SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers

Rob Van Os

Information Security, masters level
2016

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers

*Photo of VISA SOC by Melissa Golden

Master Thesis, Information Security Program

<table>
<thead>
<tr>
<th>Name</th>
<th>Rob van Os</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student ID</td>
<td>robvan-2</td>
</tr>
<tr>
<td>Date</td>
<td>30.09.2016</td>
</tr>
</tbody>
</table>
# Contents

LIST OF ABBREVIATIONS ........................................................................................................... 3

ABSTRACT ........................................................................................................................................ 4

1 INTRODUCTION ................................................................................................................................ 5

1.1 BACKGROUND .................................................................................................................................. 5
1.2 RESEARCH GAP ................................................................................................................................. 6
1.3 PROBLEM STATEMENT ....................................................................................................................... 6
1.4 THESIS OUTLINE .............................................................................................................................. 7

2 METHODOLOGY ............................................................................................................................... 8

2.1 DESIGN SCIENCE RESEARCH ......................................................................................................... 8
2.2 PROPOSED SOLUTION ....................................................................................................................... 12
2.3 LITERATURE REVIEW ....................................................................................................................... 12

3 PHASE I: PROBLEM IDENTIFICATION ............................................................................................. 13

3.1 LITERATURE RESEARCH – PART 1 .................................................................................................. 13
3.2 IDENTIFY PROBLEM ......................................................................................................................... 13
3.3 EXPERT INTERVIEWS ....................................................................................................................... 13
3.4 PRE-EVALUATE RELEVANCE ........................................................................................................... 13

4 PHASE II: SOLUTION DESIGN .......................................................................................................... 15

4.1 LITERATURE RESEARCH – PART 2 .................................................................................................. 15
4.2 SURVEY ........................................................................................................................................... 23
4.3 DESIGN ARTIFACT ........................................................................................................................... 31
4.4 THE DESIGN ARTIFACT: SOC-CMM ................................................................................................ 42

5 PHASE III: EVALUATION .................................................................................................................... 43

5.1 REFINED HYPOTHESES ................................................................................................................... 43
5.2 EXPERT SURVEY ............................................................................................................................ 43
5.3 CASE STUDY / ACTION RESEARCH ................................................................................................ 44
5.4 LABORATORY EXPERIMENT ........................................................................................................... 44

6 PHASE IV: SUMMARISE RESULTS ................................................................................................... 47

7 CONCLUSION ...................................................................................................................................... 48

7.1 REQUIREMENTS EVALUATION ....................................................................................................... 48
7.2 REFINED HYPOTHESES EVALUATION .......................................................................................... 50
7.3 CENTRAL HYPOTHESIS EVALUATION ......................................................................................... 52
7.4 FINAL CONCLUSION ....................................................................................................................... 53

8 DISCUSSION ...................................................................................................................................... 54

8.1 RESEARCH METHODOLOGY .......................................................................................................... 54
8.2 RESEARCH PARTICIPANTS ............................................................................................................... 56
8.3 RESEARCH RESULTS ....................................................................................................................... 57
8.4 FURTHER RESEARCH ....................................................................................................................... 59

9 A FINAL WORD .................................................................................................................................. 61

ANNEX A: LITERATURE STUDY OUTCOME ....................................................................................... 62

ANNEX B: SURVEY INTRODUCTION PAGE ......................................................................................... 64

ANNEX C: LABORATORY EXPERIMENT EVALUATION FORM ............................................................. 65

ANNEX D: LIST OF FIGURES AND TABLES ......................................................................................... 68

ANNEX E: REFERENCES ....................................................................................................................... 69
List of Abbreviations

ACM  Association for Computing Machinery
ADR  Action Design Research
AHP  Analytic Hierarchy Process
AR   Action Research
C2M2  Cybersecurity Capability Maturity Model
CEO  Chief Executive Officer
CERT Computer Emergency Response Team
CMM  Capability Maturity Model
CMMI CMM Integration
CMMI-SVC CMMI for Services
COBIT Control Objectives for Information and related Technology
CSBN Cyber Security Assessment Netherlands (Cyber Security Beeld Nederland)
CSIRT Computer Security Incident Response Team
CSOC Cyber Security Operations Center
DR   Design Research
DSDM Dynamic System Development Methodology
DSR  Design Science Research
FAA-iCMM Federal Aviation Administration integrated CMM
FTE  Full Time Equivalent
HPE  Hewlett Packard Enterprise
HPE SOMM HPE Security Operations Maturity Model
ICS-SCADA Industrial Control System Supervisory Control And Data Acquisition
IDPS Intrusion Detection and Prevention Systems
IEEE Institute of Electrical and Electronics Engineers
ISAC Information Sharing and Analysis Center
ISMS Information Security Management System
IT   Information Technology
ITIL Information Technology Infrastructure Library
LR   Literature Review
MoSCoW Must have, Should have, Could have, Won’t have
NIST National Institute of Standards and Technology
NIST CSF National Institute of Standards and Technology Cyber Security Framework
NSA National Security Agency
O-ISM3 Open Information Security Management Maturity Model
SIEM Security Information and Event Management
SLR Systematic Literature Review
SOC  Security Operations Center
SOC-CMM Security Operations Center Capability Maturity Model
SSE-CMM Systems Security Engineering CMM
SQuaRE Security Quality Requirements Engineering
Abstract
This thesis addresses the research gap that exists in the area of capability maturity measurement for Security Operations Centers (SOCs). This gap is due to the fact that there is very little formal research done in this area. To address this gap in a scientific manner, a multitude of research methods is used.

Primarily, a design research approach is adopted that combines guiding principles for the design of maturity models with basic design science theory and a step by step approach for executing a design science research project. This design research approach is extended with interviewing techniques, a survey and multiple rounds of evaluation.

The result of any design process is an artefact. In this case, the artefact is a self-assessment tool that can be used to establish the capability maturity level of the SOC. This tool was named the SOC-CMM (Security Operations Center Capability Maturity Model). In this tool, maturity is measured across 5 domains: business, people, process, technology and services. Capability is measured across 2 domains: technology and services. The tool provides visual output of results using web diagrams and bar charts. Additionally, an alignment with the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) was also implemented by mapping services and technologies to NIST CSF phases.

The tool was tested in several rounds of evaluation. The first round of evaluation was aimed at determining whether or not the setup of the tool would be viable to resolve the research problem. The second round of evaluation was a so-called laboratory experiment performed with several participants in the research. The goal of this second round was to determine whether or not the created artefact sufficiently addressed the research question. In this experiment it was determined that the artefact was indeed appropriate and mostly accurate, but that some optimisations were required. These optimisations were implemented and subsequently tested in a third evaluation round. The artefact was then finalised.

Lastly, the SOC-CMM self-assessment tool was compared to the initial requirements and research guidelines set in this research. It was found that the SOC-CMM tool meets the quality requirements set in this research and also meets the requirements regarding design research. Thus, it can be stated that a solution was created that accurately addresses the research gap identified in this thesis.

The SOC-CMM tool is available from http://www.soc-cmm.com/
1 Introduction

Cyber criminals are continuously searching for new ways to infiltrate businesses through their Information Technology (IT) systems or simply disturbing the business by exhausting their IT resources. More recent examples include the theft of large sums of money from several institutions through Chief Executive Officer (CEO) fraud (also known by the name of ‘Business Email Compromise’) [1, 2], the hacking of the national Security Agency (NSA) [3], cyber attacks on banks [4], attacks on the Ukrainian power grid [5, 6] and the theft of information on 500 million Yahoo accounts [7].

The professionalism of the ‘adversaries’ requires a professional approach from companies defending against such threats as well. Part of the defence strategy is the aggregation of several dedicated operational security functions into a single security department. This way, an overview is created that allows the department to gain insight into the current state of security for the organisation. In turn, this allows this department to identify threats, weaknesses and current attacks and provides a means for appropriate response. This security department is known as the Security Operations Center (SOC). Note that the United States English spelling is used here, as this is the spelling that is commonly used in the industry.

This thesis examines a specific topic for governance in SOCs: capability maturity measurement. Capability maturity measurements are used in many areas, both within and outside the IT domain, for determining how processes or elements in an organisation are performing. This outcome can then be used to determine weaknesses and strengths of those elements and thereby determine areas that require improvement. By regularly assessing maturity and capabilities, and using the output to provide direction to the governance process, it becomes possible to achieve the goals set by the SOC in a demonstrable way.

1.1 Background

As indicated, a SOC is an organisational entity in which operational security elements, such as security incident response, security monitoring, security analysis, security reporting and vulnerability management, are centralised. These operational processes and tasks are often aggregated into the SOC as the organisation grows in size. This way, security-related operational processes are carried out by the same personnel and under the same accountable organisational entity. This has advantages in organisational and operational sense, but also makes sense from a knowledge management perspective as security expertise can be aggregated and optimised. Additionally, the SOC allows for a more coordinated effort in incident detection and response that reduces security risks [8].

Determining how the SOC performs within the enterprise is important in understanding the security risks that the organisation is faced with. A well performing SOC is able to detect and react to security threats, thus reducing the impact of potential security incidents. To determine the performance of the SOC, regular measurements are required. These measurements should focus on determining the weak and strong elements in the SOC. Such measurements help to create a roadmap to more mature and capable security operations. The information can be used to provide focus where required and keep on track with information security maturity goals. Additionally, the information can be used to
proof to senior management that the SOC is performing as expected, or potentially that it requires additional funding or other (such as human) resources [9].

1.2 Research gap

Maturity measurements are a widely used tool for evaluating strengths and weaknesses. Because different kinds of security-related activities are aggregated into the SOC, determining the maturity level of the SOC as a whole requires determining the maturity level of each of those elements. Currently, there are no well-established capability maturity level assessments available SOCs. This is mainly because there is no standard of which common elements are present in a SOC. In other words, there is no such thing as a ‘standard SOC’ or ‘Standard SOC model’. A generic capability maturity model, such as Capability Maturity Model Integration (CMMI) could be applied, but yields generic results as the context is not specific for the element under investigation. Creating a specific context requires an interpretation of the generic maturity model for that specific element.

Some research has been done in the field of SOC models, but these do not provide sufficient detail or a specific focus on capability maturity. For example, Jacobs et al. [10] have researched a SOC classification model, which is based on maturity, capability and aspects. Aspects, in this paper are SOC functionalities or services. In their paper, Jacobs et al. explicitly state that insufficient literature is available on this particular subject. Kowtha et al. [11] have researched a Cyber SOC (CSOC) characterisation model which is based on 5 dimensions: scope, activities, organisational dynamics, facilities, process management and external interactions. Although maturity is mentioned in their work, this is not the focus of the research. Therefore, there is not sufficient information regarding maturity in their work. Their research is based on interviews with many SOC managers to determine similarities between SOCs. A more detailed outcome of their research can be found in their paper “An Analytical Model For Characterizing Operations Centers” [12]. Lastly, Schinagl et al. [13] have researched a framework for SOCs by performing a case study with several SOCs. This was required because, as they state: “each SOC is as unique as the organization it belongs to”. They describe some common SOC functions and elements that a grouped into 4 areas: intelligence, secure service development, business damage control and continuous monitoring. The paper also presents a model in which the SOC can be scored on using a rating level for each element identified. However, this scoring is not elaborated in detail and is not an indication of maturity, but rather of satisfaction, which is more prone to interpretation. As a last note, it must be stated that the previously mentioned research efforts are mostly based on case study research and some best-practices and whitepapers released by commercial companies. These are important indicators that research in this area is currently insufficient.

Note that this research focuses on capability maturity to evaluate the SOC. Other characteristics, such as operational performance (efficiency and effectiveness), are not within scope of this research.

1.3 Problem statement

In order to address the previously stated research gap regarding the availability of SOC capability maturity models, research is required. The proposed research as outlined in this document aims to address the following research question:

"How can the performance and improvement of a Security Operations Center be measured?"
The next chapter outlines the methodology for addressing this research question. The research question is answered in chapter 7.

