilation of the data, etcetera. Is it performed regularly? No. We could do better. We are now planning to perform one yearly."

[HCSM:02] "Yes and that is in order in every audit we do, where are we talking about? By the way not just in IT audits. I started an advice audit yesterday concerning a certain juridical structure here and I asked the director do you have an idea what it is about. Money, the number of limited liability firms, the number of foundations, the number of internal and external employees? And they are just give me a sheepish look. Good question. So first we mapped that. And for a lot of people that was completely new to see that together. And then they asked us to develop a good governance model for that structure. And that is not related to IT, but you see this everywhere. People do not know in which environment they work."

[HCSM:04] "We are at the verge to implement a change to, eh, force the whole hospital to do a risk assessment with every change. Then when a risk assessment is done you could take the current one and update this, because you should do a risk assessment."

[CSE:02] "Yes, no, well. That is always the game, so those guys that, you should, but every time when you change that architecture. What is an architecture change within a hospital. Is that when you insert something new in the architecture? Is that an architecture change, than you should perform a risk analysis every two days."

[CSE:04] "Look, if you have a very stable system that does the same for ten years, I notice that in particular those kind of systems are subject to change. All kinds of functions and bells and whistles are built into it. Connections with external MPR and other organizations, like primary practitioners, data links that are defined. With this kind of risk enhancing factors you should look more often, maybe even at every change, but at least more often at such."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Scope and Frequency	No risk assessment is performed with a specific cyber scope	Cyber security risk assessments are performed ad hoc with an unclear scope	A structure is in place that defines when cyber security risk assessments are performed. The focus of the risk assessment is placed on the most important assets	A structure is in place that defines when cyber security risk assessments are performed. The focus of the risk assessment is placed on the most important processes	A structure is in place that defines when cyber security risk assessments are performed. These are done with a process centered scope on both policy and technical level

Figure 39: Maturity Dimension 1 Scope and Frequency

7.3.2 Cyber Security Risk Assessor Authority

To perform well CSRAs the risk assessor needs the right amount of internal authority (requirement 28).

Element 2.1: The risk assessor should be able to access the needed information sources, including employees, to obtain the information he needs (requirement 19 & 29). In the optimal situation the hospital employees are aware of the risk assessor's task and he is pro-actively helped by the organization to perform his task.

Element 2.2: It is important that the risk assessor has direct connections to the board (requirement 20), as this provides extra authority and retains his message to be filtered by department managers.

The full maturity level is provided in Figure 40.

[HCSM:06] Here I am, I report directly to the board of directors, I am accountable to them as well even though I am seated here on the ICT department I am independent. And the main part of our job is digital nowadays so that is why I am seated at the ICT, because I want to stay in touch there, I can take a seat on the 7th floor with the board of directors, but…"

[CSE:06] "I am not sure about that, that is done more often nowadays. I believe it is good. But according to us they are not obligated to do that."

[HCSM:09] "I should report to the board, here I report to ICT."

[HCSM:10] "Yes, that is a kind of combination for me of stakeholders and top management. In our organization the system owner is always on board level, thus they accept the risks or not."

[HCSM:06] "The moment we did a penetration test here and we talked it through with the ICT and the full board. And then they are never able again to claim they did not knew it."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Risk Assessor Authority	The cyber security risk assessor is appointed by a division and reports to a division head	A cyber security risk assessor is appointed by the board and reports to a division head	The cyber security risk assessor is appointed by and reports directly to the board	The cyber security risk assessor is appointed by and reports directly to the board and has the authority to interview the people and obtain the information needed for the RA	The cyber security risk assessor is appointed by and reports directly to the board and has the authority to interview the people and obtain the information needed for the RA and is proactively helped by the organization for this

Figure 40: Maturity Dimension 2 Risk Assessor Authority

7.3.3 Stakeholder Involvement

In CSRA an important aspect is to involve the people who are affected by these risks, the measures which will be taken against the risks and who are responsible for the assets and processes or in other words: the stakeholders (requirement 2).

Element 3: All the before mentioned stakeholders should be included or at least represented in the risk assessment to gain support for the risk assessment measures which will be taken after the risk assessment

(requirement 28) and to make the stakeholders aware of the risks they are currently exposed to. When stakeholders recognize and understand the risks they are more likely to engage them. A broad spectrum of stakeholders is needed as cyber risks affect the whole organization and not just ICT or medical technology. The full maturity level is provided in Figure 41. Two cells were purposefully left open at this time as no useful content could be added.

[HCSM:03] "And we are trying to let the board set a part of the impact in categories, instead of in management groups and that has nothing to do with better information, but mainly with the awareness and better cover of the board. <…> To ensure board members and management to navigate on those points with a review. Because I am not sure if you know this, but in an average organization the board tells there managers: important, important, important! And he gives them a lot of important messages, the management layer needs to prioritize. They filter and they give instructions to the work floor about subjects they believe are important for their board review. That work floor might have really interesting insights in information security, but they do not reach through the management layer and thus you will need to sell that information security policy to that management layer as well."

[HCSM:04] "Who are the stakeholders when something is implemented. Thus in case of a system, who is the main user. Who has the funds and the resources and the decision authority to, in case something goes wrong, to deal with the situation. You put all those people in one session."

[HCSM:06] "Yes, I map the risks, you the board and management, you are responsible for the risks, you decided we are working with the computer. In those cases I reflect their decision, this are the risks, this are the terms. That includes more than just buying a monitor and a keyboard. No, there is more behind it. So in that case you should invest more, which is something you should take into account. And that is my task and again, everything is fine with me."

[HCSM:07] "A standard straight forward. And if the system owner recognizes it, he will engage the red spots thus the high risks. And I am willing to help him with that. But in the end he is responsible for it and he should deal with it."

[HCSM:09] "Yes certainly in my function, I think from a risk management perspective certainly, because it does not happen enough. But I believe it is twofold, I believe that should sprout from the organization. And sometimes the management or the board of directors are not aware and you should inform them to create that pressure."

[HCSM:10] "The most important is always the stakeholder, because he accepts the risks or indicates how they should be engaged. I see you have that included."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Stakeholder Involvement	No stakeholders are involved		Only stakeholders from one or a few disciplines are involved		All stakeholders within the scope, from all disciplines, are actively involved in the CSRA process

Figure 41: Maturity Dimension 3 Stakeholder Involvement

7.3.4 Risk Registration

Element 4: As the CSRA process gains a higher maturity the storage of previous done risk assessments becomes more important as it can help to iteratively improve the process (requirement 15). It should therefore be stored centralized and actively updated after each risk assessment. In the optimal situation a link should be implemented to systems which contain threat and vulnerability management such as a SIEM. The advantage of such is that the risk assessment process becomes extremely agile and allows frequent updates of the risk landscape without the investment of a high amount of resources.
The full maturity level is provided in Figure 42.

[HCSM:09] "In the ideal situation the p,d,c,a, that is the whole cycle we go through and do what we do and again an analysis, okay, we can check this one of the list, and ow this one was green, but it is now red, so

something went wrong there. Thus in the basics we have a strong picture concerning our situation, only the approach to level it up is often not in place. That is just like, I develop a nice management document and nobody uses it. Or I write a policy and nobody reads it. <…> It is important you use previous risk assessments again and communicates them and have a well secured process. That is still difficult here."

[HCSM:10] "Yes, you will need a knowledgebase for sure, whether that includes tooling or not, it is of importance. Because even if you use it to do a recalibration of the existing information system, you will need that risk analysis and that is important."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Risk Registration	No previous information can be obtained in new CSRAs	Information is saved decentralized	Information is stored centralized in the risk register	Information is stored centralized in the risk register. The risk register is actively updated	Information is stored centralized in the risk register. The risk register is continually updated

Figure 42: Maturity Dimension 4 Risk Registration

7.3.5 Tooling

Element 5: Tooling aids the risk assessor in the information gathering, processing and distribution of the data during the risk assessment, making the risk assessment more efficient and effective (requirement 15). Tooling in its simplest form usually consists of risk matrixes, questionnaires, lists of standard threats and controls, standard report formats and other stencil based formats to structure the process and documentation of it. Most widely used methods contain an abundance of such tools. In more advanced scenarios these tools could be automated and contain certain levels of intelligence to aid the analysis and evaluation of the risks. In the optimized scenario software based tooling is present which applies (near) real time information is collecting, analyzing and presenting in dashboards. The full maturity level is provided in Figure 43.

[HCSM:08] "Yes, we use standard formats."

[HCSM:10] "The question is whether a different approach is more efficient or effective. I am convinced that if it can be done more effective in another way. A&K analyses self, because, you have SPRINT as a method as well, which is based on the A&K analyses, which contains templates to execute it, but in those cases we do not all talk about the fact that your organization communicates during the process, your method does not decide how you communicate with your organization. Thus in that respect I would say: tooling is nice if you would like to use the workflow to steer your organization. I prefer sitting down with the end user itself, with the stakeholder, than doing it through tooling. I want to have some feeling, I want to do something with it. So for that matter not yet, but maybe in the future."

[HCSM:11] Tooling is very useful, especially in combination with documentation.

[HCSM:09] "But we do not have that, because that was too much. And someone from <…> build a derivative for us. In the meantime that thing does not work anymore and now we are looking for something else. Some parties present themselves as well, also because of the CPB story. Do you want to be in control then we will visit you. Well then they come over and they talk about a tool. And the NVZ has a tool for that as well. So we are looking into that. That is useful."

[HCSM:06] "Yes, yes, I have a tooling with which I do things and it contains certain measures. Those are connected to it, those derive from it. I have a set of measurements that is connected to the measures prescribed by the NEN 7510, how the NOREA and the NIAZ view them and when they audit us and how we equipped it."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Tooling	No tools are used	Ad hoc developed tools are used	Documentation and structure aiding tools are used	Software based tools are used to streamline the information gathering process and aid analysis process	Software based tools are used to provide a real-time input in the information gathering process, analyze this following the used models and show the results in a dashboard

Figure 43: Maturity Dimension 5 Tooling

7.3.6 Information Gathering from Internal Sources

Information considering the main processes and their assets, threats, vulnerabilities, and controls that need to be identified for the risk assessment (requirement 3, 5, 6 and 7) is often present within the organization. A distinction can be made in the types of information gathering from internal sources shown in Figure 44. Information can be obtained from different testing activities (requirement 23), e.g. penetration tests, IT audits, input-output testing and code analysis, through different types of monitoring activities from employees within the organization (requirement 31), e.g. by interviews, workshops or questionnaires, through incident reports, through cyber security exercises and from registers and databases.

Element 6: There should be a structured approach in each risk assessment which systematically obtains relevant information from internally available information sources in a logical and complete manner. Information from interviews and workshops with employees are often used first and completed with information gathered from internal systems. Often managers of care divisions, asset owners and board members responsible for processes or assets within hospitals are used as source. However when this process is more sophisticated dependence on information directly from employees might reduce and been used more for validation and awareness purposes. Then more information from testing, monitoring, reporting, exercising, registers and databases will be used. In an optimized state these information sources are connected directly to a software based tool.

Important to note is that except for information gathering from employees most processes are not part of the risk assessment process, but rather the information resulting from these processes are used. Information from registers and databases refers to asset, vulnerability, threat and control lists stored in registers and databases, not to be confused with the other information which may be stored in databases as well. The full maturity level is provided in Figure 46.

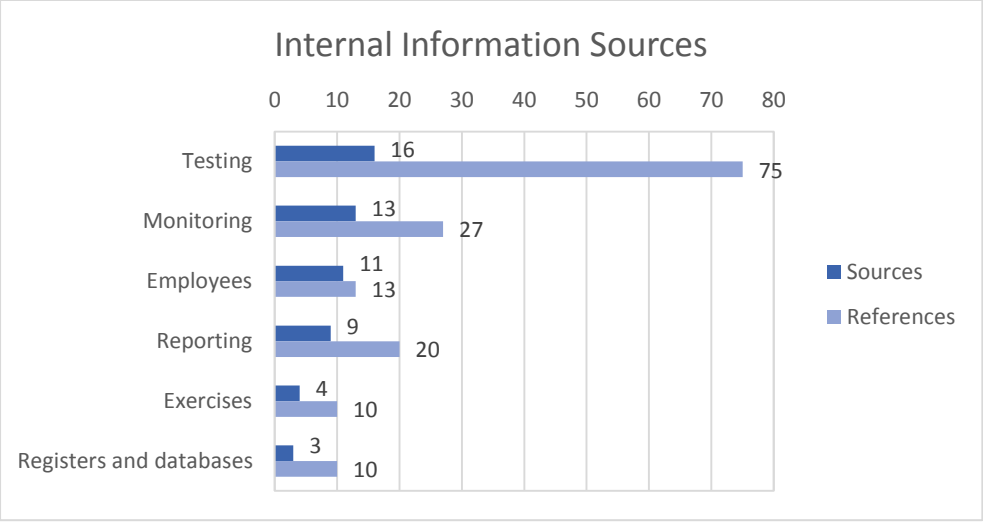


Figure 44: Internal Information Sources

Testing

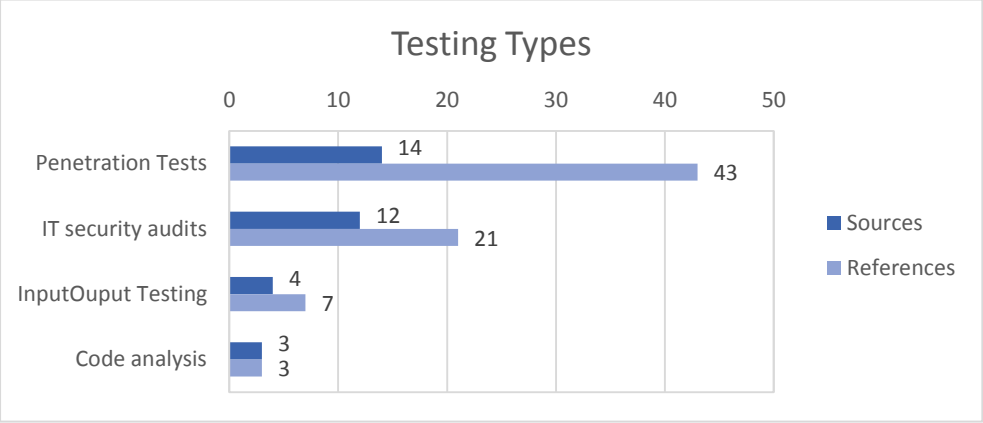


Figure 45: Testing Types

Testing is a strong method to identify vulnerabilities in the organization and systems. In Figure 45 an overview of the testing types is presented. Testing can be done on several levels. A high level form of testing is the use of social penetration testing in which a mystery guest or social engineer tries to exploit the human weakness, for example through phishing mails. IT audits are another form of high level testing in which on a tactical level the implemented controls are checked. More technical tests are penetration tests on web portals, testing whether the inserted input delivers the expected output and code analysis.

Penetration tests:

Penetration tests are tests developed to test whether it is possible to obtain access to certain assets, which should not be possible. This could happen on a higher level using social engineering and on more technical levels. Mostly this type of test is used to test internet connections such as web portals as potentially everybody with internet access could obtain access when the security is not in place. The quality of technical penetration tests could vary from simple automated vulnerability scanners to highly skilled ethical hackers using a variety of tools and creative methods.

[HCSM:03] "It does not happen often enough, but I believe you should run a vulnerability scanner on your network or all your systems at least twice a year. So not over the clients, but over the server systems, but it is even more important that they follow a hardening norm for the adhesion of your hosts and test those hosts if they still respect the hardening norm. Whether no portals and servers are needlessly open."

[HCSM:05] "Once a year we have an ethical hack. Then we let them research us, as try to enter us from the outside."

[HCSM:04] "Only for the outside of the hospital, there where things such as personal data is used. And the risk is large to be hacked on that side or to lose information on that side."

[HCSM:07] "That is a year or two ago already, we hired a company that send a mistery guest to walk around here, they also send phishing mails and did some calls, for example to the helpdesk to ask for a password."

IT security audits:

IT security audits are often include other forms of testing, such as penetration tests. IT audits are more focused on tactical level implemented security measures, such as access management. Often they focus on financial systems in fraud prevention. However important IT systems, such as the EMR are often included in these audits as well. IT audits are mandatory done on the financial systems yearly by external auditor, but internally or in collegial collaboration these can be executed in a broader scope and more frequent.

[HCSM:10] "Yes, but here are thus the audits, but I will call them technical audits, the penetration tests and alike are included in them, they contain both organizational and technical audits and they provide you with the information of your current position."

[HCSM:07] "Well the accountants look a little bit around the financial systems, so that is actually the only real yearly audit. And ehm, what we need to do of course for the NEN is to let your organization being audited, provide an auditor with insight on how to handle that, how you look at the processes, how you look at the systems."

[CSE:04] "It is not necessary to always let an external company do an audit, you can do it internal as well. You have a lot of good methods for that with collegial reviews. But it depends how mature they handle that. It could be possible that one club audits the other. Collegial reviewing."

Input-Output testing:

Input-Output testing is testing whether systems produce the right output at certain inputs. Especially in architectural changes or when systems connected in chains are updated this might provide valuable information. Especially when no direct action is undertaken this kind of testing provides vulnerabilities that should be taken into account in the risk assessment.

[CSE:06] "The doctors should actually test that, because they know best that if something goes into the system, what should be the output. But they usually do not have time for that. So it usually is the ICT that tests that and they do their best, but in the cases that doctors would be able to make up, it goes wrong."

[CSE:06] "We often saw reports of medical devices that are just connected to a network and it is doing things that are unknown to the manufacturer and unknown to the hospital. Yes and that is a difficult one, it would be nice if you could monitor that, like what data traffic is going in and out."

Code analysis:

Code analysis is the analysis of program code rule by rule. This is often a very expensive process and not used often.

[HCSM:10] "Yes, for really important things we do code testing. But someone does it for us, we do not do it ourselves. It is very expensive, that is not something you do just like that."

Monitoring

Three main types of monitoring exist: external data or actors trying to gain access to assets, monitoring outgoing data and monitoring of internal data behavior. Monitoring could provide interesting information considering attack frequencies and malware or threat actor behavior. Also internally is could be used to identify unwanted interactions between connected systems.