1.4 Thesis outline

This thesis consists of 9 chapters:

1. Introduction. The current chapter, which describes the background and problem statement for this research.
2. Methodology. In this chapter, the methodology for the research into SOC capability maturity measurement is explained. Additionally, the artefact that is the result of the research as described in thesis is identified.
3. Phase I: Problem identification. This chapter describes the first phase of the research, in which the main problem is identified and made concrete.
4. Phase II: Solution design. This chapter describes the second phase of the research, in which the solution is created.
5. Phase III: Evaluation. This chapter describes the third phase of the research, in which the solution is evaluated and improved.
6. Phase IV: Summarise Result. This chapter describes the final phase of the research, in which the results are summarised.
7. Conclusion. In this chapter, the results from the previous phases are evaluated and conclusions about the research are presented.
8. Discussion. In this final chapter, the research is discussed. Possibilities for further research are identified as well.
9. Final word

Additionally, there are 6 annexes added to this thesis.
2  Methodology

The methodology used in this research is a proactive research methodology: The Design Science Research (DSR) or simply Design Research (DR). This type of research is appropriate for research areas that are not clearly defined as is the case for SOCs: there is no formal definition of what elements are part of the SOC and no complete model of when these characteristics can be considered ‘mature’. Because of the lack of research in this field, the creation of a solution to the problem described in the previous chapter must be carried out in a more proactive manner. DR provides a scientific research approach for this pragmatic and more creative process aimed at innovation and building a bridge between theory and practice [14, 15, 16]. This is also the main goal of this research: to create a solution that can be immediately applied by companies everywhere to determine the capability maturity of their SOC, outline the steps for improvement and measure the progress. The result should thus be first and foremost a practical one.

2.1  Design Science Research

The methodology used in this thesis is based on 3 perspectives on design research:

1. The work by Walls et al. [14], who outlined several basic concepts for design research: meta-requirements, meta-design, kernel theories and testable design product hypotheses.
2. The work by Becker et al. [17], who have outlined 8 requirements for the design of maturity models. These requirements are based on the 7 guidelines for design research by Hevner et al. [18]. Hevner et al. describe a conceptual framework that combines behavioural science (through development and justification of theories) and design science (through building and evaluation). This means that the end result is both useable and based upon formal research, thus matching the research goal stated in the previous paragraph.
3. The work by Offermann et al. [19], who outline a step by step methodology for doing design research.

These 3 perspectives are described below.

2.1.1 Basic concepts of DSR

According to Walls et al., design science should have a strong theoretic foundation. Maturity models generally lack such a theoretic foundation [20]. The foundation for design research, according to walls et al. lies in 4 aspects:

1. Meta-requirements. These are the foundation requirements that guide the design process. In this case, the design product should be: effective in determining the maturity level and strengths and weaknesses, accurate in determining the right maturity level and easy to use in order to support the possibility of self-assessment.
2. Meta-design. This is the class of artefacts that need to be created in order to fulfil the design goals set in the meta-requirements. In this case, the main class of the artefacts is “maturity models”. Additionally, given the fact that self-assessment is required, the maturity model is also an instantiation of a “self-assessment tool”.
3. Kernel theories. Kernel theories are a central part of the theoretic foundation in design research. This is emphasised in other research [21, 22] as well, although different views exist [23]. In this particular case, the kernel theory revolves around 2 basic concepts:
   - A maturity (self-)assessment can be used to determine the next steps for progression and improvement [24, 17]. This is also confirmed by the practical application and widespread adoption of maturity models throughout organisations [25].
- Decision making around a complex subject like maturity can be done by breaking it down into criteria and sub-criteria and evaluating those. The theoretic basis for this is in analytic hierarchy process (AHP) [26, 27] and relative decision making [28]. This is similar to the work done by Van Looy et al. [29].

4. Testable design product hypotheses. The last central element in the design research perspective by Walls et al. is testable design product hypotheses. These are used to determine whether the meta-design (artefacts) is appropriate to fulfil the goals set in the meta-requirements. These hypotheses overlap with the research steps as outlined by Offermann et al. and are discussed in paragraphs 3.4 and 5.1.

2.1.2 Step-by-step methodology of DSR
The step-by-step methodology as presented in the work by Offermann et al. is applied to this research. Chapters 3 through 6 are outlined in accordance with the phases and steps as described in their research. The methodology consists of 11 steps, executed in 3 research phases. These phases are:
- Problem identification
- Solution Design
- Evaluation

The research phases and steps are depicted in Figure 1 (source: Offermann et al., “Outline of a Design Science Research Process” [19]).
The figure shows the 3 main phases of the research and the way in which each of the steps are interconnected. The arrows represent advancement possibility through the research steps. The dotted lines represent the possibility of having to re-design the artefact or even restate the problem based on results of the case study / action research. Each of the phases will be briefly discussed below.

**Phase I: Problem identification**

The first phase of the methodology aims at clearly defining the problem statement and making the goals of the research concrete. This phase includes an initial literature review (LR), combined with expert interviews and relevance determination in order to create a relevant and well-founded problem statement.

**Phase II: Solution design**

The second phase of the methodology focuses on the creation of a design artefact. A second round of literature review is required to create an artefact that has sufficient scientific foundation. In this research, the solution design phase was carried out using a literature review on 3 different topics:

1. SOCs as a whole
2. Elements of SOCs
3. Capability Maturity Models (CMMs) and their applicability to the elements uncovered in topic 1 and further specified in topic 2

An additional step was introduced into the research methodology to determine the correctness of the information found in literature review. This additional step consists of performing a survey. The reason for adding this step to the research methodology is the lack of formal research on SOCs. There are many publications on SOCs, but most of these are whitepapers and best-practices. Since these are not scientific publications, there is insufficient formal input for a well-founded scientific artefact. Thus, the additional step of performing a survey to test the requirements was introduced. Therefore, the solution design phase for this research looks somewhat different from the standard methodology, as depicted in Figure 2.

![Figure 2: Modified Solution Design phase](image-url)
The figure shows that an additional verification step (survey of SOCs) is added between the LR on SOCs and the creation of the design artefact. In the survey, all elements and their details found in the literature review are tested for application in actual SOCs. This allows for differentiation between theoretical SOC elements and practical (actual) SOC elements. The LR on CMMs was used directly as input into the ‘Design Artefact’ step as this literature had sufficient scientific foundation. The output from the survey, together with the LR is used to create the design artefact (tool).

**Phase III: Evaluation**

In the evaluation phase, the Design Artefact is evaluated and refined. For evaluation, different approaches can be applied. Hevner et al. describe 5 different evaluation methods that can be used in this phase (see Figure 3). From these methods, the case study (observational method) and controlled experiment (experimental method) are aligned with the evaluation phase as described by Offermann et al. The case study method allows for an in depth application of the artefact to a business environment. The controlled experiment method allows for the use of the artefact (tool) by several organisations for testing purposes in a controlled experiment. The goal is to uncover any potential defects, validate the functional appropriateness and accuracy of the tool and improve the tool from the feedback obtained from the participants of the test. By testing in multiple iterations, the tool is created and tested in a controlled fashion.

<table>
<thead>
<tr>
<th>Table 2. Design Evaluation Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Observational</strong></td>
</tr>
<tr>
<td>Case Study: Study artefact in depth in business environment</td>
</tr>
<tr>
<td>Field Study: Monitor use of artefact in multiple projects</td>
</tr>
<tr>
<td><strong>2. Analytical</strong></td>
</tr>
<tr>
<td>Static Analysis: Examine structure of artefact for static qualities (e.g., complexity)</td>
</tr>
<tr>
<td>Architecture Analysis: Study fit of artefact into technical IS architecture</td>
</tr>
<tr>
<td>Optimization: Demonstrate inherent optimal properties of artefact or provide optimality bounds on artefact behavior</td>
</tr>
<tr>
<td>Dynamic Analysis: Study artefact in use for dynamic qualities (e.g., performance)</td>
</tr>
<tr>
<td><strong>3. Experimental</strong></td>
</tr>
<tr>
<td>Controlled Experiment: Study artefact in controlled environment for qualities (e.g., usability)</td>
</tr>
<tr>
<td>Simulation – Execute artefact with artificial data</td>
</tr>
<tr>
<td><strong>4. Testing</strong></td>
</tr>
<tr>
<td>Functional (Black Box) Testing: Execute artefact interfaces to discover failures and identify defects</td>
</tr>
<tr>
<td>Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artefact implementation</td>
</tr>
<tr>
<td><strong>5. Descriptive</strong></td>
</tr>
<tr>
<td>Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artefact’s utility</td>
</tr>
<tr>
<td>Scenarios: Construct detailed scenarios around the artefact to demonstrate its utility</td>
</tr>
</tbody>
</table>

*Figure 3: Design Evaluation Methods from Hevner et al.*

In figure 3, the 5 different high-level testing methodologies and the 12 different detailed methodologies for evaluation of the artefact are shown. This research uses case study and controlled experiment methods.
Phase IV: Summarise results

The final phase of the research is to summarise and publish the results. A summary of the results is provided in the conclusion chapter. The publication is this thesis.

2.1.3 Design of maturity models

In their research, Becker et al. indicate that the work by Hevner is an excellent basis for design research in general. However, they also conclude that these are generic practices that can be adapted specifically to the design of maturity models for a more focused approach. These claims are based on the work done by Zelewski [30]. These adaptations are represented in the form of requirements (R1 through R8). The following concrete mapping between the 8 requirements for design of maturity models by Becker et al. and the 7 guidelines defined by Hevner can be made:

- R1: Comparison with existing maturity models (interpretation of Hevner guidelines 1 and 4)
- R2: Iterative Procedure (interpretation of Hevner guideline 6)
- R3: Evaluation (interpretation of Hevner guideline 3)
- R4: Multi-methodological procedure (interpretation of Hevner guideline 5)
- R5: Identification of Problem Relevance (interpretation of Hevner guideline 2)
- R6: Problem definition (interpretation of Hevner guideline 2)
- R7: Targeted Presentation of Results (interpretation of Hevner guideline 7)
- R8: Scientific Documentation (interpretation of Hevner guideline 7)

By applying the requirements set by Becker et al. to this research, the guidelines as set out by Hevner et al. are applied indirectly as well. The application of the guidelines discussed in chapter 8.

2.2 Proposed solution

A central part of the practical and proactive design research approach is the creation of an IT artefact (U.S. English spelling). This is the first guideline set by Hevner et al. and is also a central part of design research according to Walls et al. (meta-design). The IT artefact should come in some “socially recognizable form such as hardware and/or software” [31]. The artefact is created from the data gathered in the research and is a more or less tangible and central result of the research. Artefacts can be constructs, models, methods or instantiations [32]. In this particular case a tool is created that can be used to measure capability maturity in SOCs. This tool is based on a capability maturity assessment model. The tool itself is an instantiation type of artefact: a software solution that brings the model into practice directly. The underlying assessment model can be viewed as an intermediate artefact that is used as a basis for the tool.

2.3 Literature review

A note on literature review in this thesis: normally, the literature review is a separate chapter in the thesis. In this case, however, the research steps as presented in the methodology by Offermann et al. are followed chronologically. These research steps include a 2-part literature review: one part to identify the research gap (problem identification phase) and one part to create the artefact (solution design phase). Thus, the literature review in this thesis is distributed and can be found respectively in paragraph 3.1 (with references to chapter 1) and paragraph 4.1.

The next chapters outline the phases of the research project, starting with the first phase: problem identification.
3 Phase I: Problem identification

The first phase of the research method as outlined by Offermann et al. is the problem identification phase. For this phase, 4 steps have been described and need to be executed. Part of this phase is already described in the previous chapters, thus the steps here are described briefly.

3.1 Literature research – part 1

The literature research for this part of the research was mainly aimed at identification of the research gap. The lack of available scientific literature regarding SOC models and SOC capability maturity and the resulting research gap are discussed in paragraph 1.2.

3.2 Identify problem

Paragraph 1.3 outlines the problem that is studied in this research. To summarise: currently, there is insufficient research regarding SOC models and capability maturity levels specifically for SOCs. There are some proprietary models, but these are not open for use by the public. Additionally, these models are not meant for self-assessment, but for consultancy purposes instead.

3.3 Expert interviews

For this design research approach, research participants were required because of the fact that there is insufficient literature available as a basis for the artefact. These participants were contacted through Information Sharing and Analysis Centers (ISACs) in the Netherlands. The research plan was presented at two different occasions before a number of information security representative (mostly (Chief) Information Security Officers) and SOC managers. During these occasions, maturity for SOCs was discussed and feedback was provided on the research. This information was used to further refine the problem statement. Note that these discussions are not formal one-on-one interviews, but rather a form of interactive workshops in which the problem and the proposed solution were discusses using a presentation on the subject. These workshops serve the same purpose as interviews: to gain insights from experts into the problem statement.

3.4 Pre-evaluate relevance

In this step of the research process, a hypothesis is created that supports the identified problem. This hypothesis is central to the remainder of the research steps and should match the research question posed in chapter 2.3. To support the design research methodology, a solution-oriented hypothesis was chosen. The central hypothesis used in this research is:

“The creation of a self-assessment tool for SOCs can help gain insight in- and control over their capability maturity level”

This hypothesis was also posed in the presentations for the potential participating organisations. During these presentations, it was established that a self-assessment tool for determining the capability maturity level is a viable solution to the research problem.

It was evident that several SOCs were interested to participate in the research and in the outcome of the research. The number of organisations willing to participate in this research is a clear indicator of the relevance of this research. Additionally, the existence of commercial proprietary maturity capability models also indicates that such a model is of value to organisations and can, in fact, be
used to establish capability maturity levels. Hewlett Packard Enterprise (HPE) Security Services alone has assessed 114 SOCs in 154 assessments since 2008 [33]. It must be noted that these commercial models are assessments by experts rather than self-assessments.

With the problem identification stage completed, the next phase of the research can be executed. The next chapter outlines the second phase of the research: the design of the solution artefact.
4 Phase II: Solution design

In paragraph 3.2, the proposed solution is outlined: a tool must be created that can be used to assess the capability maturity level of a SOC. To create this tool, two research steps must be conducted in the second phase of this research:

1. Literature research – Part II
2. Survey of SOCs
3. Design artefact

This paragraph further explains these steps and their outcome in detail.

4.1 Literature research – part 2

The literature study done in this thesis is based on the Systematic Literature Review (SLR) methodology as described by Kitchenham and Charters [34] and further refined by Budgen and Brereton [35]. These methodologies prescribe 6 steps to take in the systematic review. Each of these steps is explained below for each of the 2 parts of the literature review: literature review on SOCs and literature reviews on capability maturity models.

4.1.1 Literature on SOCs

An SLR was carried out to determine the available information on SOCs. The 6 steps by Kitchenham and Charters were used:

1. Define research questions. For the creation of a model, sufficient information on characteristics is required. These characteristics can be divided into logical groups, hereafter called ‘domains’. The domains used in this research are based on the Information Technology Infrastructure Library (ITIL) standard [36], that gives us the domains people, process and technology. However, these 3 domains do not cover all possible characteristics. Therefore, an additional domain is required. Both the HPE and IBM commercial SOC assessment methodologies use the above mentioned 3 domains, but add an additional domain as well. HPE adds ‘Business’ as a 4th domain, IBM adds ‘Governance/Metrics’ as a 4th domain. For this research, an additional domain named ‘Business & organisation’ was added to include aspects that were outside of the scope of the 3 basic domains. Using these domains, the following research questions were created:
   - What are common models for SOCs?
   - What are common processes for SOCs?
   - What are common services for SOCs?
   - What are common roles in SOCs?
   - What are common technologies in SOCs?

2. Define a search strategy. The search strategy in this particular case was straightforward. Since the number of scientific publications on SOCs is very limited, the search strategy should be aimed at non-scientific publications, such as whitepapers. While these whitepapers sometimes have a strong commercial background, the information in these papers can still be relevant for this research. However, using these sources as part of this research must be done carefully. For this reason, the information extracted from these sources is validated using a survey with a number of SOCs. This is further explained in paragraph 4.2.

To obtain whitepapers regarding SOCs, the Google search engine was used with the following search terms:
- “SOC maturity”
- “SOC capability”
- “SOC measurement”
- “SOC design”
- “SOC roles”
- “SOC personnel”
- “SOC performance”
- “SOC best practices”
- “SOC model”
- “SOC services”
- “SOC processes”
- “SOC technologies”

These search terms are based on the previously mentioned research questions, augmented with terms related to this research. Instead of the abbreviation, the full term “Security Operations Center” was also used in these queries. With the queries from the previous step, a large number of search results was returned. After further evaluation, a total of 41 potentially relevant sources were found. Further selection of relevant studies was carried out in the next step.

3. Study Selection. For the selection of relevant literature, a set of inclusion criteria was created. The inclusion criteria are the following:
   - Does the publication explicitly define SOC elements, such as services, processes, roles and technologies?
   - Is the publication a formal publication? (i.e., not a weblog entry)
   - Does the publisher have some industry credentials? This is an indicator of trustworthiness of the information.

Using these inclusion criteria, 20 sources were deemed relevant from the previous list of 41 resources. These sources include whitepapers [37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55] and industry event presentations [56, 57].

4. Quality Assessment. Under normal circumstances, the quality assessment would focus on the methodology applied in the research, the research rigor and other aspects of the publication such as the quality of the journal in which it was published. In this case, due to the nature of the information, such quality indicators are not present. Therefore, this step was skipped in the literature review process. Instead, an additional research step in the form of a survey was executed. This step is a verification step and has a similar quality assessment function.

5. Data extraction. An analysis was performed on these sources by creating an overview subdivided into the 4 domains: people, process, technology and business & organisation. Then, following information was gathered for each of the above mentioned papers:
   - Information regarding the source itself:
     - Name: the name of the source
     - Author(s): the author or authors of the source
     - Publisher: the publisher of the source
     - Year: year of publication
   - Detailed reference:
     - The page number in which the information was found
The SOC elements described in the source:
- For the ‘people’ domain, this was the role mentioned in the paper
- For the ‘process’ domain, this was the name of the process mentioned in the paper
- For the ‘technology’ domain, this was the name of the technology mentioned in the paper
- For the ‘business & organisation’ domain, this was the name of the business aspect mentioned in the paper

Maturity information:
- Maturity indicators mentioned in the paper
- Maturity level mentioned in the paper. This information was relatively scarce in the papers examined.

6. Data Synthesis. Lastly, data synthesis was performed on the data extracted in the previous step. For this purpose, normalisation was applied to the SOC element column. This was required due to the fact that many different terms were used for the same element, making aggregation of results impossible. For example, the normalised element ‘Mission, Vision, Strategy’ contains the following 9 elements from 7 different sources:
- Demonstrate Vision
- Mission
- SOC Definition
- Service Vision & Strategy
- Charter
- Strategy
- Objectives
- Deliverables
- Business Process
- SOC Mission

By normalising this information and grouping it into a single element, an analysis can be done on the occurrence of these ‘element groups’ in literature. These normalised groups were created by grouping elements that are closely related. Annex A contains the aggregated results for all domains.

Figure 4 shows the summary with the number of elements found per domain. It is clear that the ‘process’ domain by far has the most elements. Many of the sources have an explicit focus on the process conducted by the SOC. No apparent reason for this focus was found in the literature analysis. Further research would be required to determine the reason for this focus.
The data synthesised in the last step was used to address the research questions. As indicated, validation of these results is done in the survey, as described in paragraph 4.2.

4.1.2 Literature on capability maturity models

The second part of the SLR focused on capability maturity models. Before going into the details of the SLR itself, a definition of capability and maturity is required.

Maturity levels are described in the Capability Maturity Model Integration (CMMI) for services (CMMI-SVC) [58]: “The maturity level of an organization provides a way to characterize its performance [...] A maturity level is a defined evolutionary plateau for organizational process improvement”. Subsequently, each of the maturity levels has its characterization described in detail. So maturity is about how well a process is performing. While this is important to establish, it is not the only thing to evaluate. A process may be executed and described efficiently and effectively, but may still not have the desired effect. This can be the case when the process lacks certain capabilities.

Capabilities are indicators of how complete the process is. The difference between capability levels and maturity levels are visualised in Figure 5. To summarize, maturity assesses how a process is carried out, while capabilities focusses on what the process looks like. Some of the models mentioned previously have a strong focus on capabilities, while others are more focussed on the maturity characteristics. CMMI was created to explicitly consider both maturity and capabilities. The model and artefact that were created for this thesis consider both capability and maturity as well.
The figure also shows that maturity is represented as a staged process, while capability is continuous. In this research, both maturity and capability are continuous.

Another SLR was carried out to determine the available information on Capability Maturity Models. Again, the steps by Kitchenham and Charters were used:

1. Define research questions. The research questions for this part of the systematic literature review are:
   - What different types of capability models exist?
   - What capability maturity levels exist?
   - What are the capability maturity levels based on?

2. Define a search strategy. For this part of the literature review, both scientific research and non-scientific research is available, so the search strategy should focus on obtaining relevant information from both sources. For non-scientific literature, the Google search engine was
used. For scientific literature, 3 relevant libraries were identified: ScienceDirect Journals, Association for Computing Machinery (ACM) Digital Library and Institute of Electrical and Electronics Engineers (IEEE) Xplore. The relevancy of these libraries was using the library focus and contents. The following search terms were derived from the research questions and applied to the library search engines:

- “Capability Maturity Model”
- “Security + Maturity”
- “Security + Capability”
- “Security Service + Maturity”
- “Security Service + Capability”
- “Maturity Levels”
- “Capability Levels”

3. Study Selection. The following inclusion criteria were used to evaluate the literature for non-scientific research:

- Does the publication provide original insight into capability maturity?
- Is the publication a formal publication? (i.e., not a weblog entry)
- Does the publisher or publishing organization have some industry credentials?

The following inclusion criteria were used to evaluate the literature for scientific research:

- Is the research published recently? Preferably, the research should be published in the last 5 years. Due to the more static nature of this research, earlier research can also be included, but has less value to the SLR.
- Does the research provide original insights? Literature reviews can also be included, as a means of providing additional basis for other research.
- Is the research published in a scientific journal or scientific symposium?

With the search terms from the previous step, a large number of search results were returned. These were trimmed down based on the research abstract or introduction. Finally, using the inclusion criteria, 24 sources were found that were deemed relevant to this research.

4. Quality Assessment. The quality assessment was carried out on the scientific literature as a final check to determine if the paper was of sufficient quality. For this purpose, the references used in the papers were examined. This led to the exclusion of one of the papers found.

5. Data extraction. Data extraction was performed on the 23 remaining sources. Data extraction focused on the research questions. Thus, the maturity levels (if indicated) were noted. Data extraction also focused on the characteristics of the different maturity levels and the advancement between these levels. Finally, the capability maturity model as described in the paper was classified in one of four types: generic, information security, SOC-specific, service-specific.

6. Data synthesis. Data synthesis for this part of the literature review focused on two main elements: different types of models and different capability maturity levels used in models. These elements are described below
Capability maturity model types

In the literature review, 4 types of capability maturity models were encountered:

1. Generic (capability) maturity models. Maturity models are usually generic and can be applied to any element under assessment. Since security is an integrated part of most services, one of the most commonly used maturity models, CMMI-SVC, has not included any security-specific content. However, in a later publication, some security goals and practices were released [59] (even though they remain not officially part of the CMMI model). Similar work was done by Ibrahim et al. for Federal Aviation Administration Integrated CMM (FAA-iCMM) and CMMI [60].