A special form of monitoring are honeypots. These are traps set to identify and observe malware and gain more information about threat actor behavior and tactics. Although not used by the interviewed experts they might provide added value to battle and better understand threat actors [HCSM:06, CSE:01].

[CSE:01] "There is certain intrusion detection software. You could use it to see which data goes to a medical device. That is quite unambiguous information, the communication flow should in essence be limited, since it should only communicate with one other system. You are able to monitor that very well, you could use some sort of learning system that learns what the standard communication is and all the abnormal communication could be set aside to let someone check it."

[CSE:04] "You need to monitor what happens."

[CSE:05] "There are hardcore technical options. Those are usually called data leakage protection, DLP. Or data loss prevention, those are synonyms. Eh, and that is just technical and monitors where the data goes. And if someone tries to e-mail it outside a signal is given and a security officer is warned to check it out."

[HCSM:10] "Yes, yes, we have systems in our organization on which suppliers do monitoring and they report us certain statuses and based on that we are able to do analyses ourselves. And based on those analyses you are able to look at threats."

[HCSM:05] "What we do mostly, we implement stuf that monitors and updates the security. You buy a more expensive firewall with wildfire threat prevention, because when he sees traffic what he does not recognizes he will connect to the internet and looks for the pattern to see if it is recognized or not. And if not it is shut down."

[HCSM:09] "We do not yet have DLP, not yet an intrusion detection system, we do not have prevention either, but we have normal monitoring. Thus of the exchange of e-mail traffic, your network traffic monitoring. If there is a virus at a station it is nicely reported, central to the administrator of the anti-virus environment."

Employees

Often employees are a rich source of information concerning cyber security risks. Hospitals with a low level of cyber security usually gain the bulk of their information for their risk assessment process from this source. As other sources become richer, the portion of information gained directly from employees might decrease. A wide variety of methods is used to obtain information from employees such as sticky posting, workshops, questionnaires and direct interviews.

[HCSM:01] "We have in this room, or the one next door, a poster with categories of infratechnique, the AIC classifications that are nameable hanging behind it and we said, boys, past stickies on it that you would identify as a risk, a threat, a vulnerability, you may use it all together as far as I am concerned."

[HCSM:03] "That are indeed standard threats, a Looije has about 25 standard areas. In fact that is the starting point from which you and some experts in a workshop setting can visualize how these threats might occur here."

[HCSM:04] "By asking questions about all aspects that are within the scope, about the system, but also about the people that work with it."

[HCSM:07] "That is based on an interview with the system owners, functional designers and key user. Then it is worked out based on a structured questionnaire. You try to oversee where the threats are and possible the impact when something goes wrong."

[HCSM:08] "That is mostly in committees, you gather people that have something useful to say, you put them together."

[CSE:04] "Ehm, one of the eye openers for me was actually, we organized a session and we indicated data profiles and where are the crown jewels. And we looked okay, how are cybercriminals able to enter the organization and when they have entered how do they reach to the crown jewels.

Reporting

Reporting refers to all kind of reporting activities that might occur in a hospital. On the most basic level, this could include registered reports of employees concerning vulnerabilities or incidents. It could also include helpdesk incident management applications or even complete whistleblowing activities.

[CSE:04] "Yes, they often have some kind of helpdesk incident management application. A lot of hospitals use Topdesk. That provides them with support. In that software it is possible to register incidents."

[HCSM:02] "If there is an incident or a patient safety incident, report, report, and again report, so that we are able to learn from and improve the situation."

[HCSM:02] "We have a whistle blower policy. And that is managed through the department ICT of the <…>. And in that policy is the internet and computer use included. In practice intrusion incidents and alike enter through the department ICT, other whistle blowers reports often go through the media. Very simple, people do not go to their boss anymore or talk to their manager. They go to the paper immediately and tell them what goes on. So

that is strongly incident driven. The last couple of years the <…> was in the paper several times with all kind of incidents. But there is a formal whistle blower policy that enables you to go to an ethical commission with all kind of misconducts."

[HCSM:04] "Almost all ICT in smaller hospitals is outsourced. Thus there is always a desk between and the trouble shooting of such is difficult if you do not have incidents."

[HCSM:08] "Yes, we have different systems to monitor information security. And that is mainly through the ICT helpdesk. They have a special monitoring tool. Or a registration tool of reported incidents."

[HCSM:10] "You say yes, you have different channels, one of the aspects if of course your end users and if they observe that something does not run properly or they have information concerning vulnerabilities that they will nicely report to such parties. That is a goal to enable them to report and actually report."

Exercises

Although not often used, exercises could be a valuable source of information considering the impact and success factor of certain types of cyber threat manifesting in the organization. This could include simple table-top exercises, but could also become as extensive as full unannounced red teaming exercises.

[HCSM:09] "Unfortunately enough, because we have good emergency procedures, but unfortunately enough we have to little possibilities to test them. Just like the BA does security exercises."

[HCSM:10] "In your risk analysis you might need an emergency plan, which should be organized and tested and because those emergencies an organization will be equipped and new findings will be found a they will provide information for new risk analyses. Like, wait a minute, we notice that there usually only is one administrator and if that one is sick, nobody is here. That kind of information you would take as input in your new risk analysis. That contains a lot of trend analysis…"

[CSE:05] "Yes and in general the trick at such a red team exercise at the highest maturity level is to start such things at 3 o'clock a.m., to obtain an overview of the reachability of employees. And you will let them work for 48 hours straight, often in the weekend, to see how far they would go. I can imagine that if you do this during Christmas or in the weekend a couple of your people that are needed to solve the crisis, internal or external, will not be reachable and what would you do in those cases? And such a scenario, as second step, could be written down into detail and discussed with people."

Registers and databases

Registers and databases are often valuable resources of assets, threats, vulnerabilities and controls. Assets are often stored in a configuration management database (CMDB). If a threat and vulnerability management process is in place, these are as well in a database. Implemented controls as well can be stored in control registers or risk assessment tools.

[CSE:04] "Of course they need a CMDB to know where it all runs. In such a CMDB you should be able to classify what is critical and less critical."

[HCSM:10] "Let's see the system itself, classification I already mentioned, that should always be available in your CMDB and the connections between systems is usually very important for us, that is how we approach the information systems, is it just in-house or is it, thus more according to the environment, the domain in which the information system is approached, if that is done through the internet that would of course require extra attention opposed to an intern system that is only internally connected."

A CMDB, previous risk assessments and a control overviews register are used [HCSM:11].

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Information Gathering from Internal Sources	No information is gathered from internal sources	Information of assets, threats, vulnerabilities and controls is obtained by ad hoc interviews and complemented with ad hoc reports constructed from threat and vulnerability indicators	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes and registers	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes, registers and systems	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes, registers and systems. Internal information is constantly renewing and improving.

Figure 46: Maturity Dimension 6 Information Gathering from Internal Sources

7.3.7 Information Gathering from External Sources

Element 7: Additional information mainly concerning threats, vulnerabilities and control effectiveness can be gathered through a variety of external sources. Information considering incidents of similar hospitals may prove interesting as trends in such could be detected and hospitals could take necessary measures to prevent them from happening at their organization. Also information considering previously not known vulnerabilities should be used before threat actors would be able to exploit these. Figure 47 gives an overview of the mentioned external information sources. At a high maturity more and richer external information sources are used and a structured approach is used to extract the right information. In an optimized state sources are reviewed on their usefulness and quality and new and improved sources are continuously searched for.
The full maturity level is provided in Figure 48.

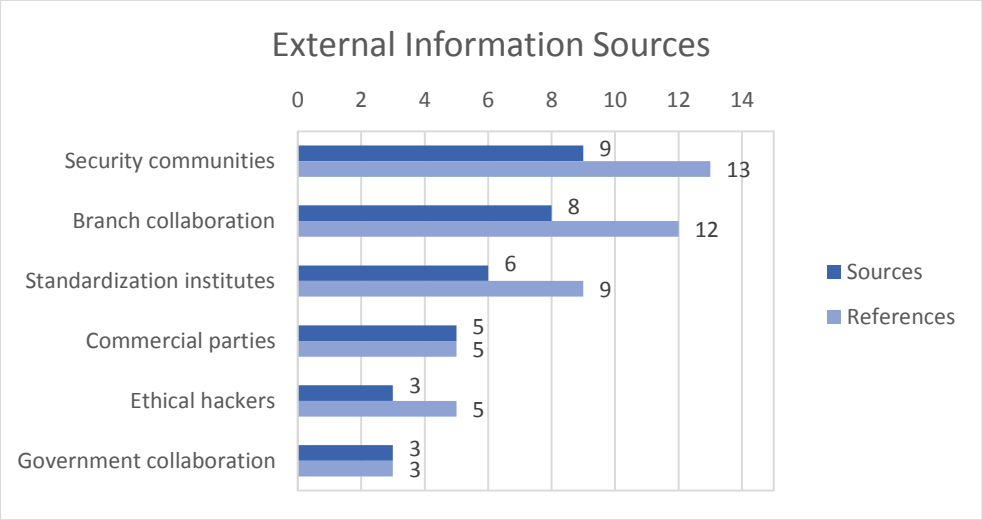


Figure 47: External Information Sources

Security communities

Security communities are valuable resources of threat landscapes, fact sheets, malware types and reviews considering controls (requirement 22). It is however always important to take into review the quality of the source before using information published by them.

[CSE:05] "I would use the OWASP for everything that is web related and I would use the NIST for everything cloud computing related."

[CSE:01] "Every application can have its own weaknesses. And at that point you are able to rely on the available frameworks. If there is a web application, in this case it is not, you could obtain the OWASP guidelines. For SCADA like systems you could obtain the SANS controls. You have some papers with all possible software mistakes that people could make. And those are updated continuously. <…> Well they are maintained by the community. Thus in those cases you rely on something that continuously is maintained. I believe it is important with other methodologies that your input stays up to date."

[HCSM:04] "Gartner develops a neat report yearly and the virus, the anti-virus software developers, they develop nice reports and there are open source sources that provide trend analysis."

[HCSM:09] "The actualities indeed. Yes, yes, I think the source is always important, where does it result from. Just as described in the CSBN they refer to the NCSC and Fox IT is mentioned in there as well and those tell, those sources are quite reliable. Look if it is in some computer magazine you will want to know the source, where is derived from. You can scare everybody, but… We would certainly take those into account."

Branch collaboration

Branch collaboration is a form of horizontal collaboration (requirement 22), organized by a branch organization, between similar organizations. For general and top clinical hospitals in the Netherlands this is organized by the NVZ. For academic hospitals in the Netherlands this takes place in academic hospital context organized by the NFU and in academic organization context organized by SURF. Also local privacy or security committees exist, in which some hospitals participate together with other local (healthcare) organizations.

[CSE:06] "I know that the NVZ is working on that, they gather once in a while with security officers and they exchange mainly knowledge and know how."

[HCSM:02] "But there they use all kind of material of the NFU, the federation of academic hospitals. But also hospital associations, there are all kind of models developed with questionnaires, thus according to best practices there is quite a complete picture on how to be complete in your risk assessment."

[HCSM:06] "That does not stand, you generally see everybody and that is what you see at the NVZ in our counsel, where we meet every quarter and of the 92 hospitals there are always 40 or 50 at the table. So yes, they are not all present and that has a reason. We sometimes have to do with long hours, but we have been there with 60 or 70 as well."

[HCSM:10] "So you must receive a signal somewhere. When you do not receive these within your own hospital that is difficult. That is why those collaborations are so important, also between academic hospitals for example, if you have a trend with the eight of you, if at some certain incidents occur it should be noticed, you should be alert to that."

Collaboration occurs for academic hospitals as well in SURF context [HCSM:11].

Standardization institutes

When a closed risk assessment type is used security standards are an important measurement tool. In closed risk assessment methods these are less important in the risk identification process, but may still be used as a reference. Standards such as the ISO 27005 contain a lot of resources for risk assessment processes, such as standard threat and vulnerability lists (requirement 26).

[HCSM:01] "In general you cannot say this is secure or this is not. That is the case, we work a lot with baselines for surfer configuration and network configuration. And such a baseline is just a measurement tool. It is just like a ruler, you can hit with it, but it does not do more. I want to see whether the right measurement is taken. That the sever complies with the baseline. Whether he deviates on 2 points and he approved it and this is the reason. Then you are in control over such servers and the baseline. Well in fact you have that and it depends on the baseline, since that baseline alone does not offer you any security."

[HCSM:05] "Well that was the old NEN 7510, which still contained norms. The new one is mainly process focused. You need to work on your processes and you can lay out your own norms. That makes life a lot more interesting, you are consciously aware of the process and can decide yourself where you decide to end."

[CSE:05] "I would chose to, no, I would follow standard frameworks, I would take the ISO 27001 and 2 and take things from there, I would take the OWASP for everything that is web related and I would use the NIST for cloud computing, for all that is cloud computing."

Commercial parties

To obtain extra knowledge about for example current threats and trends, information could be bought at commercial parties specialized in cyber security. Also collaboration with suppliers of information systems, medical devices and SCADA systems could be useful, as they could pass through information concerning incidents and discovered vulnerabilities.

[CSE:05] "What if your risks were completely unknown, then you would talk with experts to which you will literally ask what the risks are."

[HCSM:05] "Next we often have a session with our supplier <…>, what are the threats, how can you mitigate them."

[HCSM:10] "In this case we have the collaboration with suppliers that we have as well. So I miss those, they deliver services as well that provide us with information at the threat side."

Ethical hackers

Ethical hackers are often individuals closely connected to script kiddies and cyber researchers, these however are prepared to inform the organization of their vulnerabilities. For the organization to harvest this free or cheap source of information a good responsible disclosure policy should be in place. It should however always be careful with this source to prevent the hospital provokes additional damages.

[CSE:02] "Yes, but we have a protocol for that. If there are hackers. We reward them for the fact that they hacked you and informed you about it. So a nice protocol. So report what you have hacked and how you did that. Provided that, only, on one condition, provided they give you the time to solve it."

[CSE:05] "Do you have responsible disclosure in it? A good responsible disclosure policy. <…> That is something, certainly when talking about cyber, when people report things to you voluntarily, you should answer timely and appropriately. That might provide you with a lot of free information."

[HCSM:09] "But if it origins from an external source then I believe it is important to know his motives to do such. If someone reports it, because maybe he does it to gain something from it. Does he report it because he believes that the healthcare is important? There are always interests. You need to be clear that those interests are not contradictory. Otherwise you will take something for granted what might be your biggest downfall. And you should watch for that, you should stay critical.

Government collaboration

Government collaboration is a form of vertical collaboration, in which government departments collaborate with hospitals and provide them with additional information that result from their activities (requirement 21). In the Netherlands this form of collaboration is mainly done from the National Cyber Security Centre (NCSC) and the national intelligence and security service (in Dutch Algemene Inlichtingen en Veiligheidsdienst or AIVD). The main form of collaboration mentioned was the ISAC-Zorg, an information sharing and analysis center for the healthcare in the Netherlands [CSE:02, HCSM:07, HCSM:10]. Other activities may include the distribution of fact sheets or the warning of hospitals.

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Information Gathering from External Sources	No information is gathered from external sources	An ad hoc search is done for relevant current threats and vulnerabilities on the internet	Important external threat and vulnerability input sources are identified and consulted	Important external threat and vulnerability input sources are identified and consulted. Partnerships are established and used to improve the information quality.	Important external threat and vulnerability input sources are identified and consulted. Partnerships are established and used to improve the information quality. A process is in place that rates the usefulness and quality of current sources and actively seeks to obtain new relevant sources

Figure 48: Maturity Dimension 7 Information Gathering from External Sources

7.3.8 Identification of Consequences

Element 8: The identification of consequences process uses the information gathered and combines these (requirement 8). In its simplest form this merely uses the threats, in more sophisticated forms this information is used to developed incident scenarios, depicting what could happen, preferably taking into account connections in networked environments (requirement 14). At higher maturity levels this is done structured, taking into account all accessibility, integrity and confidentiality consequences (requirement 13). Consequences at hospitals are often related to: patient and employee safety aspects, financial aspects, hospital brand image aspects, compliance to law and employee morale. In the optimized state an evaluation is done concerning the quality of previously made scenarios to iteratively improve their quality.
The full maturity level is provided in Figure 49.

[CSE:02] "The development of scenarios. But with a lot of things you are able to gain a quick overview. If it is not possible anymore to make heart movies, well then you know like guys there is a group of people that should be transferred, which is limited."

[CSE:04] "And then in what kind of scenarios is it possible to access the crown jewels. <…> So scenario thinking. You cannot check everything. However on a certain moment when you know those scenarios and okay on these points measures are taken and on those points less, or we thought less of that. But well, that is the weakest link in the story. Or how do the users deal with that situation. In such a way you gain a complete risk landscape, such that how is that put together."

[HCSM:08] "You appoint individual threats I mean. We did not really work with scenarios I believe. We should look into that."

[HCSM:10] "Yes in that regard we look at the behavior and environment. Thus as I just said, integrity is high, what does is mean when another system suddenly cannot guarantee that, what does that mean and how do you mitigate that. And how do you check that? How do you guaranty that that information is stored correctly."

[HCSM:10] "Yes what we as organization do is define 35 to 40 threats and periodically evaluate these with the organization whether we on management level still believe whether it is a real plausible threat. You will then gain an overview of the management part. We do the same for the reported incidents to see whether, well it is a different view, vision, well, what does it mean for the threats we see and from that a picture is developed for the <…> and that is used for the risk analysis."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Identification of Consequences	No identification of consequences is done	Incident scenarios are developed ad hoc based on the gathered information	Incident scenarios are developed based on the gathered information following a predefined structure or method	A structured method is used to integrate gathered information and develop incident scenarios for accessibility, integrity and confidentiality degradations	A structured method is used to integrate gathered information and develop incident scenarios for accessibility, integrity and confidentiality degradations The incident scenarios are constantly improved based on previous made scenarios which are evaluated

Figure 49: Maturity Dimension 8 Identification of Consequences

7.3.9 Assessment of Consequences

During the assessment of consequences process an assessment is made of the impact of the identified consequences for the organization. This is often referred to as the business impact assessment.

Element 9.1: In some organizations the assets are ranked on importance first (requirement 4), furthermore the impact a possible incident could have on assets and processes is rated as the incident impact (requirement 9). In its simplest form the impact is rated on an ordinal scale (e.g. low, medium, and high). The rating can become more advanced by rating on damage ranges (e.g. 0-1000, 1001-10.000, etcetera) or even fully quantified. Some models use a gross impact and net impact. The gross impact is the impact on the organization without mitigation. The net impact is the impact the incident will have after subtraction of mitigating measures, such as back-up systems.

Element 9.2: To improve the assessment process often the impact is rated on different impact areas (e.g. finance, safety, reputation, compliance to laws and regulations, employee morale, etcetera), which allows for targeted and defined risk assessment. To obtain more sophistication (requirement 12) and more quantification (requirement 17) of the consequence assessment, historical data of incidents at the own and other similar organizations can help to gain an idea of the real impact an incident will have. At the optimized maturity level a method is in place to translate the historical data to the current situation of the organization as opposed to letting someone assessing it ad hoc.

For the assessment of consequences it is always of importance to involve the stakeholders as they have the best insights in the consequences of incidents for their business. The full maturity level is provided in Figure 50.

[HCSM:05] "Ehm, no we have a scale from 1 to 5. 5 is complete indispensable, the care process stops. 1 is, well, we can live a week without it."

[HCSM:07] "Yes well, concerning the availability we have a few questions, this is the same for integrity and confidentiality. Then we interview the stakeholders and they will rate subjects. You gain a certain score, between one and five. And one is a very low impact and five is a very high impact."

[HCSM:07] "But if you look at the business questions that are stated, thus damage for the patient care, for the business, are management decisions harmed, law and regulations, damage to reputation, trust, of course costs, fraud and then a number is given and with a system a higher score is given and there a lower score and that will result in a final score, thus the total. And this looks quite low, but in the end the highest questions weigh the most. And it is a high score as well, a four. But then again when this happens it is worse. And that, this two, those return later on. And in the same fashion integrity and confidentiality are assessed. There as well we look at damage for patients, damage for care. From there out a score is returned. The law on for protection of personal data, that is where the twos and threes are scored in the healthcare systems. And then indeed the maximal down-time, what is the pain tolerance, if the system is down for an hour it is bothersome, but a day will become difficult."

[HCSM:08] "I believe we rate them with scores from one to five, where the risks were mainly of a financial kind, I do not remember it by heart anymore."

[HCSM:04] "I work from a business perspective. Eh, I always perform a business impact assessment. What I do at the moment, look at my scope, to what we do at the moment, and I figure out who the stakeholders are. At that moment I identify a couple of strategic risks. And within the concept of information security, availability of information, integrity and confidentiality I let them formulate a couple of business statements. Like how long may the systems be down and when should it be back in the air. And they all state it should never go down. Well in those cases I specify the demands we should ask from the suppliers."

[HCSM:04] "I test that against a legal framework, against a financial aspect a human aspect, that is I believe five aspects are that. <…> Yes, that is a renowned list I believe. With five groups. Morale I believe. <…> Of the employees."

[HCSM:09] "Well I believe we always follow the AIC principles. That is what we use, we look at the impact and we prefer to do that with the owners of the data and then we will look how we deal with that. Thus really the AIC, threat analysis, impact analysis."

[HCSM:10] "We can give an indication for the costs of a single system or a double system. Or in case of the integrity of the entering by 1 person, 2 persons, because you should check that, we can incidentally calculate the costs of that, okay, it will cost you this much more if you implement a double system or not. I cannot indicate whether that is acceptable for his business or not."

[CSE:04] "I have to enter or manage patient data, that might be a process or a task. Thus you might say what is the impact when the system is unavailable, what is the impact if I enter the wrong data. What is the impact when I obtain the wrong data. What is the impact when the data is made public. In that regard based you can based on image damage, financial damage, legal and regulations, process frustration in an organization, unwanted media attention, etcetera…<…> Patient safety. And those are then rated on a low, average or high impact."

[CSE:04] "A quantitative aspect is very difficult to assess. It requires you to know the organization well and that often costs more time. To execute that. And often there is no budget and time for such. And the added value of the quantitative compared to the qualitative is in those cases relative little for the extra money that should be spend. In those cases you perform it qualitative and you will try to quantify it, in those cases you can assess financial damage till 150.000 euro, between 150 and 250 and 250 till one million, you may apply that."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Assessment of Consequences	No assessment of consequences is performed	Analysis is done by stakeholders rating incident scenarios on an ordinal scale	Rating is done by stakeholders on damage ranges. Different impact areas are defined.	Historical data of the own and other organizations is used to aid stakeholders with a quantification of the consequence assessment. Different impact areas are defined.	Historical data of the own and other organizations is used to aid stakeholders with a quantification of the consequence assessment. A specific method is in place to translate this historical data to the current situation of the organization. Different impact areas are defined.

Figure 50: Maturity Dimension 9 Assessment of Consequences

7.3.10 Assessment of Incident Likelihood

During the assessment of incident likelihood process an assessment is made of the likelihood that the identified consequences occur (requirement 10).

Element 10.1: In its simplest form the impact is rated on an ordinal scale (e.g. low, medium, and high). The rating can become more advanced by rating on likelihood ranges (e.g. it happens: once a day, once a month,

once a year, once every ten years, etcetera) or even fully quantified. Some models use a gross likelihood and net likelihood. The gross likelihood is the likelihood a threat will occur. The net likelihood is the likelihood the attack attempt will succeed despite of the organization's security measures.

Element 10.2: To obtain more sophistication (requirement 12) and quantification (requirement 17) in the consequence assessment trend analysis on historical data of incidents at the own and other similar organizations can help to obtain a more sophisticated likelihood. At the optimized maturity level a method is in place to translate the historical data to the current situation of the organization as opposed to letting someone perform an ad hoc trend analysis.

For the assessment of likelihood it is advised to involve the stakeholders as they have strong insight in their business. The full maturity level is provided in Figure 51.

[HCSM:01] "Taking the risk perspective. Assess on a scale from 1 to 4 the likelihood that you believe this will happen."

[HCSM:06] "No, we look at the context, how often it happens. <…> Yes, something like that, often in consultation. Those people already work here a long time." On interviewing people on likelihood estimations.

[HCSM:07] "Together with the people around the table in the interview I discuss and assess what the change is a threat happens. So rate it with a value. <…> For example several times a year or several times a month or ones every ten year."

[HCSM:09] "It should not be a gut feeling. That should be statistical."

[CSE:04] "Personally I always find likelihood to be a difficult one, I did it a couple of times different. One way is to give a workshop and everybody gives marks from one to five. A one is low, a five is a high change. With several people it is possible to generalize the results. That was quite meaningful. Another time I told people to motivate there reason, then people should motivate why they think that change is higher. Another aspect what I found interesting is that risk, a supplier of a risk management tool, did a study using an insurance approach. Insurers strongly look to certain risk factors whether they are present or not. For a boy that, eh name something, I do not know how old you are, that is 18, or 19, or 20, something like that and he obtains his driver's license, buys a care often and mostly not a new one. Well the change that something happens with it is larger than someone of 50 like me who drives more calmly with those kind of things. That is how an insurance company looks at statistics. And what they did, what that party did, they did research on organizations that have implemented such a norm like the NEN 7510 for example. What is the change they become a victim of an incident, against companies that did not or only partly implemented it."

[HCSM:02] "Yes, those figures are all known, you can find them on the suppliers website as well." Concerning down-time.

[HCSM:10] "Yes, well that is difficult to determine when you are attacked from the outside, why does someone choses you as target. Maybe because he expects that you are weaker than similar organizations. But it is also possible that you possess more interesting information than other organizations. That is difficult to determine. Pragmatism is a factor in this as well. That will always be the case. Even if you look at the five areas there is still a part assumption. And that will always be there. We mostly look at historical incidents. <…> We also look at trends. Like I said with for example hardware. There have been a lot of hardware malfunctions. You may say that does not happen, but a certain change should have been made in the management or development of hardware platforms that gives you a reason to say otherwise."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Assessment of Incident Likelihood	No assessment of incident likelihood is performed	Analysis is done by rating incident scenarios on an ordinal scale	Analysis is done by rating incident scenarios on likelihood ranges assisted by information gained from threat and vulnerability trends	Trend analysis is done based on historical data to quantify the likelihood of incident scenarios and aid the stakeholder quantifying the likelihood.	Trend analysis is done based on historical data to quantify the likelihood of incident scenarios and aid the stakeholder quantifying the likelihood. A specific method is in place to translate this historical data to the current situation of the organization.

Figure 51: Maturity Dimension 10 Assessment of Incident Likelihood

7.3.11 Risk Evaluation

Element 11: During the risk evaluation the risk scores (often impact * likelihood) are evaluated (requirement 11). An often used tool to aid this process is the risk matrix in which likelihood and impact are mapped against each other, leaving a high likelihood, high impact risks to be mapped in one corner, which certainly need attention and low likelihood, low impact risks to be mapped in the opposite corner. At higher maturity levels a structured method is used to clearly identify a gap between the acceptable risk and the current risks (requirement 12). This increases the insight in the need to address certain risks, which cannot always be done in risk matrixes, e.g. some medium risks are acceptable, while others are not. The decision what an acceptable risk is depends on the risk appetite of the organization. Also higher risks could be accepted when mitigation of them might drain too many resources. At an optimized maturity level feedback is used to iteratively improve the risk evaluations.
The full maturity level is provided in Figure 52.

[HCSM:04] "Is it a low level impact? In those cases I am able to work with checklists or a baseline, with matters that already have been researched. So the business statement, that is weighted against the risk analysis after that and it tells you something about the detail of the risk analysis. Should I do a detailed risk analysis then I will continue till the last screw and that means that you will indeed have a lot of sessions, with all, what is the name, risk assessments were threats are presented, very specific for that subject that should lead to measures. Well that will provide a whole list of things. And those measures you will compare against the business impact, like okay the stakeholders said they think this is important. Thus the attention will most likely be on those mitigating measures to implement them first. Well, those are returned to the stakeholder. And they are confronted with their business impact, and this are the measures coming forth from it. And what you told me should have been according to these measures that I present to you. So you should at least implement these. Well that is when the price tag arrives."

*[HCSM:07] "Whether those threats are defined as a seven for availability and an eight for integrity and a seven for confidentiality, what is the change they occur and is it possible to further specify the impact. And in those cases you create a matrix with the scores that I have multiplied <impact * likelihood>. <…> And then you gain a number and you have red, orange and green risks."*

[HCSM:06] "Yes, yes, those matrixes with on the right or left above starts with red and diagonally down."

[HCSM:01] Yes, in the safer method are a few methods to prioritize risks. And then you end at a matrix."

[CSE:04] "Because even a hacker chooses the largest change and the least amount of effort. And you should prioritize your priorities as such, how am I going to arrange my security."

[CSE:02] "You might say, the impact is higher than 100.000 euro. The damage is higher than 100.000 euro, when you will need 10 euro to prevent that, you should do that. But if the damage is 100.000 euro on a daily turnover of 10 million, what no hospital has, yes, well, okay, you might accept it."

[HCSM:08] "If the gross score of the patient safety factor is the highest, you might want to take security measures there first. And you might be searching, you have risks, and you can weigh your risks as well. I am not

sure if we had a separate weighting factor. Probably it would have worked in that way. In that case you are able to say a risk with patient security is more important than a financial risk."

[HCSM:10] "Well the impact that remains those are the risks. So what remains, well the availability is high, but we have a single system equipped according the requirements of the stakeholders and the stakeholder says I accept that. But then I will tell them, are you sure you are accepting that the system will be down longer in case of fore example hardware malfunctions. Do you agree, yes or no. And if he tells me yes then the impact might be your business operations halt. If you tell him this system is of such an importance that if it is down your whole operations will be down. Do you still agree. Well then the game begins, what is the importance of the system for the stakeholder and what kind of risk are you willing to accept."

[HCSM:04] "Well, because of the DigiD I tackled the website. Purely because appointments are made there and thus contains personal data. And the whole DigiD is for example in the risk assessment turned off because it became too expensive. <…> Well, that is a business decision. I did the business impact, using the stakeholders and said, listen, this should comply to legal requirements. This is the price tag. Well then they took a look at it, we only use it a certain times a month, compared against the costs of a penetration test and the maintenance costs that are included. Turn it off. Well that is a risk evaluation. Risk gone."

[HCSM:06] "And what is their risk appetite. About such a hospital, how far are you going? Take for example the risk appetite of a hospital where they tell a security officer that they are allowed to spend two hours a week for it, the risk appetite is quite high there. That is what they are saying, let it go, as long as the IGZ does not visit me and the CBP does not visit me, then I will tell them I do not act to it. Or that is nice that you would like a security officer, but we are not spending money for that. So your risk appetite is quit high and as security officer you should do something about that. Otherwise you will constantly keep on planning, but nothing will happen."

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Risk Evaluation	No risk evaluation is performed	Risk evaluation is done ad hoc and provides a rough ranking of risks, which is validated by stakeholders.	Risk evaluation is done with a structured approach assisted by risk matrixes and validated by stakeholders	Risk evaluation is done with a structured approach gaining insight in the gap between acceptable risk and current risk. This is validated by stakeholders	Risk evaluation is done with a structured approach gaining insight in the gap between acceptable risk and current risk. This is validated by stakeholders. Based on feedback the risk evaluation approach used is iteratively improved

Figure 52: Maturity Dimension 11 Risk Evaluation

7.4 HCRAMM Version 1.0 Result Overview

The result of the HCRAMM version 1.0 can be found in Appendix D. An overview of the framework and explanation per maturity dimension is provided in Figure 53.

		0: Incomplete 1: Initial 2: Repeatable 3: Defined 4: Optimized
Scope	Scope and Frequency	*A clear scope of risk assessment is needed. Also it should be clear how often this should be performed, under what kind of circumstances.*
People	Risk Assessor Authority	*The risk assessor needs a form of authority to perform his job well, his authority should be clear in the organization.*
	Stakeholder involvement	*Stakeholders from all disciplines should be involved or represented in the risk assessment process.*
Techniques	Risk Registration	*Information concerning risk assessments should be stored central and maintained, preferably in a risk register*
	Tooling	*Tools should be used to aid the risk assessment process. A lot of sophisticated tools could be used improve the quality and efficiency of the process.*
Information gathering	Information Gathering from Internal Sources	*A structured approach should be followed to obtain data from internal sources.*
	Information Gathering from External Sources	*A structured approach should be followed to obtain data from external sources.*
Analyses	Identification of Consequences	*Gathered information should be combined into incident scenarios according to certain principles.*
	Assessment of Consequences	*The consequences of possible incidents should be assessed.*
	Assessment of Incident Likelihood	*The likelihood of possible incidents should be assessed.*
Evaluation	Risk Evaluation	*The risks and their values should be evaluated whether they need to be dealt with and in which order.*

Figure 53: Overview of HCRAMM v1.0 framework

8 Survey

In order to further improve the maturity model and test the maturity model in the real world a survey was developed based on the HCRAMM. The results of this survey will provide an insight in the maturity of risk assessment in Dutch hospitals and identify certain aspects that provide large opportunities for improvement. First the development of the survey will be explained and after this the results of the survey will be discussed.

8.1 Development

In this sub-chapter the translation approach from the HCRAMM to the survey is explained. Starting with the translation of the question and followed-up by the score system which will be used.

8.1.1 Translation

In order to enable hospital to measure their maturity level (ML) per maturity dimension (MD), the maturity model was translated into a survey (Appendix D). The individual cells in the maturity model are translated into questions representing certain capabilities. Some maturity dimensions however consisted of several elements (described in chapter 7.3) and could thus not be united into one question. These elements each obtained their own question. The mapping of the questions per dimension and per element is shown in Table 20.

Maturity Dimension	Dimension Name	Element	Questions
MD 1	Scope and Frequency	1.1	10
MD 1	Scope and Frequency	1.2	11
MD 1	Scope and Frequency	1.3	12
MD 2	Risk Assessor Authority	2	13
MD 3	Stakeholder Involvement	3	14
MD 4	Risk Registration	4.1	15
MD 4	Risk Registration	4.2	16
MD 5	Tooling	5	17
MD 6	Information Gathering from Internal Sources	6	18, 20
MD 7	Information Gathering from External Sources	7	21
MD 8	Identification of Consequences	8	24
MD 9	Assessment of Consequences	9.1	25
MD 9	Assessment of Consequences	9.2	26
MD 10	Assessment of Incident Likelihood	10.1	27
MD 10	Assessment of Incident Likelihood	10.2	28
MD 11	Risk Evaluation	11	29

Table 20: Maturity Dimension and elements to Question Mapping

As the maturity model was not yet tested in practice feedback was gathered in the form of open questions asking respondents for feedback concerning the survey.

8.1.2 Score System

Most maturity dimensions are build up from one element. In those cases the score rewarded is simple as each maturity level has one answer. Answer (a) will correspondent with maturity level 0, answer (b) with maturity level 1, etcetera. This is the case for maturity level 2, 3, 4, 7, 8 and 11.

Maturity dimension 6 is a little more complex as question 18 only provides information about the structure. To obtain maturity level 3 and 4 information from registers and systems should be obtained as well. Therefore for each consecutive answer at question 18 1 point is added, starting at zero (corresponding with level 0). As there are four answers a maximum of 3 points can obtained with question 18, which corresponds with maturity level 3. When in question 20 registers are added as an information source a half point is added. When in question 20 systems are added as an information source another half point is added, concluding to a maximum level of 4.

Maturity dimensions 4, 9 and 10 consist each out of two elements, each represented by a question. In this stage for now each element has the same basic scoring as the maturity dimensions with one element, except that the total score is divided by two, since twice the questions may lead to twice the points. This structure is chosen as no clear difference between the importance of these elements was found in the literature or interviews. Logically the most complex element is set on higher maturity levels, but for the sake of the survey this judgment will not yet be implemented.

Finally maturity dimension 1 consists out of three elements. However they are not all of the same value as element 1.1 (scope both on policy and technical level), while during the interviews only little hospitals implemented this element fully. A probable reason for this is that it drives up the costs for a hospital much more than the other two elements. Therefore this element was needed to upgrade from maturity level 3 to 4. The other two elements would provide an equal amount of points, filling up maturity level 0 to 3 evenly, meaning that for each consecutive answer 0.75 points would be given.