2. Information security (capability) maturity models. Specific maturity models for information security were also encountered. These maturity models include the ISA-CMM [61], Gartner ITScore for Security & Risk Management [62], Risk Management Process Maturity [63], Cybersecurity Capability Maturity Model (C2M2) [64], Information Security Management System (ISMS) (Im)-Maturity Capability Model [65], Systems Security Engineering CMM (SSE-CMM) [66, 67], Open Information Security Management Maturity Model (O-ISM3) [68] and lastly Control Objectives for Information and related Technology (COBIT) [69]. All these models deal with more abstract topics like security management, risk management and security engineering.

3. SOC-specific (capability) maturity models. In the literature study, specific capability maturity models for SOCs were also encountered. These models are proprietary and part of a commercial offering. Thus, no information is provided as to the details of those models. Examples of commercial models are: the HP Security Operations Maturity model (HP SOMM) [70] and the maturity measurement as part of IBM SOC consulting services [71].

4. Service-specific (capability) maturity models. Lastly, maturity models specific for security services were also encountered. For example, Bromberger and Maraschino define 6 levels of maturity (from 0 to 5) specifically for security log management [72]. They describe prerequisites, activities, integration, staff, tools and training for each level. This is basically a method to apply people, process and technology to each maturity level. Another example of a single-service model is the Enisa Industrial Control System Supervisory Control And Data Acquisition (ICS-SCADA) maturity [73] model. Lastly, several publications are available regarding security incident management, mostly under the name of Computer Security Incident Response Team (CSIRT). This shows again that security incident management is considered an important security task. Examples of security incident management-specific capability maturity models are SIM3 [74] (and the CSIRT maturity tool [75] based on that work), the Enisa CSIRT capabilities evaluation [76] and the RSA capability maturity model [77].

Some comparisons of (capability) maturity models were also found in the literature review, such as the works by Akridge and Chapin [78], Dzazali et al. [79] and Stambul and Razali [80]. In these works, many of the previously mentioned models, especially COBIT, CMM-SSE and CMMI, are discussed.

Maturity levels

Maturity models have maturity levels. The idea is that, through assessment and planning, advancement can be made to higher levels by organisations desiring a higher maturity level. In the
literature review, maturity models have been identified with 3, 5, 6 and 9 levels. Table 1 shows the number of times a particular number of levels was encountered.

<table>
<thead>
<tr>
<th>Number of levels</th>
<th>Number of times encountered</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

Most commonly, 5 or 6 levels of maturity are distinguished. Where 6 levels are present, these mostly include a level ‘0’, which is non-existent. 5-level maturity models usually start at level ‘1’ (initial). CMMI distinguishes 4 levels of capabilities (starting with level ‘0’) and 5 levels of maturity (starting with level ‘1’). Many other models are based on the CMMI maturity and capability model and thus share the number of maturity and capability levels.

Descriptions of maturity levels vary greatly between publications. Not all sources specify what the maturity levels are exactly and how advancement from one maturity level to the next is possible. This is especially true for commercial models (i.e. HP SOMM, IBM). Other sources specify the activities that need to be taken place at each of the maturity levels, or a brief description of process or organisation characteristics at each of the maturity levels. Other sources are relatively complete by stating the activities that need to be carried out for each level and a statement of when a new level is reached. In all sources where this is made explicit a new level is reached when all requirements of the maturity level and levels below are satisfied. Requirements are usually stated as ‘goals’ or ‘activities’.

While this information is mostly irrelevant for the survey, the information is important input into the creation of the design artefact.

Some additional findings unrelated to the research questions have also come from the literature review on capability maturity models. These findings include CMM domains, guidance for using models and visualisation and are described below.

About domains
Some maturity models divide capabilities in several domains. Common domains are people (or human), process, technology (or tools) and organisation. Other domains are business and foundation. This is consistent with the findings in the literature analysis regarding SOCs. A subdivision in domains provides additional insights as these domains are usually managed in a different way. Technology-driven organisations may have a high technology maturity, but not have a high process maturity. This should be balanced out for optimum performance. Thus, the tool should also use domains to more effectively measure strengths and weaknesses.

About model guidance
The CMMI-SVC document provides guidance on advancing through capability and maturity levels. Additionally, the document provides information on how to use the model. The same applies to the
A C2M2 model. Since the tool is intended to be used as self-assessment, this should be described as well.

**About visualisation**

Visualisation of maturity assessment outcomes is done in several documents. The main visualisation methods are using a bar chart that indicates maturity levels for particular service, controls or capabilities (for example: ISA-CMM and CMMi-SVC). In other documents, a radar chart is presented as a means of showing maturity levels for different areas (for example: SIM3, Jacobs et al., ENISA ICS-SCADA maturity, Mayer and Fagundes). While radar diagrams work well to provide an overview (with a limited number of elements), a bar chart is more efficient for large amounts of information. Both should be considered for the tool.

### 4.2 Survey

As indicated, most of the literature regarding SOCs was non-scientific. Thus, a survey was added as an additional step to verify whether the aspects identified in the literature analysis exist in actual SOCs. The survey was created using the information gathered in the literature study on SOCs (see paragraph 4.1.1). For survey design, the 6 principles as indicated by Andrews et al. [81] were used:

- Support multiple platforms (and browsers). The survey was created using Microsoft Word. This makes it compatible with any system running Microsoft Office or any productivity suite compatible with Microsoft Office. Since the survey is an offline survey (due to confidentiality reasons), browser requirements do not apply.
- Prevent multiple submissions. This requirement does not apply. Multiple submissions are not expected in survey. Submissions are done via email, optionally encrypted.
- Present questions in a logical or adaptive manner. The survey was divided into six logical parts:
  - Part I: Contact and general information. This part consists of 7 questions regarding the contact information for the organization under evaluation, the sector in which the SOC was operating and whether the participant was willing to participate in the maturity tool try-out.
  - Part II: SOC Organisation. This part consists of 10 questions regarding the current (perceived or measured) maturity level, service delivery, SOC scope, SOC size, outsourcing and Computer Emergency Response Team (CERT) integration.
  - Part III: Business. This part consists of 6 questions regarding customers, business drivers, governance, budget and a charter document.
  - Part IV: People. This part consists of 7 questions regarding number of employees, roles and tiers, people management and hierarchy.
  - Part V: Process. 17 questions are asked regarding processes in the SOC. 16 processes are evaluated in detail, the last question deals with 5 processes high-level. The reason for this is that most services were mentioned in many documents, but some were scarcer. For the more scarce processes, the amount of detailed information present was low. This is a strong indication that the service is not part of ‘normal’ security operations and should not be investigated in detail. These services were added to the survey confirm this. See appendix A, Table 10, for details regarding the number of times a service was mentioned in the literature.
For each of the process, the process execution, service delivery, process importance and perceived maturity level are inquired about. Additionally, specific capabilities and process artefacts (such as procedures) are listed as checkbox items where the participating organisations can indicate whether or not the item is present in their SOC. This results in a large amount of information to be processed. For example, security incident management alone has 36 artefacts and capabilities that need to be evaluated. This level of detail requires a significant time investment from the participants, but is required to validate the information found in non-scientific sources. The level of detail also has an impact on the need for confidential information processing. This is discussed in paragraph 4.2.1.

- **Part VI: Technology.** In the last part of the survey, 4 questions are asked regarding available technology in the SOC. 3 technologies are inquired about in detail: Security Information and Event Management (SIEM), Security Analytics and Intrusion Detection and Prevention Systems (IDPS). Additionally, 12 technologies are inquired about high-level. Again, the reason for this division is the number of references to the technology as well as the number of details (particularly capabilities) found in the literature.
  - Provide opportunities for saving. Given the size of the survey, this requirement applies. The auto-save function in Microsoft Office enables automatic saving and recovery in cases of unexpected program terminations. Additionally, it provides the option for manual saving so that the survey can be completed in multiple sessions.
  - Collect selection options and narrative type questions. Both these types of questions were included. Mostly, the selection options were used to reduce the amount of time required to complete the survey and to promote consistency among answers. Most questions in the survey provided an option to specify “other values” or “remarks”. Every section ended with an option to provide general feedback regarding that section.
  - Provide feedback “thank you”. Due to the type of survey, automated feedback was not possible. This was a manual activity. After completion of the survey, all participants received regular (monthly) updates on the research progress.

As indicated, the survey was sent via email. A period of 2 months was provided to each of the participants to return the completed survey form. This extensive time period was applied due to the length of the survey and the period (end of calendar year) in which the survey was distributed. The detailed results from the survey are discussed in paragraph 4.2.3.

### 4.2.1 Confidentiality and anonymity

As indicated in the previous paragraph, the level of detail of the survey presents a risk to participating organisations as the strengths and weaknesses of their security defences are revealed. To ensure sufficient participation to the survey, the following agreement was made with all participants:

“A note on privacy: detailed results from this questionnaire will not be published. Only aggregated values are used to determine the contents of the toolkit and the underlying model. From these aggregated values, it will not be possible to deduce which organizations have taken part in this research or which answers have been provided by a participating organisation. Participating organisations will not be named.”
4.2.2 Guidance
To ensure that the results from the survey are consistent across participating organisations, an introduction page was created that provides guidance on how to use the survey. This introduction also explains what survey parts should be answered by the SOC manager, and what parts should probably be answered by a (senior) SOC employee. The introduction page to the survey is added to this thesis in Annex B.

Additionally, a glossary was created that explains the terminology used within the survey. This glossary contains 83 terms. The advice given in the introduction was to print out the terminology pages and use them as a reference when filling in the survey. For every term explained in the glossary, a reference was provided to the section in which the term was used. Not every term was explained, but an option was provided for support in case of questions regarding the terminology or the survey itself.

4.2.3 Survey results
In total, there were 20 organisations initially willing to participate. When the survey was completed, 2 participants withdrew from the study due to confidentiality issues. The survey was thus sent out to 18 organisations, 16 of which returned the completed survey (80%). The returned survey forms were analysed as a single data set.

For a study to be representative, it is important that the participants form a diverse group. Thus, SOCs were needed from different sectors and different ages and stages of maturity. Additionally, for added diversity, the SOCs should be different in size and scope. Figure 6, Figure 7, Figure 8, Figure 9, Figure 10 and Figure 11 show the diversity of the SOCs under investigation. Note: ‘N/A’ is displayed when the information was not provided by the participant. This may be due to confidentiality reasons or simply because the information is not available.

![Figure 6: SOC sectors](image-url)
Figure 6 shows that most participants operate in the finance sector. However, 5 other sectors are represented as well.

![Figure 6: SOC age - number of years in production](image)

Figure 7 shows that most SOCs are relatively new (5 year or less in existence). This is an indication of relatively slow adoption of SOC in the industry. This research does not provide an explanation for this. Further research on the adoption rate is required.

![Figure 7: SOC age - number of years in production](image)

Figure 8 shows the perceived or measured maturity levels. Most SOCs indicated that they perform at CMMi level 3 (managed). Only 2 SOCs actually used some methodology or consulting to measure their SOC.

![Figure 8: SOC Maturity - Perceived (estimated or measured) maturity levels](image)
Figure 9: SOC size - number of monitored assets

Figure 9 shows the number of monitored assets in the SOC. The sizing numbers are taken from the Mitre study [52].

Figure 10: SOC size - staffing (in FTE)

Figure 10 shows the SOC size in number of Full Time Equivalent (FTE).
Figure 11 shows the geographic scope of the SOC. Most participants operate either at the national or global level. The scope is taken from the Mitre study [52].

These figures show that the SOCs under evaluation differ in size, scope, maturity and number of employees. These aspects indicate that the participants in the survey represent a diverse group of SOCs that is suitable for research. The differences in maturity are especially relevant given the focus of this research.