The placing of the elements on certain maturity levels is at this point based on the concept of that maturity level. It will be tested whether the structures used in maturity dimension 1, 4, 6, 9 and 10 still hold up to this logic based on the answer patterns given by hospitals, for example if one element is more often fulfilled than another one within the dimension, this will lead to the assumption it is of a more lower maturity (i.e. hospitals first obtain this element and then the other, higher maturity element).

8.2 Results

This sub-chapter presents the results of the survey. It will first discuss the demographics of the participants, followed by the maturity results of the hospitals and finally discuss feedback on the HCRAMM by the participants.

8.2.1 Demographics

Of the 87 hospitals in the Netherlands 14 (16.1% of the total population of Dutch hospitals) participated in the survey. One was excluded as none of the maturity model related questions were filled in. An anonymized demographic distribution of the interviewee's functions is presented in Figure 54, the types of hospitals they represented are presented in Figure 55.

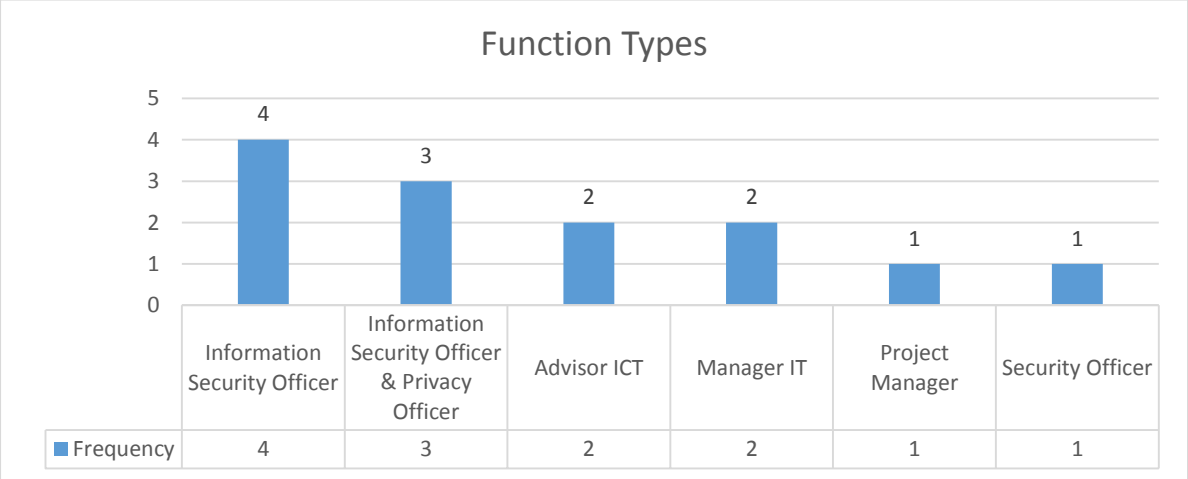


Figure 54: Frequency Function Types of Surveyed

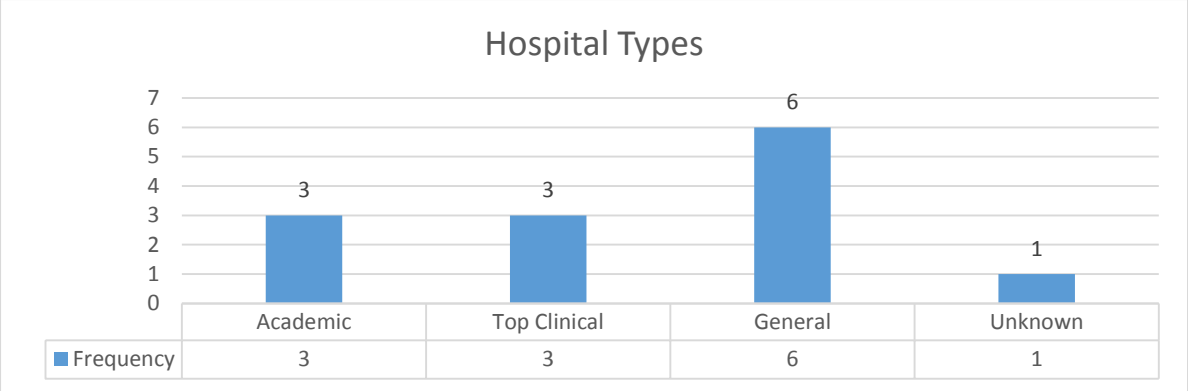


Figure 55: Frequency of Hospitals Types Participated to the Survey

8.2.2 Survey Analysis

The maturity levels per dimension per hospital are given in Appendix G. The averages of all scores per dimension per hospital together provides the overall score. In Figure 56, an overview of the frequency per half overall maturity level is given.

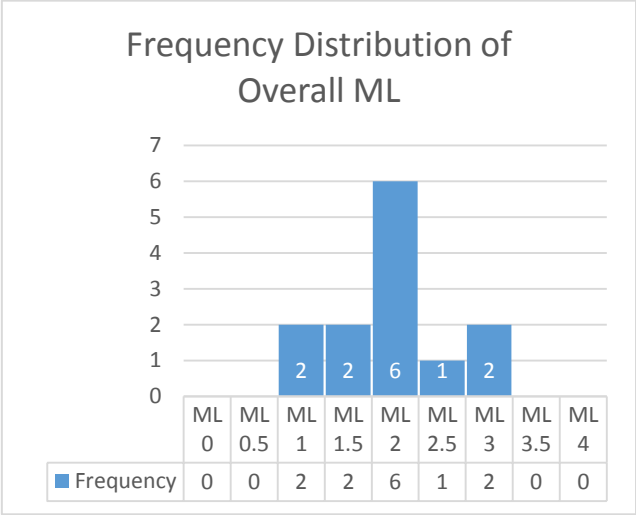


Figure 56: Distribution of Maturity Level of Surveyed Hospitals

There is quite a large spread between the highest and lowest overall rewarded score to hospitals with a difference between the best and worst participated hospital of 1.6 (=2.8 – 1.2).

Considering the individual maturity levels, the average difference between the highest and lowest score on a maturity dimension is 2.8.

Only five hospitals have every maturity dimension at least at level one, which suggests they miss important parts of their CSRA. Often they missed the lowest average scored maturity dimension 5: Tooling (average 0.9). The highest average scored maturity dimension on the other side was maturity dimension 3: Stakeholder involvement (average 3.1). Although some nuance could have been fallen away, as this maturity dimension does not include a level 1 and level 3 maturity level.

In Table 21 an overview of the frequencies of rewarded maturity levels per dimension is given. A color is given based on the frequency on a scale from red to green. Except for maturity dimension 2 (risk assessor authority), 5 (tools) and 11 (risk evaluation), frequencies are centered on maturity level 1, 2 or 3 with lesser density frequencies on adjacent maturity levels and flattening further on. This suggests that the most maturity dimensions have a normal distribution among them.

	MD1	MD2	MD3	MD4	MD5	MD6	MD7	MD8	MD9	MD10	MD11
ML 0	0	2	0	1	4	0	1	0	2	1	2
ML 1	2	2	N.A.	4	3	0	3	3	2	11	4
ML 2	3	1	6	5	5	10	6	3	6	1	1
ML 3	6	6	N.A.	3	1	3	3	6	3	0	6
ML 4	2	2	7	0	0	0	0	1	0	0	0

Table 21: Frequency of Maturity Level Scored per Maturity Dimension

Considering MD6: information gathering from internal sources, the frequency of internal sources used to extract information next to interviews are presented in Figure 57. Most often information is extracted from virus scanners, employee reports, penetration tests and IT audits. More complex systems and processes are used less often by hospitals, as would be expected.

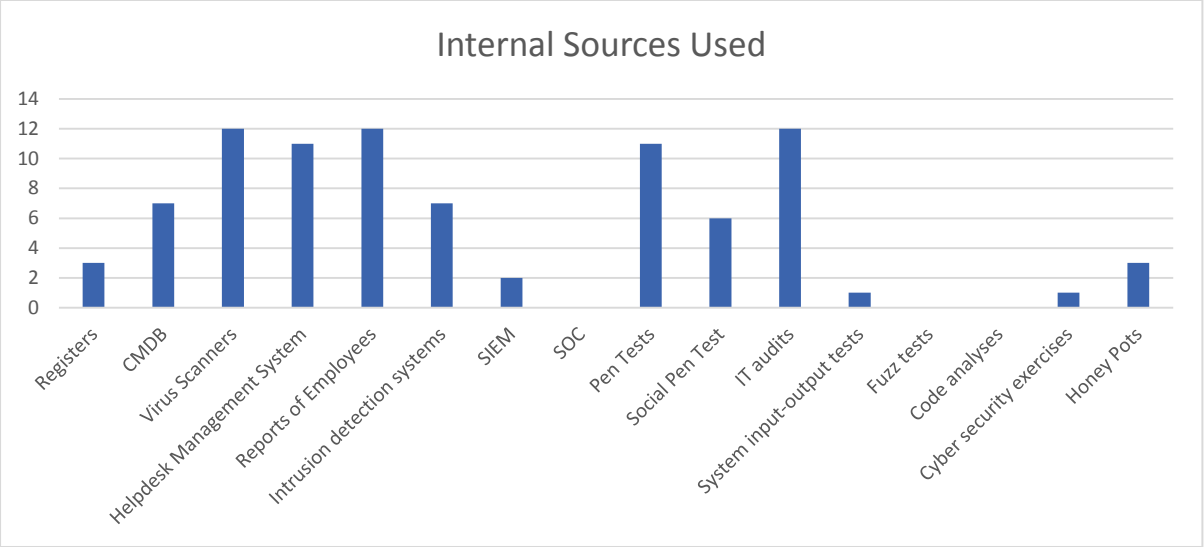


Figure 57: Frequency of Internal Source Types Used

Considering MD7: information gathering from external sources in Figure 58, the frequency of external sources used during CSRAs are presented. More general sources such as security standards and threat landscapes are used the most often and more specific and detailed sources such as fact sheets and specific security standards, e.g. specific for cloud use or web technology). Considering collaboration types (Figure 59), nearly all hospitals (12/13) seem to collaborate in branch relationship, i.e. through NVZ, NFU or SURF connection. 5 out of 13 hospitals have no collaboration other than through branch relationship.

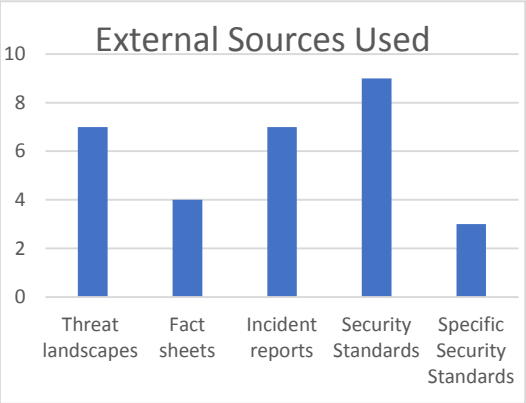


Figure 58: Frequency of External Source Types Used

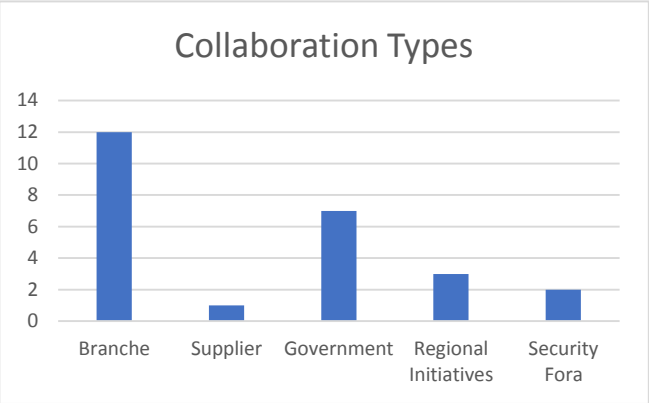


Figure 589: Frequency of Collaboration Types

Considering the results of the survey some assumptions arose which are tested. The first assumption is in regard to a possible relation between the total revenue of the hospital and the maturity of the CSRA. One would expect that hospitals who have a higher revenue, would have more funds available for their cyber security and related activities. With the percential same budget as a small hospital a hospital with a larger revenue could achieve relatively more than would be needed to fit the size of the hospitals needs.

Assumption 1: *There is a correlation between the budget of the hospital and the overall maturity level of cyber security risk assessment of the hospital.*

This assumption was tested by using a Pearson's r correlation between the overall maturity score of the hospitals and the revenue of the hospitals as obtained from their annual financial statements of 2012 as most hospitals did not yet finished 2013 at the time of research. The annual financial statements were retrieved from *jaarverslagenzorg.nl* (CIBG, 2014). The anonymous hospital was excluded from this correlation as no annual financial report could be found. The calculated correlation was very low ($r = -0.084$) and above all not significant ($p = 0.398$) for $\alpha = 0.05$. Therefore it is concluded no correlation was found.

The second assumption is in regard to a possible relation between the possession of valuable assets and the maturity of the CSRA. This is different from assumption 1 as it is possible for a hospital to have a relatively low revenue, but still have valuable assets, who increase the risk profile of the hospital. Between these generally a difference can be made between hospitals with increased research capabilities and higher levels of valuable intellectual property (academic and top clinical hospitals) those without (general hospitals).

Assumption 2: *Hospitals with more research and more valuable intellectual property have a higher overall maturity level of cyber security risk assessment of the hospital.*

This assumption is tested with a t-test in which the overall maturity of academic and top clinical hospitals ($N = 6$, $M = 2.05$, $SD = 0.47$) is compared against general hospitals ($N = 6$, $M = 1.94$, $SD = 0.65$). The anonymous hospital was excluded from this t-test as nothing could be said about the type of hospital it was. The t-test resulted in $t(10) = 0.34$, $p = 0.741$ which is not significant for $\alpha = 0.05$. Therefore it is concluded no difference in maturity between top-clinical and academic versus general hospitals was found.

Finally the third assumption is in regard to the general level scored. In advance it was expected that through the regulations in the Netherlands such as the NEN 7510:2011, all hospitals would have at least maturity level 2, which means they have a structure in place concerning the maturity dimension to ensure a standard maturity of CSRA. As this is clearly not the case we still assume that the majority of hospitals will satisfy this criteria.

Assumption 3: *The cyber security risk assessment maturity of the majority hospitals is at least level 2 or higher.*

Depending on how the maturity levels are rounded variations in the results to this question may occur. However this assumption will be tested following strict measurements, in which the rounding in Appendix G (1 decimal) is leading, causing 8 hospitals to satisfy the criteria and the remaining 5 not to satisfy the criteria. If the survey was filled in at random the both groups would have obtained an expected frequency of 6.5. A Chi-squared test was performed to see whether there were significant differences in both groups and thus the larger group that satisfies the criteria results in $\chi^2(1, N = 13) = 0.69$, $p = 0.41$, which is not significant for $\alpha = 0.05$. Therefore it is concluded that not

8.2.3 Survey Structure and Survey Feedback

Some maturity dimension were build up from different elements and thus consisted of more survey question (one question per element). This was the case for maturity dimension 1, 4, 9 and 10. In these cases it could be that an element A which was for example only placed in maturity level 3 and 4 did occur, while an element B which should occur starting from level one did not occur until element A was implemented. However none of the maturity dimensions had answer patterns that were inconsistent with the structure in the maturity model.

Feedback was asked in two different questions during the survey. The first feedback question asked whether important CSRA aspects were still missing (question 30), this provided feedback on the maturity model. The second feedback question asked whether questions appeared unclear (question 31), this provided feedback on the questionnaire.

Considering the missing important CSRA aspects, the following feedback was given:

1. The awareness and expertise of the employees as an important driver of cyber security and risk assessment.
2. Often risk assessment methods are too close to known risks, causing them to miss unknown risks.
3. Compliance with the law and regulations.

Of these aspect the first was mentioned three times, the others were mentioned once. The first feedback point is added to the HCRAMM. Important for this process is that employees receive the right amount of training to obtain this expertise and awareness thereby better fulfilling the requirement to have personnel with the right skills (Table 18: requirement 29) . When they improve this information extracted from interviews will improve (Table 18: requirement 30), validation of the information and the risks will improve (Table 18: requirement 16) and finally processes such as risk assessment, likelihood assessment and risk evaluation will improve (Table 18: requirement 9, 10, 11). The result is presented in Figure 60.

	0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Awareness and Expertise of Employees	No awareness and skill improving activities are provided for employees	Ad hoc awareness and skill improving activities are provided for employees	Awareness and skill improving activities are structurally provided for employees	Awareness and skill improving activities are structurally provided for employees. Sometimes a form of examining is present	Awareness and skill improving activities are structurally provided for employees. Employees are examined regularly and based on results activities are adjusted

Figure 59: Added Maturity Dimension Awareness and Expertise of Employees

The second feedback, although a valid point in general, is exactly what this research hopes to prevent from happening. Especially when the gathering of information from both internal and external sources is optimized according to HCRAMM, hospitals should be able to detect previously unknown risks. The third feedback point is already included in the identification of consequences and the assessment of consequences. Unable to be compliant to law and regulations and the impact of such are indeed important parts of the risk assessment. This was probably not noticed as the survey questions were one abstraction higher, not going into detail about the different types of impacts.

Considering the unclear questions, the following feedback was given:

1. Question 16: the option ‘we have no risk register’ is missing.
2. Question 18, 19, 20: it is asked whether certain information sources are used, but not for what purpose.
3. Question 23: every hospital is a member of the NVZ or NFU, this alone gives no information.
4. Question 25: the impact of incidents should be formulated as the impact of *possible* incidents.
5. Question 25 and 27: this can be done without the stakeholder as well.

Based on feedback points 1,4 and 5 minor changes are made and updated in the self-assessment tool in Appendix I. Feedback point 2 and 3 are more complicated as they are focused on the content rather than the form. Feedback point 2: the purpose of the information that is gathered, is partly answered by other questions (24/29) and is integrated in the whole maturity model. It is however interesting for further research which sources provide the best of information to identify risks. Finally considering feedback point 3, the question is altered to ask whether they actively participate in branch wide collaboration with the NVZ or NFU considering CSRA. A new version of the HCRAMM is added to Appendix H and a self-assessment tool to test a hospital’s maturity on this maturity model is provided in Appendix I. A summarized framework of the HCRAMM version 2.0 is provided in figure 61.