For each of the domains in the survey, an analysis was conducted to determine if the SOC elements identified in the non-scientific literature actually exist in actual SOCs. For the ‘domains’ business and ‘people’, all of the elements identified in the literature analysis and inquired on in the survey were found among the participant, albeit that the occurrence varies: some elements were only encountered among 1 or 2 participants, while others exist among all participants.

In the questionnaire, the participants were given the option to indicate for each process whether or not the SOC played a role in the process and whether or not that role was exclusive to the SOC or shared with another department or external team. In the analysis, an aggregated view was created that displays the number of times a particular process was encountered among the participants. This view can be used to determine which services should be part of the tool. Figure 12 shows these aggregated results.
To limit the scope of the tool to a set of processes that apply to most SOCs, all services that are common in the majority (>50%) of the survey participants are candidates for inclusion into the research. These services are: “Security Incident Management”, “Security Monitoring”, “Security Operations”, “SOC Reporting”, “Security Analysis”, “Security Incident Management”, “Threat Intelligence”, “Vulnerability Management” and “Log Management”.

Additionally, the criticality of the service was also inquired about: how important is the service to the SOC under evaluation? Services that are considered to be of ‘low’ or ‘no’ importance are excluded from the selection. Figure 13 shows the criticality of services as indicated by the participants. The services “Security Incident Management” and “Security Monitoring” clearly stand out as most critical services. The figure also shows that the other services mentioned above also represent the most important services for the SOCs under evaluation. Thus, no services are excluded from the initial selection based on majority.
Similar to the process domain, the participants were also inquired about the tooling in use by the SOC. Participants were able to indicate for each tool whether they performed technical management and functional management or whether they were merely a user of the tool (which is managed by another team). This question was used to determine which tools should be within scope of the capability maturity assessment tool. Figure 14 shows the overview of tools used by the SOC and the activities performed by the SOC. 7 different combinations of activities were found.

The most important tools to include in the capability maturity assessment tool are those in which the SOC has a functional and/or technical management role. This is because mere usage of the tool only
provides a limited opportunity for improvement as such improvements are either technical and functional and thus outside of the span of control for the SOC. Figure 15 shows a simplified view of the tools in which only tooling usage and tooling management is shown.

![Figure 15: Simplified tooling view](image)

Figure 15: Simplified tooling view

Again, to limit the scope of the capability maturity assessment tool, only the tools that are used in the majority (>50%) of the SOCs are candidates for inclusion. These tools are: SIEM, Vulnerability Management Tooling, IDPS, Ticket Management System, Malware Detection Tooling, Security Analytics and Log Management Tooling. This research only includes those tools, for which the majority (>50%) of SOCs has indicated that the tool is within their span of control. Thus, Ticket Management System (54% outside of the SOC span of control) and Malware Detection Tooling (72% outside of the SOC span of control) are excluded. This leaves the following tools to be included into the research: SIEM, Vulnerability Management Tooling, IDPS, Ticket Management System and Security Analytics.

### 4.3 Design Artefact

With the completion of the survey, sufficient information is available to create the artefact. This paragraph discusses the design and creation of the artefact: a tool for self-assessment of the SOC capability maturity levels. This is done by first looking at maturity model design in general, and then focusing specifically on the artefact created in this thesis through requirements, design of the model itself and implementation.

#### 4.3.1 Maturity model design

According to Laehmann et al. [82], 2 basic approaches exists for designing a maturity model: a top-down approach, where the maturity levels are defined first and the characteristics are filled in later, and a bottom-up approach, where the characteristics are determined first and later on mapped to maturity levels. In this case, a bottom-up approach is used. The characteristics have been identified by performing a literature review and validating the results using the survey. Laehmann et al. also summarize a development methodology for maturity models, which is consistent with the
methodology applied in this research (Offermann et al.) and the design science research approach as defined by Hevner in general.

Maturity models also have common characteristics. These characteristics are outlined in the work of Raber et al. [83]:

- **Object of maturity assessment.** In this case, the object of the maturity assessment is the SOC.
- **Dimension.** Dimensions are defined as ‘capability areas’ in the work of Raber et al. In this case, 5 dimensions are applied. These 5 dimensions are based on the survey outcome and a logical grouping of elements. This is further elaborated in paragraph 4.3.3.
- **Level.** Levels are used as a concrete indicator of maturity for the SOC. In this case, 6 maturity levels are used, starting at level 0 (non-existent) up to level 5 (optimising). The naming convention for levels 1 through 5 is consistent with the names used in CMMI. Additionally, the description of the CMMI levels was used to determine which questions are asked for each aspect under evaluation, thus putting the bottom-up approach in practice. This is explained further in in paragraph 4.3.3.
- **Maturity Principle.** According to Fraser et al. [84], 2 basic types of maturity models exist: staged models and continuous models. For staged models, different activities are specified at different maturity levels. Staged maturity means all activities for a certain level need to be met in order to function at that maturity level or advance to the next maturity level. Activities can exist in multiple maturity levels, but are different in details and goals in different maturity levels. Continuous models, however, assess items independently. Thus, there are no ‘prerequisites’ for maturity levels.

For this artefact, a continuous maturity model is used. This is due to the fact that insufficient (objective) information is available on the performance of the characteristics on each maturity level. Additionally, it was found that creating staged maturity assessment tool, based on dependencies and pre-requisites for each level is technically not feasible. So where the CMMI shows maturity as staged and capability as continuous (Figure 4); in this artefact both capability and maturity are continuous.

- **Assessment.** Lastly, Raber et al. indicate that a maturity assessment can be created using qualitative or quantitative approaches. In this research, both types of approaches are applied to optimize the outcome.

### 4.3.2 Requirements

In order to build a satisfactory artefact, a set of requirements was created. These requirements are based on the ISO/IEC 25010 (Security Quality Requirements Engineering, SQuaRE) model for software quality [85]. The decision for this model was based on a review of software quality models performed by Miguel et al. [86] and was selected due to the fact that it is an industry standard. Figure 16 shows the ISO/IEC 25010 standard attribute profile.
The ISO/IEC 25010 standard is a quite extensive standard that has a lot of attributes. Not all of these are applicable to this tool, as the standard mainly applies to software development, which is not done in this research. Additionally, some of the attributes are covered by Microsoft Excel, in which the assessment tool was built. A specific attribute profile was created and is shown in Figure 17. The attributes covered by Microsoft Excel are marked in green. These attributes are briefly discussed.

**Functional suitability**

Appropriateness. Naturally, appropriateness is one of the most important attributes for the tool. Basically, appropriateness is an indication of how well the tool is capable of performing its primary function: determining strengths and weaknesses of the SOC using maturity and capability levels. The appropriateness of the tool was determined in a try-out evaluation. This requirement is aligned with the meta-requirement ‘effectiveness’ from paragraph 2.1.1.
Accuracy is an important aspect as well: the tool should be accurate in determining the maturity level. Without some sort of standard or reference, this is difficult to determine. Thus, in the try-out evaluation, there should also be focus on how well the output from the tool matches the organisations expectations (or actual measured values). This requirement is aligned with the meta-requirement ‘accuracy’ from paragraph 2.1.1.

Reliability
For reliability, fault tolerance was selected as the primary attribute. The artefact should be fault tolerant by limiting input options or checking input provided by the persons performing the self-assessment. For recoverability, Microsoft Excel provides recovery options in case of unexpected program terminations.

Performance efficiency
The performance of the artefact depends on the performance of Microsoft Excel in general. Naturally, the performance of Microsoft Excel can be affected by complex calculations in the Microsoft Excel file. Thus, only standard Microsoft Excel elements are used and complexity is avoided in general. This also increases maintainability of the artefact and increases fault tolerance at the same time.

Operability
Several of the aspects within the operability quality area apply to the artefact:

- Appropriateness recognisability. This requirement indicates that the organisation using the assessment should quickly be able to determine whether or not the tool is appropriate for their needs. This requires an explanation of the purpose of the tool and a scope definition that allows the organisation to determine whether the tool matches the setup of the SOC.
- Learnability. Given the fact that the artefact is meant for self-assessment of the SOC, learnability is a very important aspect. The tool should be straightforward in its use and guide the person using the tool in the right direction. For this purpose, a flow is created in the tool using Excel tabs. Additionally, a brief introduction is provided that explains how to use the tool. This requirement is aligned with the meta-requirement ‘easy to use’ from paragraph 2.1.1.
- Ease of use. Similar to the previous requirement, the tool should be easy to use. For this purpose, the tool uses dropdown menus for most answers. This reduces the number of options for the person using the tool, and additionally helps to standardize output and keep the tool as simple as possible, thus making it more fault tolerant. This requirement is aligned with the meta-requirement ‘easy to use’ from paragraph 2.1.1.
- Attractiveness. The tool should be attractive to use, and especially provide attractive results to the person using the tool. Thus, layout is an important aspect. As indicated in paragraph 4.1.2, bar charts and radar charts can be used for visualising results.
- Technical accessibility. This attribute is covered by Microsoft Excel.

Security
Most security requirements are not applicable to the tooling because of its purpose. The most important attribute is confidentiality. While this attribute can be covered outside the environment of the tool, it is also possible to encrypt the document using standard Microsoft Excel functionality.
Compatibility
For compatibility, interoperability was selected as a relevant attribute. In this case, the focus is not on technical compatibility (which is covered by Microsoft Excel), but compatibility of the output of the tool to other frameworks. This is important to increase the value and acceptance of the tool. The tool should at least be compatible with some existing framework. The choice was made to align the output of the tool to the NIST Cybersecurity framework [87]. This framework is being adopted more and more in the security industry, as it includes COBIT, ISO27001 and NIST standard requirements. Lastly, since the security incident response process has some detailed maturity scoring models available (see paragraph 4.2.1.2), a possibility should be provided to align with other maturity models. This is implemented by allowing a ‘score override’ specifically for the security incident management process.

Maintainability
Maintainability attributes are not very important for this artefact, although it is possible that the artefact will be maintained in the future. Again, simplicity is applied throughout the artefact to support maintainability as well as other attributes.
- Modularity. From literature, we know that there is great diversity between SOCs. The survey results confirm that this is indeed the case. Thus, the artefact should preferably support some form of modularity so that additional services, technologies can be added later. This attribute is addressed by using a standard template for services and technologies (in which the SOCs show the most diversity).
- Reusability. Reusability of the artefact is covered by Microsoft Excel itself. By creating a copy of the self-assessment document, the artefact can be used multiple times.
- Changeability. The tool should preferably be adaptable to the needs of a particular SOC. This attribute has a strong connection to modularity and is enabled by simplicity.

Transferability
The final attribute group is transferability, in which 2 attributes are important: portability and installability. Both these attributes are covered by using Microsoft Excel as a basis for the tool.

Not all requirements are deemed equally important. Therefore, a prioritization is applied to the requirements using the MoSCoW technique [88, 89], a prioritization technique used in the Dynamic System Development Methodology (DSDM). This technique applies prioritization by labelling requirements as ‘Must haves’, ‘Should haves’, ‘Could haves’ and ‘Won’t haves’. While the MoSCoW technique does not provide for very accurate prioritization [90], it is sufficient for this small set of requirements.

Table 2 shows the requirements with prioritization applied. Only the requirements that were not covered by Microsoft Excel itself are part of this prioritization, as the other requirements are met regardless of the outcome of the artefact design process. Therefore, the priority of those requirements is not relevant.
Table 2: MoSCoW prioritisation of requirements

<table>
<thead>
<tr>
<th>Requirement group</th>
<th>Requirements</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Suitability</td>
<td>Appropriateness</td>
<td>Must have</td>
</tr>
<tr>
<td></td>
<td>Accuracy</td>
<td>Must have</td>
</tr>
<tr>
<td>Reliability</td>
<td>Fault tolerance</td>
<td>Could have</td>
</tr>
<tr>
<td>Operability</td>
<td>Appropriateness recognisability</td>
<td>Must have</td>
</tr>
<tr>
<td></td>
<td>Learnability</td>
<td>Must have</td>
</tr>
<tr>
<td></td>
<td>Ease of Use</td>
<td>Must have</td>
</tr>
<tr>
<td></td>
<td>Attractiveness</td>
<td>Should have</td>
</tr>
<tr>
<td>Compatibility</td>
<td>Interoperability</td>
<td>Could have</td>
</tr>
<tr>
<td>Maintainability</td>
<td>Modularity</td>
<td>Should have</td>
</tr>
<tr>
<td></td>
<td>Changeability</td>
<td>Could have</td>
</tr>
</tbody>
</table>

‘Won’t have’ requirements are not in this table. The requirements that were not selected from the initial SQuaRE model can be considered ‘Won’t have’ requirements.