		0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Scope	Scope and Frequency	*A clear scope of risk assessment is needed. Also it should be clear how often this should be performed, under what kind of circumstances.*				
People	Risk Assessor Authority	*The risk assessor needs a form of authority to perform his job well, his authority should be clear in the organization.*				
	Stakeholder involvement	*Stakeholders from all disciplines should be involved or represented in the risk assessment process.*				
	Awareness and Expertise of Employees	*The risk assessor and other personnel involved in the risk assessment should be provided with the right training activities to ensure they are aware and skilled concerning their tasks in the cyber security risk assessment processes.*				
Techniques	Risk Registration	*Information concerning risk assessments should be stored central and maintained, preferably in a risk register*				
	Tooling	*Tools should be used to aid the risk assessment process. A lot of sophisticated tools could be used improve the quality and efficiency of the process.*				
Information gathering	Information Gathering from Internal Sources	*A structured approach should be followed to obtain data from internal sources.*				
	Information Gathering from External Sources	*A structured approach should be followed to obtain data from external sources.*				
Analyses	Identification of Consequences	*Gathered information should be combined into incident scenarios according to certain principles.*				
	Assessment of Consequences	*The consequences of possible incidents should be assessed.*				
	Assessment of Incident Likelihood	*The likelihood of possible incidents should be assessed.*				
Evaluation	Risk Evaluation	*The risks and their values should be evaluated whether they need to be dealt with and in which order.*				

Figure 60: Overview of HCRAMM v2.0 framework (Final Version)

8.3 Conclusion Survey

Between the hospitals participating a balanced mix between academic, top-clinical and general hospitals was present, although not corresponding exactly to their respective percentage of occurrence in the Netherlands. Relative to the occurrence of hospital types in the Netherlands a relatively high amount of academic and top-clinical hospitals participated.

The maturity dimensions on which the most improvement could be gained is tooling (mean = 0.92). The use of simple tools such as standard questionnaires or risk matrixes could already help improve the CSRA and assist the process. More extensively software based tools could improve the oversight and efficiency at least, more advanced tools would be able to assist in the analysis process as well and help obtaining data from a variety of sources, decreasing the workload on the risk assessor and supporting a more agile process.

The assessment of likelihood (mean = 0.97) also appeared to be a difficult subject, which already was brought up throughout the interviews, because of the high level of abstraction of this maturity dimension. In the surveys hospitals scored low on this subject, not one hospital reached maturity level 3 or higher. Hospitals could vastly improve this process by not just assessing it themselves or letting stakeholders assess it based on opinions, but assist this process by historical data obtained from external and internal sources. A possibility to improve overall is to focus their people, processes and technology more on iterative development of the process. Next to these areas opportunities lay at the registration of risks, the gathering of external information, the assessment of consequences and risk evaluation as well, as these are generally not that developed yet.

Three assumptions were statistical tested. The first two researched whether budget or type of hospital would influence the CSRA maturity at hospitals. Now connection could be found. Furthermore it was tested whether a statistical majority had at least maturity level 2, which would indicate they have a structured CSRA process. At this assumption hypothesis 0 could also not been disregarded. However the small group that could be used to test these assumptions (n=13) may have been of large influence to this.

Finally based on the survey it is concluded that the order used for the individual elements in the HCRAMM build-up did not provided any strange surprises and seemed correct with these results. From the survey feed-back provided by the correspondents it however became clear an extra dimension was needed to complete the HCRAMM. This new dimension, awareness and expertise of employees, is there for added to the final version of the maturity model. Creating a conclusive result, to be used for maturity assessments of the CSRA process within hospitals, including a self-assessment questionnaire.

9 Discussion and Conclusion

9.1 Discussion

The development of the maturity model needed to be constructed from scratch as no attempt to define maturities considering CSRA of information security risk assessment was found. Important aspects considering CSRA could however be identified in the three types of literature research performed (SLR, comparison analysis, maturity model comparison). Differentiation to what elements were more important was done with the expert interviews and resulted in the structure of the HCRAMM. Although heavy reliant on this part, all the expert interviews where with Dutch based organizations. This may have caused a small bias in the model, when one for example would use it in different countries. This said, it seemed during the literature research that the principles used were relative country independent and the aforementioned bias will probably be minimal.

Considering the research method some pros and cons could be named. The validation process at this time leaned strongly on the four validation interviews and the feedback given in the survey. This provided several opportunities for validation, however a higher maturity of validation could have been reached if validation was done in the form of a workshop with experts from both hospitals, government and commercial organizations as discussion would be possible. However problems could occur in this setting as well as from the interviews it seems that experts from hospitals were more focused on the organizational and human side of the problem, the experts however, especially the experts from commercial organizations, seemed more focused on procedural and technical solutions. In the maturity model development it was attempted to include both perspectives.

As hospitals are the target group it is interesting to note that 21 individual hospitals (11 in the interviews and 13 in the survey of which 3 overlap) participated in the research, counting up to 24% of the total hospital population in the Netherlands, providing a strong basis for the research. The small overlap may have caused a small bias as these hospitals are partly scored on what they believed was important. However the average of these hospitals was negligible higher than the average of the other hospitals, letting to believe this bias was minimal.

Finally to test whether the hospitals would find their given maturity scores realistic, the hospitals were provided with their scores and asked whether they found them to be a well representation of the maturity of their CSRA. Several hospitals replied that they found it a well representation and none provided negative feedback on the model. One hospital however was shocked about its relative low score to other hospitals. A possible bias seems to exist when some hospitals fill in the survey more strictly then others. Therefore, when using the self-assessment tool hospitals should first read this thesis to prevent (slightly) wrong interpretation of the elements used in the maturity model.

9.2 Conclusion

SRQ1: What is known about the cyber security risk assessment context of hospitals?

In academic literature relatively little research is done considering information of the cyber security threat landscape. In the academic literature a clear focus lays on three main groups of threat actors: cyber terrorists, cyber criminals and internal actors. In these the first threat actor seems mainly focused on destruction, the second an economical advantage and the latter contains various reasons, but has the advantage of being on the inside of the organization. Attack vectors described in the academic literature, used by the threat actors, are often described from the point of view from those threat actors, which causes a certain limited view on the threat landscape. In threat landscapes developed by governmental and cyber security organizations more nuance and detail is given concerning cyber threats, the related threat actors and their used methods. They however provide an industry wide threat landscape, without a focus on hospitals or health care. By combining both the academic literature and other threat landscapes a theoretical basis was developed, which in turn could be used for the interviews in which information was more specified and checked for relevance for the particular sector, making it domain specific.

From this research it became clear that the threat actors relevant for hospitals were: cyber criminals, social engineers, internal actors, nation states, cyber researchers, script kiddies, VIP spies, frustrated patients and hacktivists. Cyber terrorists were mentioned as well, although there was consensus among the experts that it is not an important actor for hospitals as cyber terrorists were focused more on sectors such as telecom, energy and banking. Also no known incidents have yet occurred with cyber terrorists at Dutch hospitals.

To identify the targets of the threats, the asset groups, were identified. These were abstracted to a level in which the motivations to attack or gain access to these would be similar. Often the way in which they are protected is similar as well in these abstraction levels. Identified asset groups were: patient data, financial data, research data, medical systems and SCADA, operational data, employee data and communication systems. Student data was identified as well, since often hospitals contain medical professionals in training. However all hospitals, including the academic hospitals agreed the main storage and responsibility lay at the educational institutes of the students rather than at the hospitals.

Information of both the assets and the threats (represented by their agents), were mapped against each other in an target matrix, which gives information whether a certain threat is aimed specific at an asset group, at specific parts of an asset group or not specifically at that asset group. This information and tool are useful in the assessment of the likelihood and consequences when combined with the threat actor profile, since it provides an overview on which assets need to be extra protected against which attack vectors. For both (net) likelihood and (net) impact this should be worked out into qualitative or quantitative scores specific for the organization. This is difficult to generalize over the whole hospital sector as factors such as hospital activities, specific assets, location, regional importance, size, image and current level of cyber security highly influences the specific risk level of a hospital. A rough generalization could be made between academic, top clinical and general hospitals, which each have another gradation of research, health care and teaching capabilities. On the asset side especially research data is strongly dependent on the type of hospital.

To conclude, a lot of information concerning the threat landscape for hospitals is known somewhere, but nowhere a full picture of the threat landscape is to be found. Furthermore of the emphasis at hospitals lays on well-known and often occurring incidents. Because of this, more recently upcoming threats, such as state sponsored hackers, are often overlooked or dismissed as not important. The threat landscape constructed in this research provides a more nuanced overview of the threats, vulnerabilities and assets that hospitals have to deal with by combining information from a broad range of sources.

SRQ 2. How can hospitals perform cyber security risk assessment?

A lot of different risk assessment methods exist. In this research alone twenty-five different methods were identified. Five specialized methods within the systematic literature review, twenty general methods within the comparison analysis. The main differences between the risk assessment methods lay in the in the scope of the method, the risk model they used and the support they provided. In the literature several techniques were found to improve risk assessment. A common denominator between those techniques was the quantification of risks, as they all seem to require a more quantified approach than was used before. Although risk quantification requires more complex processes and more information, researchers view this as an important aspect to obtain improvement. A footnote however should be made that from the interviews and the survey results it became clear that the improvement of the quality of the human capital, considering cyber security awareness and skills, may however be the first priority as most hospitals still have a relatively low maturity of cyber security and CSRA. Other common elements in the general risk assessment methods were the definition of the scope and the context in which the risk assessment should take place. The stakeholders are identified and in most cases consulted during the process. Then an information gathering process starts in which information is gathered about assets, threats, vulnerabilities and in most cases controls. This is followed by several analyzes that depending of the risk model used in the method vary.

Considering information security and in its extend cyber security all hospitals should to comply to the standard for information security the ISO 27799 or for Dutch hospitals the Dutch translation in the form of the NEN 7510. The execution of a risk assessment requires certain sub-processes. According to the ISO 27799 the required processes within the scope of this research should at least include the determination of assets, rating the assets, determine dependencies between assets, determine threats, determine vulnerabilities, identify existing and planned controls, rate the risks and decide on the risk. This however still provides a lot of room for the interpretation of the risk assessment.

As the ISO 27799 still leaves a lot of room for interpretation of the risk assessment process and many different methods exist to perform such a risk assessment it is not surprising almost every hospital has its own CSRA method, often included as component of the information security risk assessment. However the majority of the used risk assessment methods is fairly high level and often internally developed or developed by the security officer. Also methods developed by external agencies and the use of the ISO 27005 are relatively high level. Additional the methods often provide little support in structured approaches and tools. Hospitals that used proven methods encountered that the employees seemed to have difficulty adjusting to them. In one case this caused the hospital to stop using such a method (CRAMM), which proved to be too extensive for the organization. The main reason given for the use of high level methods and the difficulty hospitals encountered when using methods proven in other industries concerned the hospital personnel. Most interviewed experts from hospitals indicated that the majority of hospital personnel, especially the employees working in care processes, were not used to or had difficulty adapting to a risk based thinking and the bureaucratic processes needed for this, as again stresses the need to improve the quality of human capital considering this subject.

However the use of an industry wide used method does not have to fail. During the interviews examples were provided that proved some hospitals implemented such methods, with many advantages such as a clear structured approach and assisting tooling. In the beginning a transition had to be made in the hospital culture and employees needed training on how to work according to the method, but in the long whole this results in an increased maturity of the CSRA. During the CSRA method comparison, both CRAMM and MEHARI 2010 seem to meet the most criteria. However as CRAMM seems to be too extensive, MEHARI 2010 might provide the best option. Also local widely used methods, which were out of scope in this comparison, could be a good fit.

To conclude, many CSRA methods exist. Hospitals are free in their choosing of a method as long as it complies with the ISO 27799. As the ISO 27799 only describes the basic needs of risk assessment and a few important components, hospitals still have a large amount of freedom on how to shape this process. They can choose or develop their own method, including a variety of risk models and tools. However it is important to align the CSRA with the health care by taking into account the strengths and weaknesses of the hospital personnel and train them to participate rightly in the risk assessment process.

SRQ 3. How can a maturity model based on previous maturity models be constructed to measure the maturity of the cyber security risk assessment in hospitals?

Considering the development of the maturity model, little information could be obtained from previous maturity models. Current related maturity models al seemed to have a wider scope and higher level of abstraction than was used in this research. A second problem was a general lack of documentation and validation of the maturity models. Only five related maturity models met the requirements for documentation and validation. Of these four maturity models were focused on information security or cyber security in some form. The capability maturity model integration was added as its structure is often used for other maturity models. No maturity model was found that was specifically aimed on CSRA, or information security risk assessment for that matter, defining another clearly specified research gap. The main gain from the compared maturity models was the architectural frameworks they presented. Based on these a matrix structure was chosen with maturity dimensions and maturity levels.

The maturity levels define several stages in which every improving stage improves the level of structure, accuracy and responsive velocity. At its optimal form the risk assessment should have become agile to an extend that when the threat landscape changes, e.g. due to the end of a service level agreement, the introduction of a new virus or a certain increase in attacks on the hospital's cyber assets, the consequences can be assessed fast, in a reliable manner and without extensive use of resources. The need to strive to that state of risk assessment is increasingly needed as hospitals are becoming more and more digitalized, causing hospitals to become more and more dependable on their cyber assets. On the other side cyber attacks are becoming more frequent and complicated as they are more accessible to a larger area, because of trends such as the information sharing of attack vectors and services such as malware-as-a-service, DDoS-as-a-Service and hacking-as-a-service.

To measure the maturity of the CSRA certain categories of elements or maturity dimensions were identified. Based on these maturity dimensions the maturity can be measured. The initial maturity dimensions were gained from the defined elements from the literature sections and expanded by the information gained in the interviews and in lesser extend the feedback of the survey. Important defined maturity dimensions in this research are: scope and frequency, risk assessor authority, stakeholder involvement, awareness and expertise of employees, risk registration, tooling, information gathering from internal sources, information gathering from external sources, identification of consequences, assessment of consequences, assessment of incident likelihood and risk evaluation.

To conclude, previously developed maturity models provided some useful content. Furthermore architectural principles were adopted from them, setting a framework to be filled in with more specific information. This information, obtained from different literature sources, interviews and a survey was analyzed and inserted in the framework. Concluding in the Hospital Cybersecurity Risk Assessment Maturity Model. The survey set out to use the maturity model at the target group in practice showed that it could be well used for its intended purpose.

SRQ 4: How mature is the cyber security risk assessment in Dutch hospitals and how can they improve?

In general most hospitals could increase the their CSRA vastly by choosing a stronger data driven approach, in which they do not only obtain data from stakeholders, but obtain more information from historical data (e.g. recorded incidents), predictions from reliable external sources (e.g. threat landscapes from organizations as the NCSC) and creative exploration of their own architecture (e.g. network monitoring and regular penetration tests).

Furthermore they should invest in means to structure, process and retain the data following from such a stronger data-driven approach. This would allow incremental improvement of the view on the cyber security risks of a hospital. Enabling the hospital to invest more specific in their cyber security measures, while protecting themselves better against threats, possibly obtaining an return on the investments in the risk assessment process multiple times.

Depending on the hospital's risk level the needed maturity level may vary. For a general hospital, without extra complicating factors a maturity level of 2 would probably suffice. At this level they would have the CSRA at a basic, but well-structured level. In this case the hospitals would apply to the concept of risk assessment maturity of the NEN 7510 and the ISO 27799. For hospitals with higher risk levels, especially the academic hospitals, a higher maturity should probably be reached. However further research is needed to be sure. According to these assumptions only 6 of the 13 hospitals are at the right maturity level considering their risk level. Or in other words more than half of the participated hospitals should improve their CSRA. If this is translatable to the whole population of Dutch hospitals should be further examined with a larger test group.

To conclude, the majority of participated Dutch hospitals score an average on their CSRA maturity between maturity level 1.5 and 2.5 with peaks both ways. The most important improvement areas were tooling and likelihood assessment. However large opportunities lay at the registration of risks, the gathering of external information, the assessment of consequences and risk evaluation as well. In general the scope & frequency, the risk assessor authority and the stakeholder involvement was relatively mature at most hospitals.

Main Research Question: How can hospitals improve their maturity of assessing relevant cyber security risks?

In this research an answer has been given what relevant cyber security risks are regarding hospitals and which methods and techniques can be used to assess these. Furthermore element categories considering CSRA are identified. These element categories or maturity dimensions represent the important quality factors, which mapped against maturity levels provides a measurement tool to measure the maturity of CSRA at hospitals. By mapping the status quo of CSRA in the hospital on the maturity model it is possible to identify the maturity of CSRA per dimension and on an overall level. From this stage hospitals can see which measurements need to be implemented to improve their maturity.

The maturity model was tested in the Netherlands among hospitals through a survey. The participating group of hospitals (n=14) suggested large improvements in maturity could be made by increasing the awareness and skills of human capital related to the risk assessment. This was often seen as one of the priorities during the interviews. However another large opportunity was found in the improvement of process structure, which then could enable the use of more tools and quantification as to improve the maturity. Finally a more sophisticated form of iterative improvement could be obtained from the use of centralized information storage and retrieval considering the data needed and processed during the CSRA process. This test group was however too small to provide sufficient statistical proof to generalize this to the whole Dutch hospital population and further research should be done to examine this. However the HCRAMM proofed its use as an useful measurement tool for CSRA maturity measurement.

9.3 Future Research

During this research multiple research questions outside the scope of this research arose. First the threat landscape as it is at this point provides a certain framework on which threats, vulnerabilities, assets and the relation between them are provided. Hospitals themselves still need to quantify this towards their own organization. However for research purposes it might be interesting to research what the main variables are that increase the risk level for hospitals and research the correlation between the risk level and attempted attacks on hospitals.

Secondly, during the research a discussion came up often about the question whether a statistical model based on techniques used in the insurance branch could help hospitals to calculate their risks, and when this would be possible, how it should be developed. The experts disagreed heavily with each other concerning the usefulness of such a model, both in favor of it and against it.

Furthermore sub question 4 tried to answer how mature Dutch hospitals are considering their CSRA maturity. As the test group was too low (n=14) to draw conclusions, a larger test group should be used. From these results certain assumptions regarding the relation between the maturity and type, risk level, and budget could be measured and provide insight whether these factors influence the maturity of CSRA in hospitals.

Some estimations have been give regarding the minimum needed maturity of CSRA. It would be interesting to research what maturity level should at least be reached by the hospitals. Within this question it should then be researched whether a difference should be made between hospitals of different types, at different locations, and other possible risk increasing factors.

Finally during the interviews a presumption came up that the maturity of CSRA might rely heavily on the person responsible for the risk assessment, as, especially in smaller hospitals this is often just one person and his individual skills, motivation and experience could make a difference. But what is the weight of this difference and could the security of a hospital, with consequences for patient safety, millions of revenue and the privacy of many is dependent on the qualities of one man or can there be enough other safety nets be implemented in the organization structure.

Bibliography

ANSSI. (2010). *Expression des Besoins et Identification des Objectifs de Sécurité EBIOS Historique des modifications* (pp. 1 – 95). Paris.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare : current state of research. *Internet and Enterprise Management*, *6*(4), 279–314.

Atay, S., & Masera, M. (2011). Challenges for the security analysis of Next Generation Networks. *Information Security Technical Report*, *16*(1), 3–11.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3)

Beggs, P. (2010). *Securing the Nation ' s Critical Cyber Infrastructure Securing the Nation ' s Critical Cyber Infrastructure*.

Brockett, P. L., Golden, L. L., & Wolman, W. (2011). Enterprise Cyber Risk Management. In *Risk Management for the Future - Theory and Cases* (pp. 319–340).

BSI. (2008). *Health informatics — Information security management in health using ISO / IEC 27002 (ISO 27799:2008)* (Vol. 27002, p. 57). London.

Butkovic, M. J., & Caralli, R. A. (2013). *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale* (pp. 1–38). Pittsburgh.

Canabarro, D. R. (2013). Reflections on The Fog of (Cyber) War, (13), 1–18.

CBP. (2012). *Onderzoek naar toegangsbeveiliging van medische gegevens* (pp. 1–9). Den Haag. Retrieved from http://www.cbpweb.nl/downloads_med/rap_2012_beveiliging-medische-gegevens-rpz-ziekenhuis.pdf

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731.

CLUSIF. (2011). *MEHARI 2010 Processing guide for risk analysis and management* (pp. 1–32). Paris.

Dahl, H., Hogganvik, I., & Stolen, K. (2007). *Structured Semantics for the CORAS Security Risk Modelling Language*. Oslo.

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assess- ment Model. In *16th Australasian Conference on Information Systems (ACIS)*.

Deibert, R. J., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32.

DOE. (2014). *Electricity Subsector Cybersecurity Capability Maturity Model* (pp. 1–89). Washington.

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

ENISA. (2013). *ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats*.

Europol. (2011). *Threat Assessment: Internet Facilitated Organised Crime* (pp. 1–11).

Foltz, C. B. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, *12*(2), 154–166.

Fu, K. (2009). Reducing risks of implantable medical devices. *Communications of the ACM*, *52*(6), 25.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3), 298–303.

Gregory, M. A., & Glance, D. (2013). *Security and the Networked Society*.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., … Maisel, W. H. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *2008 IEEE Symposium on Security and Privacy* (pp. 129–142). Ieee.

Harauz, J., Kaufman, L., & Potter, B. (2009). Data Security in the World of Cloud Computing. *IEEE Security and Privacy*, 61–64. Retrieved from www.computer.org/security

Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: is the U.S. healthcare system safe? *Telemedicine Journal and E-Health*, *19*(1)

Herndon, M. A., Moore, R., Walker, J., & West, L. (2003). *Interpreting Capability Maturity Model Integration for Service Organizations – a Systems Engineering and Integration Services Example* (pp. 1–49). Pittsburgh.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, *22*(2), 175–186.

Informatieveiligheid, H. T. (2012). *Toetsingskader Informatieveiligheid in de Zorg* (Vol. 0, pp. 1–30).

Jamieson, R., Land, L., Smith, S., Stephens, G., & Winchester, D. (2009). Critical Infrastructure Information Security: Impacts of Identity and Related Crimes. In *Pacific Asia Conference on Information Systems*.

Jung, H., & Goldenson, D. R. (2003). *CMM-Based Process Improvement and Schedule Deviation in Software Maintenance* (pp. 1–47). Pittsburgh.

Kellermann, T. (2010). Cyber-Threat Proliferation. *IEEE Security and Privacy Magazine*, 70–73.

Köster, F., Klaas, M., Nguyen, H., Braendle, M., Obermeier, S., Brenner, W., & & Naedele, M. (2009). Information Security Assessments for Embedded Systems Development: An Evaluation of methods. In *8th Annual Security Conference, Las Vegas, United States.*

Krediet, I., Goossen, W., & Hübner, U. (2011). *Rapport IT-ontwikkelingen in de Nederlandse ziekenhuizen 2011*. Retrieved from http://www.windesheim.nl/~/media/Files/Windesheim/Research Publications/20120503_Rapport_IT_ontwikkelingen.pdf

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics*, *10*(1), 86–103.

Legg, P., Moffat, N., Nurse, J. R. C., Happa, J., Agrafiotis, I., Goldsmith, M., & Creese, S. (2013). Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *4*(4), 20–37.

Lemay, E., Unkenholz, W., Parks, D., Muehrcke, C., Keefe, K., & Sanders, W. H. (2010). Adversary-Driven State-Based System Security Evaluation. In *MetriSec2010*.

Levine, E. S. (2011). Improving risk matrices : the advantages of logarithmically scaled axes. *Journal of Risk Research*, *15, 2*(January 2014), 37–41.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. a, … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *PLoS Medicine*, *6*(7).

Luiijf, E. (2012). *Understanding Cyber Threats and Vulnerabilities* (pp. 52–67).

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ*, *7*(9), 889–896.

Nationaal Cyber Security Centrum. (2013). *Cybersecuritybeeld Nederland CSBN-3*. Den Haag. Retrieved from https://www.ncsc.nl/

Nicholson, a., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418–436.

Ongsakorn, P., Turney, K., Thornton, M., Nair, S., Szygenda, S., & Manikas, T. (2010). Cyber threat trees for large system threat cataloging and analysis. *2010 IEEE International Systems Conference*, 610–615.

OWASP. (2013). *OWASP Top 10 - 2013*. Retrieved from www.owasp.org

Pak, C., & Cannady, J. (2009). Asset priority risk assessment using hidden markov models. In *Proceedings of the 10th ACM conference on SIG-information technology education - SIGITE '09* (pp. 65–73). New York, New York, USA: ACM Press.

Pandey, S. K., & Mustafa, K. (2012). A Comparative Study of Risk Assessment Methodologies for Information Systems. *Bulletin of Electrical Engineering and Informatics*, *1*(2), 111–122.

Pau, L.-F. cois. (2009). Business and social evaluation of denial of service attacks in view of scaling economic counter-measures. *MPRA*.

Ponemon Institute. (2012). *Third Annual Benchmark Study on Patient Privacy & Data Security Sponsored by ID Experts*.

Porras, P. (2009). Inside risksReflections on Conficker. *Communications of the ACM*, *52*(10), 23.

Saint-Claire, S. (2011). Overview and Analysis on Cyber Terrorism. *School of Doctoral Studies*, (3), 85–98.

Saitta, P., Larcom, B., & Eddington, M. (2005). *Trike v . 1 Methodology Document [Draft]* (pp. 1–17). Retrieved from http://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf

SANS. (2002). *A Qualitative Risk Analysis and Management Tool* (pp. 1–15).

Savola, R. M., & Abie, H. (2013). Metrics-driven security objective decomposition for an e-health application with adaptive security management. In *Proceedings of the International Workshop on Adaptive Security - ASPI '13* (pp. 1–8). New York, New York, USA: ACM Press.

Seale, C., Gobo, G., Gubrium, J., & Silverman, D. (2004). *Qualitative research practice*. (J. Ritchie & J. Levis, Eds.) (1st ed., pp. 1–349). London: SAGE Publications. Retrieved from http://books.google.com/books?hl=en&lr=&id=aP57yvIjmIAC&oi=fnd&pg=PP1&dq=Qualitative+Research+Practice&ots=9Nkk-jsdfV&sig=LujcJsuZYrsF1JC_DDGucpS77TA

SEI. (1999). *Systems Security Engineering Capability Maturity Model* (pp. 1–336). Pittsburgh.

SEI. (2005). v01_octave-s_intro v1. Carnegie Mellon University.

SEI. (2007). OCTAVE Allegro Method v1. Carnegie Mellon University.

SEI. (2010). *CMMI for Services, version 1.3* (pp. 1–520). Pittsburgh. Retrieved from http://repository.cmu.edu/sei/286/

Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: towards a business practice perspective. In *Australian Information Security Management Conference* (Vol. 8, pp. 119–130). Retrieved from http://ro.ecu.edu.au/ism/98/

Singh, A. K. (2011). New Face of Terror : Cyber Threats , Emails Containing Viruses. *Asian Journal of Technology & Management Research*, *01*(01).

Szpyrka, M., Jasiul, B., Wrona, K., & Dziedzic, F. (2013). Telecommunications Networks Risk Assessment with Bayesian Networks. *Computer Information Systems and Industrial Management.*, 277–288.

The Open Group. (2011). *Open Information Security Management Maturity Model* (pp. 1–105). Berkshire.

Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., & Woodyard, M. (2013). How Bad is it? – A Branching Activity Model to Estimate the Impact of Information Security Breaches. In *12th Workshop on the Economics of Information Security* (pp. 1–47).

Van de Weerd, I., & Brinkkemper, S. (2009). Meta-Modeling for Situational Analysis and Design Methods. *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, 35–54.

Webster, J., & Watson, R. T. (2009). Analyzing the past to prepare for the future: writing a review. *MIS Quarterly*, *26*(2).

WEF. (2012). *Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience*. Geneva. Retrieved from www.weforum.org

White, G. (2011). The community cyber security maturity model. *Technologies for Homeland Security (HST)*, *40*, 173–178. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6107866

Wrona, K., & Hallingstad, G. (2010). Real-time automated risk assessment in protected core networking. *Teleommunication Systems*, *45*, 205–214.

Zambon, E., Etalle, S., Wieringa, R. J., & Hartel, P. (2010). Model-based qualitative risk assessment for availability of IT infrastructures. *Software System Model Journal*, *10*, 553–580.

Appendixes

Appendix A: Concept Matrix SLR

SLR	Source	Asset identification and valuation	Threat identification	Control identification	Vulnerability identification	Impact assessment	Likelihood assessment	Risk evaluation	Validation of findings	Risk model	Quantification of risks	Tools	Use in networked environments	Confidentiality, integrity and accessibility principles	Cyber Attack Historical Development	Threat actor	Threat actor motivation	Threat actor skills	Attack vectors	Vulnerability trends	Awareness	Cyber Assets	Health Care Specific
1	Atay & Masera (2011)					x	x	x															
1	Harauz et al. (2009)														x	x	x	x	x				
1	Köster et al. (2009)	x	x	x	x	x	x		x	x	x	x											
1	Lemay et al. (2010)	x	x	x	x	x	x	x	x	x	x		x										
1	Levine (2011)					x	x	x		x													
1	Pak & Canady (2009)	x	x	x	x																	x	
1	Pandey & Mustafa (2012)	x	x	x	x	x	x	x	x		x	x		x									
1	Pau (2009)	x	x	x	x	x	x	x		x	x		x	x									
1	Sheddan et al. (2010)	x	x	x	x	x		x				x											
1	Szpyrka et al. (2013)	x	x	x	x	x	x	x															
1	Thomas et al. (2013)	x				x	x	x		x	x	x		x			x	x					
1	Wrona & Hallingstad (2010)		x			x	x	x		x	x	x	x	x									
1	Zambon et al. (2010)		x	x	x	x	x	x		x	x	x	x										
2	Beggs (2010)														x	x			x				
2	Brokett et al. (2011)														x	x							
2	Canabarro (2013)																				x		
2	Choo (2011)														x	x			x				
2	ENISA (2013)															x	x	x	x	x			
2	Europol (2011)															x	x	x	x	x			
2	Geers (2010)																				x		
2	Gregory & Glance (2013)																				x		
2	Harries & Yellowlees (2013)															x			x		x	x	x
2	Hua & Bapna (2013)																				x		
2	Jamieson et al. (2009)																				x		

2	Kellerman (2010)																	x				
2	Lawson (2013)																			x		
2	Legg et al. (2013)														x			x				
2	Luiijf (2012)					x	x	x		x												
2	Manikas et al. (2010)		x			x	x				x											x
2	NCSC (2013)													x	x	x	x	x	x			
2	Nicolson et al. (2012																	x	x			
2	OWASP (2013)														x			x	x			
2	Porras (2009)																	x				
2	Saint-Claire (2011)														x	x		x		x		
2	Savola & Abie (2013)	x	x		x	x	x	x		x	x	x	x	x								x
2	Singh et al (2011)													x	x							

Appendix B: Threat and Vulnerability Vectors Identified in the Literature

Type	Sub-type	Specific	Explanation	Source
Botnets	Botnet		A botnet is a networks of compromised, remotely controlled computers, infected with malicious software and controlled as a group without the owners knowledge.	Europol (2011), ENISA (2013), NCSC (2013)
	DDoS Attack	Volume-oriented	A DDoS attack which saturates the bandwidth of the network and infrastructure, e.g. a SYN attack, Smurf attack	Europol (2011), ENISA (2013), NCSC (2013)
		Application layer oriented	A DDoS attack on the application layer, this uses a lower volume and is used to disconnect certain services or saturate certain resources	Europol (2011), ENISA (2013), NCSC (2013)
		DNS server attack	A DDoS attack directed directly at the DNS server, whereby websites become unavailable. Alternatively DNS reflection amplification can be used with the use of poorly configured DNS servers.	Europol (2011), ENISA (2013), NCSC (2013)
Social Engineering	Social network mining		Attackers gain personal information about specific employees, which they use in social engineering methods	Europol (2011)
	Spear Phishing	Watering Hole Attack	The attacker wants to attack a particular group (organization, industry, or region). The attack consists of three phases: 1.Guess (or observe) which websites the group often uses. 2.Infect one or more of these websites with malware. 3.Eventually, some member of the targeted group will get infected.	Europol (2011), ENISA (2013)
		e-mail spoofing	An attacker sends one or a select group of employees an e-mail, which seems to come from a legit source, asking for information which can be used to gain unauthorized access to company systems.	ENISA (2013)
	Pharming	Spoof websites	Collection of passwords through face websites, which are tried on other accounts of employees like e-mail and web portals.	ENISA (2013)
	Spoofing / identity theft		Pretending to be someone else and gain access to parts of the system (e.g. an attacker calls someone and pretends to be the secretary of a highly placed manager, which forgot his password and needs to know it)	Europol (2011), ENISA (2013), NCSC (2013)
	Doxing		Identifying someone's anonymous internet identity and using this to its advantage (e.g. blackmailing someone for statements this person gave on internet forums)	NCSC (2013)
	Drive-by-downloads		1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). 2. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.	ENISA (2013)
	USB distribution		The spreading of USB-sticks, e.g. leaving it on a company's parking lot, in the hope employees will plug them into a device. When the USB is plugged in a malware program will be downloaded and installed on the device.	ENISA (2013)
	Sophisticated C2		Using social media as command and control medium. Users of the social media are attacked though the social media.	Beggs (2010)
Vulnerability Scanning	Sweeper		Software which seeks for bugs in systems.	Beggs (2010), ENISA (2013)
	Network Diagnostics		Software which automatically seeks for vulnerabilities in networks.	Beggs (2010)
	Automated Probes / Scans		Automated systems who search the internet for vulnerable servers.	Beggs (2010)
	Stealth / Advanced Scan		Mechanism to perform reconnaissance on a network while remaining undetected. Uses FIN scans, SYN scans or other techniques to prevent the logging of a scan.	Beggs (2010)
	Staging (server)		A server used to test website's behaviour in order to find abnormal behavior or vulnerabilities.	Beggs (2010)

Exploits	Back Doors	A method of bypassing normal authentication to obtain acces to an system	Beggs (2010)
	Zero-day attack	When vulnerabilities are found these are often published on the internet and usable for hackers against organizations who fail to address and patch vulnerabilities fast enough.	NCSC (2013)
	Buffer overflows	An anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety. Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.	Saint-Claire (2011), OWASP (2013)
	Information leakage	This threat is differentiated from data breaches, as it merely concerns technical or organisational information that might be interesting for threat agents in order to perform reconnaissance and delivery of their attacks; as opposed to data breach which is result of a successful attack targeting customers' data. In the reporting period aggressive adware collecting information has been encountered	ENISA (2013)
Code Injections	Cross-Site Scripting (XSS or session hijacking)	A type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.	ENISA (2013), Beggs (2010)
	Directory Traversal	consists in exploiting insufficient security validation / sanitization of user-supplied input file names, so that characters representing "traverse to parent directory" are passed through to the file APIs. The goal of this attack is to order an application to access a computer file that is not intended to be accessible.	ENISA (2013)
	SQL injection (SQLi)	a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution	ENISA (2013), NCSC (2013)
	Cross-Site Request Forgery (CSRF)	A type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.	ENISA (2013)
Encryption Attacks	Transport Layer Security (TLS) Attacks	An attack on the encryption of the TLS	OWASP (2013)
	Brute Force Attack	Attackers use computer power to crack encryptions or passwords. To enlarge the capacity of this process, often botnets are used.	Europol (2011)
	Secure Socket Layer (SSL) attacks	An attack on the encryption of the SSL	
Cyber Crime as a Service (CCaaS)	CCaaS	A new underground market of cyber criminals offering cyber crime tools and activities for pay.	Europol (2011), ENISA (2013), NCSC (2013)
	DDoS-as-a-Service	A person can hire the use of a botnet for a DDoS attack and pay per hour.	Europol (2011), ENISA (2013), NCSC (2013)
	Malware-as-a-Service	A person can buy malware, the use of malware or hire a programmer to build malware.	Europol (2011), ENISA (2013), NCSC (2013)
	Crowd Funded (Cyber) Crime	The development of crowd funding platforms to raise funds for (cyber) crime actions, e.g. placing a bit coin bounty on a world leader's head.	
Malicious code / malware / crimeware	Rogueware/Ransomware/Scareware	Malicious software that locks your computer or system and asks for a ransom to release this lock. Other slightly different approaches might apply. Often when paid the virus does not disappear.	Europol (2011)