4.3.3 Model

The maturity model is divided into 5 domains. These domains are based on the 3 basic domains that are part of ITIL (people, process and technology). Since the process domain covered generic processes (such as reporting) and specific processes (such as vulnerability management), a further division was made for process domain. This domain was divided into in process (generic) and services (specific). The last domain is ‘business’, which is a simplification of ‘business & organisation’ as used in the survey. These domains were then subdivided into criteria:

- Business. The business domain was subdivided into the criteria: business drivers, customers, SOC charter and governance.
- People. The people domain was subdivided into the criteria: employees, roles & hierarchy, people management, knowledge management and training & education.
- Process. The generic processes that were identified and added to this domain are: reporting, management and operations & facilities.
- Technology. For the technology domain, the following 3 technologies were selected from the overview (see Figure 14): SIEM, IDPS and Security Analytics. Again, this selection was made based on the fact that most SOCs performed some form of technical of functional management activities for these tools. As a tooling user, it would be hard to change the maturity level, thus evaluating it as part of the SOC scope would have little added value. The vulnerability management and log management tools were also identified to be present for most SOCs. These tools, however, were included into the respective services in the ‘services’ domain.
- Services. For the services domain, the following processes were selected from the overview (see Figure 12): Security Monitoring, Security Incident Management, Security Analysis, Threat Intelligence, Vulnerability Management and Log Management. Again, the main driver for selection was the number of participants that partial or full responsibilities in executing that particular service and the criticality. Additionally, the criticality of those services as indicated in the survey (see Figure 13) was also used.

This is summarised in the capability maturity assessment model, as depicted in Figure 18.
The domains and aspects in blue are evaluated for maturity only, the aspects and domains in purple are evaluated for both maturity and capability. The next section provides more detail on maturity and capability for the artefact.

**Maturity Aspects**

For the domains ‘business’, ‘people’, ‘process’ and ‘technology’, the information that were inquired upon in the questionnaire were converted into questions and grouped logically under the aspects in the assessment model. For example, the questionnaire inquired about business drivers for the SOC. This item is converted into the following 5 questions in the tool:

- Have you identified the main business drivers?
- Have you documented the main business drivers?
- Do you use business drivers to in the decision making process?
- Do you regularly check if the current service catalogue is aligned with business drivers?
- Have the business drivers been validated with business stakeholders?

These questions are based on the descriptions for each of the maturity levels in the CMMI for services. It must be noted that there is no direct match between, and that interpretation is required. However, this form of creativity can be expected in design research [21]. The general rule for the creation of these questions is:

- Has the aspect been formally identified? This is an indicator of maturity level ‘Initial’.
- Has the aspect been formalised for repeated quality? This is an indicator of maturity level ‘Managed’.
- Has the aspect been fully documented and formalised? This is an indicator of maturity level ‘Defined’.
- Is the aspect being measured for process optimization goals? This is an indicator of maturity level ‘Quantitatively managed’.
- Is the aspect being measured for organisational optimization goals? This is an indicator of maturity level ‘Optimizing’.
For the services domain, a more direct mapping between the CMMI-SVC and the maturity tool can be used.

**Capability Aspects**

Capabilities apply to services and technologies: what (technical and procedural) features are available to the service or technology under evaluation? And thus: what is the service capable of in the service delivery sense? The capabilities used in the tool are based on the results of the survey. As indicated, all of the features in the questionnaire were found in one or more SOCs. All features were investigated for occurrence, and for those features deemed uncommon, additional examination was performed. To quantify ‘uncommon’, the percentage of mature SOCs from the pool of participants was used: 25% (see Figure 8).

The additional examination consisted of determining the maturity levels of the SOC that implemented that feature. This is because lack of occurrence in other SOCs could be due to the fact that the feature is an indicator of high maturity. Thus, if the ‘uncommon’ feature was present mostly in mature SOCS (i.e. > maturity level 3), the feature is included in the tool. If the uncommon feature was implemented in a SOC with lower maturity level, the feature is excluded from the tool.

For example, Figure 19 shows the capabilities for the security monitoring service from the questionnaire. The blue bars on the left indicate percentage of survey participants that implemented this feature.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>62.5</td>
<td>Early detection</td>
</tr>
<tr>
<td>75</td>
<td>Intrusion detection</td>
</tr>
<tr>
<td>43.75</td>
<td>Exfiltration detection</td>
</tr>
<tr>
<td>25</td>
<td>Subtle event detection</td>
</tr>
<tr>
<td>87.5</td>
<td>Malware detection</td>
</tr>
<tr>
<td>56.25</td>
<td>Anomaly detection</td>
</tr>
<tr>
<td>81.25</td>
<td>Real-time detection</td>
</tr>
<tr>
<td>56.25</td>
<td>Honeypotting</td>
</tr>
<tr>
<td>75</td>
<td>Alerting &amp; notification</td>
</tr>
<tr>
<td>37.5</td>
<td>Status monitoring</td>
</tr>
<tr>
<td>62.5</td>
<td>Perimeter monitoring</td>
</tr>
<tr>
<td>68.75</td>
<td>Host monitoring</td>
</tr>
<tr>
<td>75</td>
<td>Network &amp; traffic monitoring</td>
</tr>
<tr>
<td>81.25</td>
<td>Access &amp; usage monitoring</td>
</tr>
<tr>
<td>62.5</td>
<td>User monitoring</td>
</tr>
<tr>
<td>43.75</td>
<td>Application &amp; service monitoring</td>
</tr>
<tr>
<td>25</td>
<td>Behaviour monitoring</td>
</tr>
<tr>
<td>37.5</td>
<td>Hunting team</td>
</tr>
<tr>
<td>81.25</td>
<td>Use cases</td>
</tr>
<tr>
<td>31.25</td>
<td>Acceptable use policy</td>
</tr>
<tr>
<td>12.5</td>
<td>User consent to monitoring</td>
</tr>
</tbody>
</table>

Figure 19: Survey results for security monitoring

In this figure, 4 uncommon features (marked yellow) were investigated for matching to maturity levels and remarks made in the survey. Based on this investigation, ‘honeypotting’ and ‘user consent to monitoring’ were removed from the list of features for the security monitoring service.
4.3.4 Scoring model
For the artefact under construction, 2 scoring models are relevant: the maturity scoring model and the capability scoring model.

**Maturity Scoring**
For each of the questions created, a 5-point scale was used. In total, there are 4 of such scales: completeness (incomplete to fully complete), importance (none to critical), Occurrence (never to always), Satisfaction (no to fully). The answers selected for the questions relate to the maturity levels. Table 3 shows a scoring example for ‘completeness’.

<table>
<thead>
<tr>
<th>Answer</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete</td>
<td>0</td>
</tr>
<tr>
<td>Partially complete</td>
<td>1,25</td>
</tr>
<tr>
<td>Averagely complete</td>
<td>2,5</td>
</tr>
<tr>
<td>Mostly complete</td>
<td>3,75</td>
</tr>
<tr>
<td>Fully complete</td>
<td>5</td>
</tr>
</tbody>
</table>

Scoring of the items is done using relative decision making, where the person or group of persons performing the assessment judge the current level based on what is perceived as ‘fully’.

**Maturity Weighing**
To provide more flexibility in the determination of the right maturity level, a weighing possibility was added to the self-assessment tool. This is similar to the mechanism applied in the CREST tool [91] and is also described Open Group Service Integration Maturity Model (OSSIM [92]). For each sub-criterion under evaluation, the weighing could be changed to influence the scoring of the criterion.

This scoring can be influenced by the organisation conducting the assessment by using the weighing mechanism, which is also a 5-point scale. The weighing mechanism allows for diminishing or amplifying scores based on the importance of the aspect under evaluation within the target organisation. Basically, this mechanism provides a means to personalize the tool to the SOC under evaluation. For example: an aspect may not be implemented in a particular organisation, but if this is known and a conscious decision (for example: because it is outside of the SOC scope due to specific business drivers), the element can be removed from scoring so that it does not negatively affect the score. The weighing mechanism works by multiplying the score with a predetermined factor. Table 4 shows the weighing mechanism that is applied in the artefact.

<table>
<thead>
<tr>
<th>Importance</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (removes from scoring)</td>
<td>0 (nullification)</td>
</tr>
<tr>
<td>Low</td>
<td>0,5</td>
</tr>
<tr>
<td>Normal</td>
<td>1</td>
</tr>
<tr>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>Critical</td>
<td>4</td>
</tr>
</tbody>
</table>
Due to the fact that the assessment results can be greatly affected by setting aspects that score well to high factors and aspects that do not score well to low factors, great care must be taken. The tool contains a warning not to change the default factor (normal = 1) unless there’s a good reason to do so.

For each subdomain, the scores are calculated and modified using the weighing factors. The results are then shown in the results page for that domain. On the results page, a total score for the domain is also calculated using the average scores in the subdomains.

**Capability Scoring**

Similar to maturity level, formal capability levels as defined by CMMI dictate that advancement throughout these levels is based on meeting prerequisites in the form of predefined goals and practices. Again, a formal implementation of CMMI capability levels would add to the complexity of the tool. Instead, capabilities in this tool are measured as a percentage. If all capabilities are implemented fully, then a 100% score is reached. By providing a 5-point scale for each capability, the organisation is able to granularly define the capability level. For capabilities that are not important to the SOC, an additional option ‘not required’ is implemented to exclude those capabilities from the capability score.

### 4.3.5 Output

The layout and the output of the tool were loosely based on the CREST security incident management self-assessment tool. This tool is more complex than what is intended with the SOC capability maturity tool, but has some features that are also present in the SOC capability maturity tool:

- Scoring based on horizontal bar charts
- Scoring based on radar charts
- Weighing mechanism
- Introduction and usage
- Clear flow throughout the tool by using separate sheets

Figure 20 shows an example score from the ‘aggregated results’ sheet of the CREST tool (from: [http://crest-approved.org/wp-content/uploads/Maturity-Model-example.pdf](http://crest-approved.org/wp-content/uploads/Maturity-Model-example.pdf))
In the output of the artefact, horizontal bar charts (maturity and capability levels) as well as radar charts (maturity levels) and vertical bar charts (capability percentage) are used to visualize the results.

**4.3.6 Alignment**

In the ‘compatibility’ requirement, it was indicated that alignment with a standard framework can provided added value. This alignment was added to the tool by mapping the phases of the NIST Cyber Security Framework to the services and technologies in the artefact. For this mapping, the description from the framework for each of these phases was used and interpreted. Table 5 shows this mapping.
Table 5: Mapping the artefact to NIST Cyber Security Framework

<table>
<thead>
<tr>
<th>NIST phase</th>
<th>Aspect</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Threat Intelligence</td>
<td>Services</td>
</tr>
<tr>
<td>Protect</td>
<td>Vulnerability Management</td>
<td>Services</td>
</tr>
<tr>
<td>Detect</td>
<td>Security Monitoring</td>
<td>Services</td>
</tr>
<tr>
<td></td>
<td>Security Analysis</td>
<td>Services</td>
</tr>
<tr>
<td></td>
<td>Log Management</td>
<td>Services</td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
<td>Technology</td>
</tr>
<tr>
<td></td>
<td>IDPS</td>
<td>Technology</td>
</tr>
<tr>
<td></td>
<td>Security Analytics</td>
<td>Technology</td>
</tr>
<tr>
<td>Respond</td>
<td>Security Incident Management</td>
<td>Services</td>
</tr>
<tr>
<td>Recover</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

For the ‘Recover’ phase, no mapping could be made. Recovery is outside of the scope of the artefact. This is logical, as SOCs usually do not play an active role in the restoration of systems or accounts. This is performed by system and user management departments outside of the SOC.

4.4 The design artefact: SOC-CMM

At this point in the research, a prototype solution (artefact) has been created and can be evaluated by the participants for usability and functionality. This solution is called the Security Operations Center Capability Maturity Model assessment tool, hereafter referred to as SOC-CMM. The SOC-CMM has the following features:

- Built using Microsoft Excel. This means that the tool does not require any installation, configuration or implementation. It can simply be executed by opening the document in Excel and going through the steps as defined in the introduction sheet.
- A sheet-based workflow that consists of 7 sheets: an introduction sheet that explains the usage of the tool, 5 sheets for the actual assessment (each sheet represents a single domain) and 1 sheet for results presentation.
- Visual presentation of maturity and capability results using horizontal and vertical bar charts and web diagrams.
- 21 aspects that can be evaluated using a drop-down menu that allows for the selection of 1 of 5 answers. In total, there are 161 maturity questions and 189 capability questions.
- Additional questions without scoring that provide guidance on maturity questions
- Importance weighing for each of the maturity questions
- An option to exclude capability features from scoring.
- The option to takes notes in the tool for every domain under evaluation.

The next phase in the research is the actual evaluation of the SOC-CMM. This phase is described in the next chapter: evaluation.
5 Phase III: Evaluation

The third phase of the research methodology applied in this thesis is the ‘evaluation’ phase. In this phase, the SOC-CMM is evaluated using multiple techniques.

5.1 Refined hypotheses

Before evaluation is executed, the first step is to refine the hypothesis. According to Offermann et al., this step is required to create a detailed set of hypotheses. When this set of hypotheses is answered, this ultimately provides an answer to the initial hypotheses created in the first phase of this research. The hypotheses created for this phase of the research are the following:

1. Evaluating Business Drivers, Customers, a SOC charter and Governance aspects of a SOC is sufficient to determine the maturity level for the ‘business’ domain.
2. Evaluating Employees, Roles & Hierarchy, People management, Knowledge management and Training & Education aspects of a SOC is sufficient to determine the maturity level for the ‘people’ domain.
3. Evaluating Management, Operations & Facilities and Reporting aspects of a SOC is sufficient to determine the maturity level for the ‘process’ domain.
4. Evaluating SIEM, IDPS and Security Analytics tools within a SOC for aspects and features is sufficient to determine the capability and maturity level for the ‘technology’ domain.
5. Evaluating Security Monitoring, Security Incident Management, Security Analysis, Threat Intelligence, Vulnerability Management and Log Management services within a SOC for aspects and features is sufficient to determine the capability and maturity level for the ‘services’ domain.
6. Radar graphs and bar charts provide an effective and visually pleasing means of presenting maturity and capability results.
7. A capability maturity self-assessment based on the previously mentioned domains provides a means to determine strengths and weaknesses and help to provide direction into the development of the SOC.
8. A tool based on Excel and using sheets as a workflow mechanism provides an easy to use and easy to learn method for assessing capability maturity in the SOC.
10. A capability maturity self-assessment based on predefined selection boxes provides an effective means of determining the capability maturity level for elements under inspection.

These hypotheses are tested using three different techniques: expert survey, case study / action research and laboratory experiment.

5.2 Expert survey

In the initial presentations provided to the potential participants, the intended solution (a self-assessment tool based on a model for measuring capability maturity in a SOC) was presented and discussed. Within these groups, the viability of such a hypothetical solution was discussed (see paragraph 3.4).

This expert survey is similar, except for the fact that it focuses on the actual artefact created in the previous phase of the research. The SOC-CMM was discussed with a single participating organisation.
The SOC-CMM was presented with the focus on the workflow of the document itself, the domains, the aspects within those domains and the visualisation of the results in a single overview. From this discussion, it was decided that the SOC-CMM was likely a viable means for capability maturity self-assessment.

### 5.3 Case study / action research

An initial try-out was conducted with a small group of experts from a single participating organisation in the banking sector. The goal of this try-out was to determine the appropriateness of the toolkit. In this initial try-out, a single domain was evaluated in detail, while others were scanned briefly. With this setup, hypothesis 2 (people domain assessment) as well as hypotheses 6 (visualisation), 7 (appropriateness) and 8 (usability) were evaluated.

The outcome from this initial try-out was that the SOC-CMM provides a viable means of measuring capability maturity in the SOC. Additionally, it was found that discussions about the aspects that are evaluated provide valuable insights for the SOC. Some remarks were made regarding the layout of the tool and specific features of services and technologies (mostly based on practical experience). These changes were implemented into the tool and verified within the organisation. This confirms the statement by Offermann et al. that, due to “the nature of action research, iterations back to “design artefact” or “identify problem” are relevant’ [19].

### 5.4 Laboratory experiment

With the initial try-out completed, a more extensive laboratory experiment can be conducted. For this laboratory experiment, a selection was made of 5 participants that all operated in different sectors and had different maturity levels, perceived or measured. Thus, the applicability and added value for a multitude of organisations is tested. It must be noted that this diversity can also be a complicating factor in the interpretation of the results of the experiment. However, given the fact that SOCs are very diverse in nature, diversity in the selected participants is important to create a group of participants that is representative of a much larger group.

The experiment was set up to simulate the intended purpose of the SOC-CMM: a full self-assessment without guidance. Thus, there was no central or supervised ‘lab’ used in this research. Instead, the SOC-CMM was sent to all participants via mail without any further explanation. An option was provided to make contact via email or phone in case of compatibility issues or other problems with the usage or interpretation of the tool. This option was not used by any of the participants. To guide the participants in the execution of the assessment using the SOC-CMM, an introduction was added to the SOC-CMM that explains how the tool should be used. This approach is aligned with the ‘Controlled experiment’ approach as described by Hevner et al. (see paragraph 2.1.2). The SOC-CMM is used in a controlled fashion with the focus being on usability, accuracy and appropriateness.

An evaluation form was created to obtain the results from the experiment in a standardised fashion and to test the refined hypotheses. The initial hypothesis is answered indirectly because the answers to the refined hypotheses culminate in an answer for the initial hypothesis. Appendix C shows the evaluation form that was used in this research. Table 6 shows the mapping between the questions and the refined hypotheses.
Table 6: Mapping evaluation questions to refined hypotheses

<table>
<thead>
<tr>
<th>Refined hypotheses number</th>
<th>Question in the evaluation form</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sheet 2 (business), questions 1 and 2 &lt;br&gt;Sheet 7 (results), questions 3 and 4</td>
</tr>
<tr>
<td>2</td>
<td>Sheet 3 (people), questions 1 and 2 &lt;br&gt;Sheet 7 (results), questions 3 and 4</td>
</tr>
<tr>
<td>3</td>
<td>Sheet 4 (process), questions 1 and 2 &lt;br&gt;Sheet 7 (results), questions 3 and 4</td>
</tr>
<tr>
<td>4</td>
<td>Sheet 5 (technology), questions 1 and 2 &lt;br&gt;Sheet 7 (results), questions 3 and 4</td>
</tr>
<tr>
<td>5</td>
<td>Sheet 6 (services), questions 1 and 2 &lt;br&gt;Sheet 7 (results), questions 3 and 4</td>
</tr>
<tr>
<td>6</td>
<td>General, question 1</td>
</tr>
<tr>
<td>7</td>
<td>Sheet 7 (results), questions 1 and 2 &lt;br&gt;General, questions 4, 5 and 6</td>
</tr>
<tr>
<td>8</td>
<td>Sheet 1 (introduction), questions 1 and 2 &lt;br&gt;General, question 2</td>
</tr>
<tr>
<td>9</td>
<td>General, questions 3</td>
</tr>
<tr>
<td>10</td>
<td>General, questions 2, 4, 5 and 6</td>
</tr>
</tbody>
</table>

A period of 1 month was provided to each of the participants to return the evaluation form. This period is shorter than the amount of time provided for the survey. This is due to the limited number of participants in this part of the research, and the time period (which was not a holiday period). The returned forms revealed some shortcomings in the tool. In general, it can be stated that:

- Most participants indicated that the tool was mostly complete in terms of the criteria (aspects) being evaluated and the sub-criteria used to evaluate those aspects. The exception to this rule was the completeness of the ‘technology’ domain. Several recommendations were made to improve this domain.
- Most participants indicated that visualisation was perceived as good or very good.
- Most participants indicated that the tool was fairly accurate in determining the maturity level for the SOC aspects. The results were mostly in line with expectations. There was one exception to this rule: one participant indicated a large deviation from expectations (based on a previous measurement of the SOC by a consulting party) and the results from the SOC-CMM. After deliberation, it was clear that the deviation was mostly due to incorrect usage of the tool.
- Multiple participants indicated that the weighing mechanism was confusing. Adjusting the weighing had different results than expected. The suggestion was made to create a version without weighing. Weighing can have added value, but is not a self-explanatory feature and should be used with care. Thus, additional guidance needed to be created for using this feature.
- Most participants indicated that the self-explanatory aspect of the SOC-CMM was good, with the exception of the weighing feature and the exception of one participant (as discussed in the third bullet).
- Multiple participants indicated that not all techniques and services may be part of the SOC. A scope selection feature is required. While the SOC-CMM did accommodate such a
selection, this was not clear from the introduction. Thus, the requirements ‘ease of use’
was not fulfilled on this particular item.

Some individual comments were also made, for example regarding the relative nature of the
questions that is difficult to answer without having a formal baseline. Another example is to add
more remarks to the tool to guide the answer selection process. A final example is remark regarding
the addition of a target maturity level so that SOCs can perform the assessment against a predefined
goal. Setting such a target maturity level may be complicated by the fact that the maturity model is a
continuous maturity model, thus there are multiple ways to achieve a set maturity level (for
example, by performing outstanding on execution of an aspect while not having any formal
documentation).

The feedback from the participants was used to further refine the tool. The changes were noted in a
changelog and distributed among the participants in the lab research, so they could map their results
from the try-out version to the finalised version of the tool. The changes made to the SOC-CMM
were the following:

- 2 questions were added to the tool
- 3 questions were removed from the tool
- Bugs such as numbering mistakes, spelling mistakes, calculation mistakes, etc. were fixed
- The original introduction sheet was divided into 2 sheets: introduction and usage. The
  usage of the tool, as well as the model and scoring mechanisms are explained in more
detail. Additionally, the visual model as represented by Figure 18 is included into the tool.
- 3 more sheets were added. 2 of these sheets concern the setup of the tool: a ‘profile’ sheet
  that allows for setting the target maturity level and filling in some basic information about
  the assessment and a ‘scope’ sheet that allows for selection of services and technologies to
  be included into the tool. Finally, a sheet named ‘Next Steps’ was added that briefly
  explains how to proceed from assessment to improvement.
- Colouring was added to the sheets to further differentiate the different steps the tool.
- Selection boxes were set to be empty by default. This allows for easier progress tracking.

Finally, a second laboratory experiment round was conducted with a single participant to validate the
effectiveness changes that were made to the SOC-CMM. With the tool completed, the last phase of
the research method can be executed. This phase is described in the next chapter: summarise
results.
6 Phase IV: Summarise results

The final phase of the research methodology as outlined by Offermann et al. is the summarise results phase. In this phase, the results are summarised and published. With this thesis being the publication, the results are briefly summarised in this chapter.