	Trojans	A non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm.	Europol (2011), ENISA (2013), NCSC (2013)
	Worms	A standalone malware computer program that replicates itself in order to spread to other computers.	Europol (2011)
	Virus	A type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.	Europol (2011), ENISA (2013), NCSC (2013)
	Spyware	Malicious software that copies/ steals data from an information system or device.	Europol (2011), ENISA (2013), NCSC (2013)
	Exploit kits	These are ready-to-use software tools offering a large variety of functions, configuration options and automated means to launch attacks. Exploit kits search for vulnerabilities in order to abuse them and launch any applicable attack to take over an asset.	ENISA (2013), NCSC (2013)
	DoS	Once malware is installed this might be used to create a denial of service	NCSC (2013), Beggs (2010)
Medical device hacking	Software radio attack	A way to analyse information coming from and going to implanted devices. Hacking the medical device or feeding it corrupt information is as well possible.	Halperin et al. (2008)
	Radio traffic analysis	Eavesdropping on the traffic send to and from medical devices (often implantable devices). Through this technique it would be possible to detect people with for example pacemakers.	Fu et al. (2009)
	Battery Draining	Sending continues streams of requests to an implantable medical device to drain its battery.	Gupta (2011)
	Outdated operating systems and hardware configurations	The typical lifecycle process used in information technology is not always adhered to in managing medical devices. Often, medical devices are not replaced as timely as information systems are because they continue to “do the job.” For example Windows XP operating system is still active on many MRI scanners.	Grimes (2004)
	Other medical device hacks	Medical devices appear to be vulnerable for hacking. Most of them use wireless communication to update internal software. Hacking and eavesdropping of this wireless communication is possible.	Hanna et al. (2011)
Insider Attack	Thumb sucking	The name given to data theft using a USB mass storage device, such as a USB flash (or thumb) drive to download confidential network information, literally “sucking” the data out of the network and onto the USB drive.	ENISA (2013), Brocket et al. (2011), Nicolson et al. (2012)
	Pod-slurping	This involves using an iPod or MP3 type player to rapidly steal gigabytes of information from an enterprise's computer system.	Brocket et al. (2011)
	Increased techniques for insider attacks	With the weapons more widely available and easier to adopt, the barriers to entry will continue to fall. Even in cases where information loss is not for malicious reasons, organisations remain ill-equipped when it comes to ‘monitoring and detecting unusual or suspicious employee behaviour.	ENISA (2013)
Insider Error	Accidental data breach	A threat that can materialize due to errors and mistakes of personnel, resulting in data loss.	ENISA (2013)
	Lack of identification and authorisation authentication	The identification and authorisation authentication processes are insufficient in place.	NCSC (2013)
	UPnP	Universal Plug and Play (factory) configurations of devices can prove to be unsafe.	NCSC (2013)
	Media loss	The loss of media, e.g. laptops, of employees, who contain sensitive data.	ENISA (2013)

	Supply chain leaks		Organisations rely heavily on complex global supply chains for operations. Awareness of the problem has increased somewhat in recent years, but the supply chain is still viewed as the best attack route for any organisation. This threat will increase in criticality over the coming years as bad actors increasingly target weak points in the supply chain rather than directly attacking the intended target.	NCSC (2013)
Increased Vulnerabilities	Hyper connectivity	BYOD	Bring your own device: employees take their own laptops, smartphones and other devices and use them in the work environment. This makes it more difficult to ensure the incoming data (e.g. malware) and outgoing data (e.g. privacy sensitive data).	ENISA (2013)
		IoT	Internet of Things: the trend in which all kind of devices are connected to the internet or another type of network, e.g. refrigerators and medical devices. Search engines as Shodan can take advantage of these usually badly secured devices.	ENISA (2013)
		Control systems (SCADA)	Just as devices, more and more industrial control systems (e.g. climate control systems) are linked to internet or networks	NCSC (2013), Nicolson et al. (2012)
		Cloud	Data stored in "The Cloud" is not only accessible to all authorised users, but also vulnerable to external attacks.	Europol (2011), ENISA (2013), NCSC (2013)
		Stepping Stone	When an attacker overtakes one system it can be used to explore and attack other connected systems.	ENISA (2013)
		Hotspots	As an increasing number of companies and services provide wireless access nodes and hotspots, users expose their personal data in these environments, while others make use of open access zones and unsecured private connections to mask criminal activities, with the potential that unwitting account subscribers are held liable for criminal offences committed using their connections.	ENISA (2013)
	Big data	Extended data collection	As more sensitive data is collected by organizations, more data can be stolen.	Europol (2011), ENISA (2013), NCSC (2013)

Appendix C: HCRAMM Version 0.99

Maturity Dimension		Level 0	Level 1	Level 2	Level 3	Level 4
CSMS Configuration[24]						
Asset Awareness						
	Asset Identification[3]	None	Asset list is constructed and improved manually.	High level assets and interdependencies are listed in the Configuration Management Database (CMDB)	Detailed level and interdependencies and entry types are listed in the CMDB	Detailed level and interdependencies and entries are listed. CMDB contains all the (important) assets of the hospital
Threat Awareness[5]						
	Brand Monitoring	None	Ad hoc search on brand	Basic online brand monitoring	Online brand & social media policing is in place	Online brand is continuously followed
	External Threat monitoring	None	Firewall		Threat analytics	Honey pots are used to gain insight in external attacks
	Internal threat monitoring[14]	None	Virus scanner	Logging	Intrusion detection systems (IDS)	Network profiling/ DLP
	Incident reporting	None	Helpdesk recordings	Reporting of incidents and vulnerabilities is stimulated	Responsible disclosure (external) and Whistle blowing (internal) policy in place	Security Event Manager (SEM) is in place
Vulnerability awareness[7]						
	Penetration Tests[23]	None	Automated vulnerability scan	Use of hacker/ mystery guest / social engineer with limited time (<5 days) and only technical or social	Use of hacker(s) / mystery guest(s) / social engineer(s) with longer time (5-10 days) and wider scope	Team simulating an advanced persisted threat (for at least 3 weeks)
	System Testing[23]	None		Input-Output testing	Fuzz testing /Code Analysis	Network Traffic Monitoring focused on systems
	Cyber Security Exercises[23]	None	Table-top exercise	Table-top exercise is done with detailed writing of the scenario and response	Red teaming exercise, the response team is aware that it is an exercise, during office hours	Red teaming exercise, the response team is not aware that it is an exercise, the timing is bad (e.g. Saturday 03.00)
	Control Overview[6]	None		An overview of all controls in place is available (including whether they are fully implemented or not)		All planned and implemented controls and patches are identified and the effectiveness is known
	IT Security Audits[23]	None	Only on financial systems and EPD	Internal audits on systems	Regular with other hospitals	Both on technical and policy level
Analysis						
	Asset Valuation[4, 12, 13]	None		CIA principles used to measure intrinsic impacts		Check if interdependent/connected systems have the same impact classifications
	Impact Sophistication[9, 12, 17]	None	Ordinal scale consisting of low, medium, high	Ordinal scale consisting of damage ranges	BIA, including damages on safety, compliance to law and regulation, finance, reputation	Sophisticated BIA, both calculating damages and lost revenue mapped against the needed cost to prevent it amongst other factors such patient safety, reputation and compliance to law and regulation

	Scenario Sophistication[8, 13]	None	Open damage scenarios	Closed damage scenarios	Combination of closed and open damage scenarios	Combination of closed and open damage scenarios including actor profiling
	Likelihood of Occurrence Sophistication[10, 12, 17]	None	Standard categories with threat types	Trend monitoring	Integrated statistical model containing all threat & vulnerability data used within the organization	Integrated statistical model containing all threat & vulnerability data used sector wide
	Risk Leveling[11, 12]	None	Standard impact / likelihood matrix	Advanced matrices		
Structure						
	Interviewing[31]	None	Interviews with stakeholders		Risk workshops with voting	Risk workshops with voting and group discussed motivation of choices
	Tools[15]	None				An elaborative tool is used
	Security Requirements[26]	None	Own solution	Organization wide used solution	ISO 27799 / NEN 7510	Inclusion of extra standards for specific solutions (e.g. cloud, mobile)
	Documentation[15]	None	Documentation is done according to own insights	Standardized stencils are used	a knowledge base containing all materials exist	Previous CSRAs (including all input, analysis and output) are available and used to iteratively improve every new CSRA (together with new input)
People						
	Top Management Support[20]	None	Board is aware of risk assessment	Board is driver behind risk assessment	Assessor has right authority and resources to perform the assessment	Full support from the board, risk assessor reports directly to the board
	Stakeholder[2, 28]	None		Stakeholders accept risks		Stakeholders accept risks, active participation, used to risk thinking
	Quality of Risk Assessor[28, 29]	None				Academically schooled, Post-Doc Educations (CISO?), familiar in the organization, 10+ years experience, Affinity with IT
Collaboration						
	Internal Collaboration[19]	None		Care professionals tell ICT what is needed		Strong cooperation between ICT, medical technology and care professionals
	Supplier Collaboration	None			Threat and vulnerability input	
	Sector wide Collaboration[22, 23]	None	Based on incident	Once in a while attending NFU/NVZ meetings	Regular attending NFU/NVZ security meetings	Regular attending ISAC-Health Care meetings
	World Wide Input and Collaboration[22]	None	Reading an external threat landscape sometimes		Regular reading relevant threat landscapes (e.g. CSBN, ENISA, OWASP)	The use of up to date security communities (e.g. OWASP, NIST) for detailed threats and vulnerabilities

Appendix D: HCRAMM Version 1.0

		0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Scope	Scope and Frequency	No risk assessment is performed with a specific cyber scope	Cyber security risk assessments are performed ad hoc with an unclear scope	A structure is in place that defines when cyber security risk assessments are performed. The focus of the risk assessment is placed on the most important assets	A structure is in place that defines when cyber security risk assessments are performed. The focus of the risk assessment is placed on the most important processes	A structure is in place that defines when cyber security risk assessments are performed. These are done with a process centred scope on both policy and technical level
People	Risk Assessor Authority	The cyber security risk assessor is appointed by a division and reports to a division head	A cyber security risk assessor is appointed by the board and reports to a division head	The cyber security risk assessor is appointed by and reports directly to the board	The cyber security risk assessor is appointed by and reports directly to the board and has the authority to interview the people and obtain the information needed for the RA	The cyber security risk assessor is appointed by and reports directly to the board and has the authority to interview the people and obtain the information needed for the RA and is proactively helped by the organisation for this
	Stakeholder involvement	No stakeholders are involved		Only stakeholders from one or a few disciplines are involved		All stakeholders within the scope, from all disciplines, are actively involved in the CSRA process
Techniques	Risk Registration	No previous information can be obtained in new CSRAs	Information is saved decentralized	Information is stored centralized in the risk register	Information is stored centralized in the risk register. The risk register is actively updated	Information is stored centralized in the risk register. The risk register is continually updated
	Tooling	No tools are used	Ad hoc developed tools are used	Documentation and structure aiding tools are used	Software based tools are used to streamline the information gathering process and aid analysis process	Software based tools are used to provide a real-time input in the information gathering process, analyse this following the used models and show the results in a dashboard
Information gathering	Information Gathering from Internal Sources	No information is gathered from internal sources	Information of assets, threats, vulnerabilities and controls is obtained by ad hoc interviews and complemented with ad hoc reports constructed from threat and vulnerability indicators	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes and registers	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes, registers and systems	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes, registers and systems. Internal information is constantly renewing and improving.
	Information Gathering from External Sources	No information is gathered from external sources	An ad hoc search is done for relevant current threats and vulnerabilities on the internet	Important external threat and vulnerability input sources are identified and consulted	Important external threat and vulnerability input sources are identified and consulted. Partnerships are established and used to improve the information quality.	Important external threat and vulnerability input sources are identified and consulted. Partnerships are established and used to improve the information quality. A process is in place that rates the usefulness and quality of current sources and actively seeks to obtain new relevant sources
Analyses	Identification of Consequences	No identification of consequences is done	Incident scenarios are developed ad hoc based on the gathered information	Incident scenarios are developed based on the gathered information following a predefined structure or method	A structured method is used to integrate gathered information and develop incident scenarios for accessibility, integrity and confidentiality degradations	A structured method is used to integrate gathered information and develop incident scenarios for accessibility, integrity and confidentiality degradations The incident scenarios are constantly improved based on previous made scenarios which are evaluated
	Assessment of Consequences	No assessment of consequences is performed	Analysis is done by stakeholders rating incident scenarios on an ordinal scale	Rating is done by stakeholders on damage ranges. Different impact areas are defined.	Historical data of the own and other organizations is used to aid stakeholders with a quantification of the consequence assessment. Different impact areas are defined.	Historical data of the own and other organizations is used to aid stakeholders with a quantification of the consequence assessment. A specific method is in place to translate this historical data to the current situation of the organization. Different impact areas are defined.
	Assessment of Incident Likelihood	No assessment of incident likelihood is performed	Analysis is done by rating incident scenarios on an ordinal scale	Analysis is done by rating incident scenarios on likelihood ranges assisted by information gained from threat and vulnerability trends	Trend analysis is done based on historical data to quantify the likelihood of incident scenarios and aid the stakeholder quantifying the likelihood.	Trend analysis is done based on historical data to quantify the likelihood of incident scenarios and aid the stakeholder quantifying the likelihood. A specific method is in place to translate this historical data to the current situation of the organization.
Evaluation	Risk Evaluation	No risk evaluation is performed	Risk evaluation is done ad hoc and provides a rough ranking of risks, which is validated by stakeholders.	Risk evaluation is done with a structured approach assisted by risk matrixes and validated by stakeholders	Risk evaluation is done with a structured approach gaining insight in the gap between acceptable risk and current risk. This is validated by stakeholders	Risk evaluation is done with a structured approach gaining insight in the gap between acceptable risk and current risk. This is validated by stakeholders. Based on feedback the risk evaluation approach used is iteratively improved

Appendix E: Interview Protocol

General Data

1. Name interviewee?
2. Hospital?
3. Type of hospital?
4. Size organization?
5. Function Interviewee?
6. Experience?

Assets

7. How does the hospital identify its assets?
8. What kind of cyber assets does a hospital possess that need to be protected?
9. Which aspects of information security are important for those assets?
10. How is data classified within the hospital?
11. How does the view on the importance of assets change towards the future?

Threats and Vulnerabilities

12. How does the hospital identify its cyber threats?
13. Which cyber threats do hospitals face?
14. How does the hospital identify its vulnerabilities of information systems, SCADA/ICS systems and medical equipment?
15. Which vulnerabilities do information systems, SCADA/ICS systems and medical equipment at hospitals have?
16. How does the hospital identify its controls?
17. How are the controls evaluated on effectiveness?

Assessment of Cyber Risks

18. How is the impact of cyber risks assessed?
19. How is the likelihood of cyber risks assessed?
20. How are cyber risks prioritized / evaluated?

General Cyber Risk Assessment Methods

21. Does the hospital use a cyber / information security risks assessment method?
22. How often are cyber risks identified, assessed and evaluated?

Evaluation Method

23. How is the method/ approach you use for the identification of cyber security risks evaluated?
24. How is the method/ approach you use for the assessment of cyber security risks evaluated?
25. How is the method/ approach you use for the evaluation / prioritization of cyber security risks evaluated?

Round Up

26. Are there other important aspects of cyber security risk assessment in your hospital that were missed so far?

Appendix F: Survey

1. What is your first name?

2. What is your surname?

3. What is the name of the hospital you work for?

4. What is your function title?

5. Do you work on a technical or policy level?
   - ☐ Technical level
   - ☐ Policy level
   - ☐ Both

6. How would you describe your function?

7. How is your department or team composed?

8. Which functions are held by your direct colleagues?

9. To who do you report (which functions)?

10. The scope of cyber security risk assessments….
    - ☐ There is no risk assessment with a focus on cyber security.
    - ☐ Is focused on assets.
    - ☐ Is focused on processes.

11. The cyber security risk assessment is performed when…
    - ☐ There is no risk assessment with a cyber security focus.
    - ☐ Ad hoc, when one is ought to be needed.
    - ☐ According to preconfigured set rules this is needed. For example periodical or with an architectural change of certain magnitude.

12. The cyber security risk assessment is conducted on…
    - ☐ Policy level
    - ☐ Technical level

13. The person responsible for the cyber security risk assessment in your hospital…
    - ☐ Is appointed by a department, for example ICT or medical technology.
    - ☐ Is appointed by the board of directors. Possibly as part of function such as information security officer.
    - ☐ Reports directly to the board.
    - ☐ Has the authority to organize the needed interviews and obtain the needed data from employees.
    - ☐ Is proactively provided of the needed data before he formally requests this.

14. Concerning a cyber security risk assessment asset owners, process owners and other stakeholders of assets and processes within the scope are…
    - ☐ Not involved in the cyber security risk assessment process.
    - ☐ Only involved from one or several domains, such as ICT, Medical technology or care professionals.
    - ☐ Are involved from all domains within the scope.

15. The registration of cyber risks is…
    - ☐ Not performed.
    - ☐ Performed decentralized.
    - ☐ Performed centralized in a risk register.

16. The risk register in which the cyber security risks are stored is…
    - ☐ Not updated.
    - ☐ Updated after each risk assessment.
    - ☐ Automatically updated by software when the risk situation changes.

17. Tools used during the cyber security risk assessment are….
    - ☐ No tools are used.
    - ☐ Ad hoc developed or obtained, such as threat lists that are self-developed or found during an internet search.
    - ☐ Tools that support documentation, such as standard reporting stencils.
    - ☐ Tools that offer structure during the risk assessment, such as questionnaires on which the business impact can be rated.
    - ☐ Software based tools that support the information gathering from different divisions.
    - ☐ Software based tools that support risk analysis.
    - ☐ Software based tools that provide real-time information, such as a SIEM.
    - ☐ Software based tools that present information, such as risks, in dashboards.

18. Information considering assets, threats, vulnerabilities and controls is gathered from internal sources through…
    - ☐ No information is gathered from internal sources.
    - ☐ Ad hoc reports from relevant sources for the risk assessment.
    - ☐ A structured, predefined process or method to obtain information for the risk assessment.
    - ☐ An automatic connection with risk assessment tooling, in which real-time data is loaded (e.g. a connection with an IDS or SIEM).

19. Information considering assets, threats, vulnerabilities and controls from the following sources are used **sometimes**…
    - ☐ Registers.
    - ☐ Configuration Management Database.
    - ☐ Virus scanner.
    - ☐ Helpdesk Management System.
    - ☐ Incident and vulnerability reporting of employees.
    - ☐ Intrusion Detection Systems (IDS).
    - ☐ Security Incident and Management System (SIEM).
    - ☐ Security Operating Centers (SOC).
    - ☐ Penetration tests.
    - ☐ Social penetration testing or mystery guests visits.
    - ☐ IT audits.
    - ☐ System input-output testing.
    - ☐ Fuzz testing.
    - ☐ Code analysis.
    - ☐ Cyber security exercises.
    - ☐ Honey pots.
    - ☐ Other sources, these include…

20. Information considering assets, threats, vulnerabilities and controls from the following sources are used **always**…
    - ☐ Registers.
    - ☐ Configuration Management Database.
    - ☐ Virus scanner.
    - ☐ Helpdesk Management System.
    - ☐ Incident and vulnerability reporting of employees.
    - ☐ Intrusion Detection Systems (IDS).
    - ☐ Security Incident and Management System (SIEM).
    - ☐ Security Operating Centers (SOC).
    - ☐ Penetration tests.
    - ☐ Social penetration testing or mystery guests visits.
    - ☐ IT audits.
    - ☐ System input-output testing.
    - ☐ Fuzz testing.
    - ☐ Code analysis.
    - ☐ Cyber security exercises.
    - ☐ Honey pots.

21. Other sources, these include…

22. Considering information gathering about threats and vulnerabilities from external sources...
    - ☐ No information is gathered through external sources.
    - ☐ An ad hoc search on the internet for relevant threats and vulnerabilities is performed.
    - ☐ Important sources are structurally identified and information is obtained from these.
    - ☐ Information is continuously obtained from partnerships.
    - ☐ A process is in place to value important sources.
    - ☐ A process is in place which searches for new information sources.

23. Important external information sources used for risk assessments are…
    - ☐ Threat landscapes (e.g. from NCSC, ENISA, OWASP)
    - ☐ Fact sheets.
    - ☐ Incident reports.
    - ☐ Security standards, such as the NEN 7510 and the ISO 27001/5.
    - ☐ Specific security standards, for example specifically targeted at cloud applications or websites.
    - ☐ Other sources, these include…

24. Partnerships that are formed considering the information gathering of threats and vulnerabilities are…
    - ☐ Partnerships within the branch (e.g. SURF, NFU, NVZ).
    - ☐ Partnerships with suppliers of systems (e.g. financial systems, HR systems and medical devices).
    - ☐ Partnerships with the government (e.g. ISAC-Zorg).
    - ☐ Other partnerships, these include…

25. The impact of possible incidents is identified by…
    - ☐ This is not identified.
    - ☐ Creating ad hoc incident scenarios.
    - ☐ Creating incident scenarios according to a structured approach.
    - ☐ Developing incident impact scenarios for the availability, integrity and confidentiality of assets.
    - ☐ Using previously developed incident, which are evaluated, as basis for new incident scenarios.

26. The impact of incidents is assessed by…
    - ☐ These are not assessed.
    - ☐ Rating them on an ordinal scale.
    - ☐ Rating them on ranges (e.g. euro 0-1000, 1001-10000, etcetera).
    - ☐ Formulated them fully quantified.

27. The assessment of the impact of possible incidents is supported by…
    - ☐ This is not supported, the impact is assessed fully qualitative.
    - ☐ A distinction in impact areas (e.g. safety, costs, reputational damage, etcetera).
    - ☐ Knowledge on impact values obtained by analyzing historical incidents (including those of other organizations).
    - ☐ Knowledge on impact values obtained by analyzing historical incidents (including those of other organizations), which is translated to the own organization according to a method.

28. The likelihood that possible incidents occur is assessed by…
    - ☐ These are not assessed.
    - ☐ Rating them on an ordinal scale.
    - ☐ Rating them on ranges (e.g. daily, monthly, yearly, etcetera).
    - ☐ Formulating them fully quantified.

29. The assessment of the likelihood that possible incidents occur is supported by…
    - ☐ This is not supported, the likelihood is assessed fully qualitative.
    - ☐ Trend analysis on historical data.
    - ☐ Trend analysis on historical data using a specific method to translate the results towards the situation of the organization.

30. The evaluation of risks is…
    - ☐ This is not performed.
    - ☐ Performed ad hoc, providing a rough ranking of risks.
    - ☐ Performed using a structured method assisted by risk matrixes.
    - ☐ Performed using a structured method in which the gap between the accepted risk and current risk is determined and validated by stakeholders.
    - ☐ Done based on the evaluation of previous risk evaluations, iterative improving the risk evaluation.

31. Do you miss important aspects for cyber security risk assessment at hospitals in this survey?
32. Were there unclear question and which where these?
33. Would you like to receive a copy of the research?
34. Would you like to receive a personal version of your score on the maturity model?

Appendix G: Survey Scores

Number	MM1	MM2	MM3	MM4	MM5	MM6	MM7	MM8	MM9	MM10	MM11	Overall
H1	4,0	4,0	4,0	2,0	3,0	2,0	2,7	3,0	2,0	1,3	3,0	2,8
H2	2,3	4,0	4,0	2,0	2,0	3,0	2,7	3,0	2,0	2,3	3,0	2,8
H3	4,0	3,0	4,0	2,0	1,5	3,0	1,0	3,0	2,7	0,7	3,0	2,5
H4	3,0	3,0	4,0	3,0	0,0	3,0	2,7	1,0	2,0	1,3	1,0	2,2
H5	3,0	3,0	4,0	2,0	1,5	2,0	2,0	1,0	1,3	0,7	3,0	2,1
H6	3,3	3,0	4,0	1,0	1,0	2,0	2,0	3,0	1,3	0,7	1,0	2,0
H7	1,5	3,0	2,0	1,0	0,0	2,0	2,0	4,0	2,7	0,7	3,0	2,0
H8	3,0	3,0	4,0	3,0	1,5	2,0	0,0	2,0	2,0	1,3	0,0	2,0
H9	3,0	1,0	2,0	3,0	0,0	2,0	2,0	1,0	2,0	1,3	3,0	1,9
H10	3,0	0,0	2,0	0,0	0,0	2,0	2,0	2,0	3,3	1,3	2,0	1,6
H11	1,5	1,0	2,0	1,0	1,5	2,0	2,0	3,0	2,0	0,7	0,0	1,5
H12	0,8	0,0	2,0	2,0	1,0	2,0	1,0	3,0	0,0	0,7	1,0	1,2
H13	0,8	2,0	2,0	1,0	1,0	2,0	1,0	2,0	0,0	0,0	1,0	1,2
Min	0,8	0,0	2,0	0,0	0,0	2,0	0,0	1,0	0,0	0,0	0,0	1,2
Average	2,4	2,2	3,0	1,8	0,9	2,3	1,7	2,3	1,8	1,0	1,8	1,9
Max	4,0	4,0	4,0	3,0	2,0	3,0	2,7	4,0	3,3	2,3	3,0	2,8
Std.Dev.	1,1	1,3	1,0	1,0	0,7	0,5	0,8	1,0	1,0	0,6	1,2	0,5
Max-Min	3,3	4,0	2,0	3,0	2,0	1,0	2,7	3,0	3,3	2,3	3,0	1,6

Appendix H: HCRAMM Version 2.0

		0: Incomplete	1: Initial	2: Repeatable	3: Defined	4: Optimized
Scope	Scope and Frequency	No risk assessment is performed with a specific cyber scope	Cyber security risk assessments are performed ad hoc with an unclear scope	A structure is in place that defines when cyber security risk assessments are performed. The focus of the risk assessment is placed on the most important assets	A structure is in place that defines when cyber security risk assessments are performed. The focus of the risk assessment is placed on the most important processes	A structure is in place that defines when cyber security risk assessments are performed. These are done with a process centered scope on both strategic and technical level
People	Risk assessor authority	The cyber security risk assessor is appointed by a division and reports to a division head	A cyber security risk assessor is appointed by the board and reports to a division head	The cyber security risk assessor is appointed by and reports directly to the board	The cyber security risk assessor is appointed by and reports directly to the board and has the authority to interview the people and obtain the information needed for the RA	The cyber security risk assessor is appointed by and reports directly to the board and has the authority to interview the people and obtain the information needed for the RA and is proactively helped by the organization for this
	Stakeholder involvement	No stakeholders are involved	Only stakeholders from one or a few disciplines are ad hoc involved	Only stakeholders from one or a few disciplines structurally involved	Stakeholders from several to all disciplines within the scope are structurally involved	All stakeholders within the scope, from al disciplines, are actively involved in the CSRA process
	Awareness and Expertise of Employees	No awareness and skill improving activities are provided for employees	Ad hoc awareness and skill improving activities are provided for employees	Awareness and skill improving activities are structurally provided for employees	Awareness and skill improving activities are structurally provided for employees. Sometimes a form of examining is present	Awareness and skill improving activities are structurally provided for employees. Employees are examined regularly and based on results activities are adjusted
Techniques	Risk Registration	No previous information can be obtained in new CSRAs	Information is saved decentralized	Information is stored centralized in the risk register	Information is stored centralized in the risk register. The risk register is actively updated	Information is stored centralized in the risk register. The risk register is continuously updated
	Tooling	No tools are used	Ad hoc developed tools are used	Documentation and structure aiding tools are used	Software based tools are used to streamline the information gathering process and aid analysis process	Software based tools are used to provide a real-time input in the information gathering process, analyze this following the used models and show the results in a dashboard
Information gathering	Information Gathering from Internal Sources	No information is gathered from internal sources	Information of assets, threats, vulnerabilities and controls is obtained by ad hoc interviews and complemented with ad hoc reports constructed from threat and vulnerability indicators	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes and registers	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes, registers and systems	A structured approach is in place to obtain information about assets, threats, vulnerabilities and controls from interviews or workshops and completed by information gained from internal processes, registers and systems. Internal information is constantly renewing and improving.
	Information Gathering from External Sources	No information is gathered from external sources	An ad hoc search is done for relevant current threats and vulnerabilities on the internet	Important external threat and vulnerability input sources are identified and consulted	Important external threat and vulnerability input sources are identified and consulted. Partnerships are established and used to improve the information quality.	Important external threat and vulnerability input sources are identified and consulted. Partnerships are established and used to improve the information quality. A process is in place that rates the usefulness and quality of current sources and actively seeks to obtain new relevant sources
Analyses	Identification of Consequences	No identification of consequences is done	Incident scenarios are developed ad hoc based on the gathered information	Incident scenarios are developed based on the gathered information following a predefined structure or method	A structured method is used to integrate gathered information and develop incident scenarios for accessibility, integrity and confidentiality degradations	A structured method is used to integrate gathered information and develop incident scenarios for accessibility, integrity and confidentiality degradations The incident scenarios are constantly improved based on previous made scenarios which are evaluated
	Assessment of Consequences	No assessment of consequences is performed	Analysis is done by rating incident scenarios on an ordinal scale	Rating is done on damage ranges. Different impact areas are defined.	Historical data of the own and other organizations is used to aid the quantification of the consequence assessment. Different impact areas are defined.	Historical data of the own and other organizations is used to aid the quantification of the consequence assessment. A specific method is in place to translate this historical data to the current situation of the organization. Different impact areas are defined.
	Assessment of Incident Likelihood	No assessment of incident likelihood is performed	Analysis is done by rating incident scenarios on an ordinal scale	Analysis is done by rating incident scenarios on likelihood ranges assisted by information gained from threat and vulnerability trends	Trend analysis is done based on historical data to quantify the likelihood of incident scenarios and aid the quantification of the likelihood.	Trend analysis is done based on historical data to quantify the likelihood of incident scenarios and aid the quantification the likelihood. A specific method is in place to translate this historical data to the current situation of the organization.
Evaluation	Risk Evaluation	No risk evaluation is performed	Risk evaluation is done ad hoc and provides a rough ranking of risks	Risk evaluation is done with a structured approach assisted by risk matrixes	Risk evaluation is done with a structured approach gaining insight in the gap between acceptable risk and current risk.	Risk evaluation is done with a structured approach gaining insight in the gap between acceptable risk and current risk. Based on feedback the risk evaluation approach used is iteratively improved

Appendix I: Self-assessment Survey

Questions stated below should be scored based on the explanation provided in chapter 8.1.2.

1. The scope of cyber security risk assessments….
    - ☐ There is no risk assessment with a focus on cyber security.
    - ☐ Is focused on assets.
    - ☐ Is focused on processes.

2. The cyber security risk assessment is performed when…
    - ☐ There is no risk assessment with a cyber security focus.
    - ☐ Ad hoc, when one is ought to be needed.
    - ☐ According to preconfigured set rules this is needed. For example periodical or with an architectural change of certain magnitude.

3. The cyber security risk assessment is conducted on…
    - ☐ Policy level
    - ☐ Technical level

4. The person responsible for the cyber security risk assessment in your hospital…
    - ☐ Is appointed by a department, for example ICT or medical technology.
    - ☐ Is appointed by the board of directors. Possibly as part of function such as information security officer.
    - ☐ Reports directly to the board.
    - ☐ Has the authority to organize the needed interviews and obtain the needed data from employees.
    - ☐ Is proactively provided of the needed data before he formally requests this.

5. Concerning a cyber security risk assessment asset owners, process owners and other stakeholders of assets and processes within the scope are…
    - ☐ Not involved in the cyber security risk assessment process.
    - ☐ Only involved from one or several domains, such as ICT, Medical technology or care professionals.
    - ☐ Are involved from all domains within the scope.

6. Cyber security risk awareness and skill improving activities (e.g. e-learning trainings, trainings, seminars, etc.) for the risk assessor and risk assessment related personnel (e.g. important stakeholders) are…
    - ☐ Not provided.
    - ☐ Provided on ad-hoc basis (e.g. when an incident occurs).
    - ☐ Provided structurally (e.g. several times a year).

7. Examining of the awareness and skills of the risk assessor and risk assessment related personnel (e.g. important stakeholders) is…
    - ☐ Not performed.
    - ☐ Performed sometimes.
    - ☐ Performed regularly.
    - ☐ Performed regularly and based on results the awareness and skill improving activities are improved.

8. The registration of cyber risks is…
    - ☐ Not performed.
    - ☐ Performed decentralized.
    - ☐ Performed centralized in a risk register.

9. The risk register in which the cyber security risks are stored is…
    - ☐ We have no risk register.
    - ☐ Not updated.
    - ☐ Updated after each risk assessment.
    - ☐ Automatically updated by software when the risk situation changes.

10. Tools used during the cyber security risk assessment are….
    - ☐ No tools are used.
    - ☐ Ad hoc developed or obtained, such as threat lists that are self-developed or found during an internet search.
    - ☐ Tools that support documentation, such as standard reporting stencils.
    - ☐ Tools that offer structure during the risk assessment, such as questionnaires on which the business impact can be rated.
    - ☐ Software based tools that support the information gathering from different divisions.
    - ☐ Software based tools that support risk analysis.
    - ☐ Software based tools that provide real-time information, such as a SIEM.
    - ☐ Software based tools that present information, such as risks, in dashboards.

11. Information considering assets, threats, vulnerabilities and controls is gathered from internal sources through…
    - ☐ No information is gathered from internal sources.
    - ☐ Ad hoc reports from relevant sources for the risk assessment.
    - ☐ A structured, predefined process or method to obtain information from workshops or interviews.
    - ☐ A structured, predefined process or method to obtain information from internal processes (e.g. IT audits, Pen tests, business continuity, etc.).
    - ☐ A structured, predefined process or method to obtain information from internal registers (e.g. asset register, control register, etc.).
    - ☐ A structured, predefined process or method to obtain information from internal systems (e.g. IDS, SIEM).
    - ☐ An automatic connection with risk assessment tooling, in which real-time data is loaded (e.g. a connection with an IDS or SIEM).

12. Considering information gathering about threats and vulnerabilities from external sources...
    - ☐ No information is gathered through external sources.
    - ☐ An ad hoc search on the internet for relevant threats and vulnerabilities is performed.
    - ☐ Important sources are structurally identified and information is obtained from these.
    - ☐ Information is continuously obtained from partnerships.
    - ☐ A process is in place to value important sources.
    - ☐ A process is in place which searches for new information sources.

13. The impact of possible incidents is identified by…
    - ☐ This is not identified.
    - ☐ Creating ad hoc incident scenarios.
    - ☐ Creating incident scenarios according to a structured approach.
    - ☐ Developing incident impact scenarios for the availability, integrity and confidentiality of assets.
    - ☐ Using previously developed incident, which are evaluated, as basis for new incident scenarios.

14. The impact of possible incidents is assessed by…
    - ☐ These are not assessed.
    - ☐ Rating them on an ordinal scale.
    - ☐ Rating them on ranges (e.g. euro 0-1000, 1001-10000, etcetera).

- ☐ Formulated them fully quantified.

15. The assessment of the impact of possible incidents is supported by…
    - ☐ This is not supported, the impact is assessed fully qualitative.
    - ☐ A distinction in impact areas (e.g. safety, costs, reputational damage, etcetera).
    - ☐ Knowledge on impact values obtained by analyzing historical incidents (including those of other organizations).
    - ☐ Knowledge on impact values obtained by analyzing historical incidents (including those of other organizations), which is translated to the own organization according to a method.

16. The likelihood that possible incidents occur is assessed by…
    - ☐ These are not assessed.
    - ☐ Rating them on an ordinal scale.
    - ☐ Rating them on ranges (e.g. daily, monthly, yearly, etcetera).
    - ☐ Formulating them fully quantified.

17. The assessment of the likelihood that possible incidents occur is supported by…
    - ☐ This is not supported, the likelihood is assessed fully qualitative.
    - ☐ Trend analysis on historical data.
    - ☐ Trend analysis on historical data using a specific method to translate the results towards the situation of the organization.

18. The evaluation of risks is…
    - ☐ This is not performed.
    - ☐ Performed ad hoc, providing a rough ranking of risks.
    - ☐ Performed using a structured method assisted by risk matrixes.
    - ☐ Performed using a structured method in which the gap between the accepted risk and current risk is determined and validated by stakeholders.
    - ☐ Done based on the evaluation of previous risk evaluations, iterative improving the risk evaluation.