This research has yielded some intermediate and some final results. The intermediate result is the outcome of the survey conducted amongst the participants. The results were subsequently used as input into the ‘Design artefact’ activity of the research. Another intermediate result is the maturity assessment model as depicted in Figure 18. By combining the detailed output from the survey with the high-level assessment model, a Microsoft Excel-based assessment tool (the SOC-CMM) was created that satisfies the requirements as outlined in paragraph 4.3.2.

The SOC-CMM was then put through several rounds of testing, with the most extensive test being the ‘laboratory experiment’, in which several organisations have conducted a self-assessment to determine the several aspects of the SOC-CMM, such as appropriateness, accuracy, usability and ultimately the suitability as a tool for self-assessment of capability and maturity levels within the SOC.

With the testing completed, conclusions can be drawn as to the suitability of the SOC-CMM. These conclusions are presented in the next chapter and discussed in the final chapter.
7 Conclusion

In this chapter, the conclusions that can be drawn from the results

7.1 Requirements evaluation

In paragraph 4.2.3.2, the requirements for the SOC-CMM are outlined. In this paragraph, the resulting SOC-CMM is evaluated for matching these requirements. Only the requirements that were not covered by Microsoft Excel itself are evaluated, as the other requirements are met implicitly.

Functional suitability

Appropriateness. The appropriateness of the SOC-CMM was tested in both the case study and the laboratory experiment. The outcome from both experiments was positive. This is supported by the answers provided by the laboratory experiment participants regarding the completeness of the aspects inquired upon in the domains.

Accuracy. The accuracy of the SOC-CMM was tested in the laboratory experiment. In the evaluation form, questions were asked regarding the match between the actual results and the expected results. In general, this match was accurate. One deviation could be explained by incorrect use of the tool. It must be noted that the expected result for most participants was not based on an actual previous measurement, but on expectations based on experience.

Reliability

Fault tolerance. The SOC-CMM was made fault tolerant by using drop-down menus to choose answers instead of having free-format answers. By only performing calculations on input fields with these limitations, faults in calculations resulting in wrong results can be avoided. One of the features that is lacking is the inability to indicate that certain questions have not been filled in. An incomplete assessment yields a lower score. To counter this, the assessment was modified to have all drop-downs that need to be filled in start out empty. This enables progress tracking and allows for quick visual determination of any questions that have been accidentally skipped. It is not possible to set a drop-down menu back to empty manually after a selection was made.

Operability

Appropriateness recognisability. This requirement is covered by the ‘introduction’ and ‘usage’ sheets of the SOC-CMM. These sheets provide sufficient information about the tool and the intended use and audience of the tool. Additionally, the ‘scope’ sheet allows for a quick overview of services and technologies that are evaluated. If none of these are present in the SOC under evaluation, this tool is not appropriate.

Learnability. As indicated in the requirements previously, learnability is supported by the introduction and usage sheets. Additionally, the requirement is supported by using a workflow of Excel tabs from left to right. Lastly, remarks are added to many questions to further increase learnability and reduce ambiguousness of questions.

Ease of use. Ease of use for the SOC-CMM is supported by providing the tool in a familiar environment (Microsoft Excel) and using dropdowns for selection of answers. There are no technical skills required to perform the assessment.
**Attractiveness.** Attractiveness applies to the tool in general and to the results specifically, as these are meant to be used as a means of communication to upper management. The attractiveness of the tool was increased by using a colour scheme in the sheets (different shades of blue), coloured tabs to indicate groups of tabs, pre-defined alignment and sizing of elements and by hiding unused rows and columns. Lastly, column and row headers / numbering were also removed to provide a clean user experience.

**Compatibility**

Interoperability. Interoperability was selected as a ‘could have’ requirement. Technical interoperability is much more important, but is done implicitly by the Microsoft Excel tool. No platform-specific features were used to increase technical interoperability. Additionally, output interoperability was also implemented by aligning the output from the tool to the NIST Cyber Security Framework. Figure 22 shows an example for the NIST section of the results sheet.

![Figure 22: NIST Cyber Security Framework compatibility visualisation](image)

The results from the SOC-CMM can be aggregated with other NIST Cyber Security Framework evaluations to form a more complete picture. Alternatively, the results can be compared to an existing NIST assessment.

**Maintainability**

Modularity. Modularity was addressed in the initial version of the SOC-CMM by the ability to exclude certain services from assessment by setting the relevance of the service to ‘none’. While this was added as a remark to this part of the assessment, in practice it turned out to be counter-intuitive. Thus, the final version of the SOC-CMM implements modularity by first allowing the participant to determine the assessment scope in a separate part of the tool.

Changeability. Changeability was added to the list of requirements as a ‘could have’ requirement. While the initial plan was to make it possible to quickly add elements to the assessment, the scoring and weighing models as well as the calculations being executed to determine the results make this a difficult task. Thus, the changeability requirement was not implemented in the SOC-CMM.

To summarize, Table 7 shows the outcome of the SOC-CMM requirements evaluation.
### Table 7: SOC-CMM requirements outcome

<table>
<thead>
<tr>
<th>Requirement group</th>
<th>Requirements</th>
<th>Importance</th>
<th>Requirement met (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Suitability</td>
<td>Appropriateness</td>
<td>Must have</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Accuracy</td>
<td>Must have</td>
<td>Yes</td>
</tr>
<tr>
<td>Reliability</td>
<td>Fault tolerance</td>
<td>Could have</td>
<td>Yes</td>
</tr>
<tr>
<td>Operability</td>
<td>Appropriateness recognisability</td>
<td>Must have</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Learnability</td>
<td>Must have</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Ease of Use</td>
<td>Must have</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Attractiveness</td>
<td>Should have</td>
<td>Yes</td>
</tr>
<tr>
<td>Compatibility</td>
<td>Interoperability</td>
<td>Could have</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintainability</td>
<td>Modularity</td>
<td>Should have</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Changeability</td>
<td>Could have</td>
<td>No</td>
</tr>
</tbody>
</table>

The table shows that only the ‘changeability’ requirement is not met. This requirement is a ‘Could have’ requirements and can therefore be considered optional.

### 7.2 Refined hypotheses evaluation

From the previous paragraph, it is clear that the SOC-CMM meets all relevant requirements. Besides testing these requirements, the lab experiment was mainly aimed at determining if the refined hypotheses can either be supported or rejected. This paragraph evaluates the refined hypotheses.

1. **Evaluating Business Drivers, Customers, a SOC charter and Governance aspects of a SOC is sufficient to determine the maturity level for the ‘business’ domain.**

   This hypothesis is supported. All participants indicate that the business domain is sufficiently covered, although minor improvements were suggested and implemented.

2. **Evaluating Employees, Roles & Hierarchy, People management, Knowledge management and Training & Education aspects of a SOC is sufficient to determine the maturity level for the ‘people’ domain.**

   This hypothesis is supported. All participants indicate that the people domain is sufficiently covered, although minor improvements were suggested and implemented.

3. **Evaluating Management, Operations & Facilities and Reporting aspects of a SOC is sufficient to determine the maturity level for the ‘process’ domain.**

   This hypothesis is supported. All participants indicate that the process domain is sufficiently covered, although minor improvements were suggested and implemented. Additionally, the division between services and processes was not clear to all participants. This was explained by indicating that processes in the context of the SOC-CMM are general processes, and services are specific processes.
4. Evaluating SIEM, IDPS and Security Analytics tools within a SOC for aspects and features is sufficient to determine the capability and maturity level for the ‘technology’ domain.

This hypothesis is supported. All participants indicate that the technology domain is sufficiently covered, although some improvements were suggested and implemented. These improvements mainly involved adding, changing or further elaborating on features or capabilities.

5. Evaluating Security Monitoring, Security Incident Management, Security Analysis, Threat Intelligence, Vulnerability Management and Log Management services within a SOC for aspects and features is sufficient to determine the capability and maturity level for the ‘services’ domain.

This hypothesis is supported. All participants indicate that the services domain is sufficiently covered, although some minor improvements were suggested and implemented. It was indicated by some participants that they only had one or two services from the list of services. Thus, the assessment was ‘too’ complete for these participants. The final version of the SOC-CMM allows for scope selection and clear visualisation of services that were placed out-of-scope, thus allowing for a more transparent and easy usage of the tool.

6. Radar graphs and bar charts provide an effective and visually pleasing means of presenting maturity and capability results.

This hypothesis is supported. Most participants indicated that the visual aspect of the tool was ‘good’ or even ‘very good’. Accuracy of the results also plays a role, as deviant results are also not visually pleasing.

7. A capability maturity self-assessment based on the previously mentioned domains provides a means to determine strengths and weaknesses and help to provide direction into the development of the SOC.

This hypothesis is mostly supported. However, it must be noted that this does require a post-assessment evaluation. The results show the overall score for each of the domains, and also how the aspects of those domains are scored. However, to determine why the score is higher or lower for a single aspect, it is required to do an evaluation of the questions underlying the aspect. In short, the assessment itself is capable of determining high-level strengths and weaknesses, but a closer look on the aspects is required to determine the cause of higher or lower scores and thus to determine the next steps that need to be taken on the road to improvement.

8. A tool based on Excel and using sheets as a workflow mechanism provides an easy to use and easy to learn method for assessing capability maturity in the SOC.

This hypothesis is supported. While the initial release was not fully satisfactory regarding ease of use, the final release has addressed the issues by proving a page to determine the
scope for the assessment. The weighing mechanism was also not fully clear and was removed from the services and replaced by ‘in’ or ‘out’ of scope. Additionally, a warning was placed in the usage sheet that changing the weighing of elements should only be done when there was a well-founded reason to deviate from the standard weighing factor.


This hypothesis is **mostly supported**. Most participants indicated that a significant time investment was required to perform the assessment. Pre-defined selection boxes decrease the time spent on performing the assessment. However, due to the sheer size of the assessment, it still requires a lot of time to complete. It must be noted that participants did indicate that the time spent on the assessment was valuable. This was mostly due to discussions about aspects of the SOC-CMM to determine the appropriate maturity or capability level.

10. A capability maturity self-assessment based on predefined selection boxes provides an effective means of determining the capability maturity level for elements under inspection.

This hypothesis is **mostly supported**. Most participants indicated that the results from the SOC-CMM assessment matched their expectations accurately, thus proving the effectiveness. However, it was stated by some participants that selecting the correct answer can be difficult. Most questions are answered on a scale from ‘no’ to ‘fully’. Especially the option ‘averagely’ raised some questions. These answers indicate a form of comparison. In order to accurately compare the current situation to what could be considered ‘fully’ or ‘optimally’, some benchmark is required. Creating such a benchmark is possible, but requires a big data set where each of the aspect is investigated at different maturity levels for different SOCs. While the survey did inquire about perceived maturity levels and features of a service or technology, this does not provide sufficient detail. Acquiring such a data set is outside of the scope of this research. The lack of a baseline decreases the effectiveness of the SOC-CMM.

Now that the refined hypotheses have been discussed, the central hypothesis can be evaluated.

### 7.3 Central hypothesis evaluation

In paragraph 3.4, the following central hypothesis was posed:

> “The creation of a self-assessment tool for SOCs can help gain insight in- and control over their capability maturity level”

With the refined hypotheses all supported (albeit mostly in some cases), the central hypothesis should be implicitly supported as well. For this hypothesis to be supported, the aspects ‘insight in [...] their capability maturity level’ and ‘control over their capability maturity level’ must be adequately addressed.
‘Insight in [...] their capability maturity level’ is provided by the SOC-CMM, as it is an accurate and functionally suitable tool based on existing technology that is easy to use and easy to learn (and therefore suitable as a self-assessment tool). Strengths and weaknesses of the SOC are accurately identified and visualised in a detailed overview.

‘Control over their capability maturity level’ is provided by using the detailed results from the assessment to create a plan. This is not done by the SOC-CMM itself, but rather by the organisation performing the assessment. The SOC-CMM provides a means for guidance as well as monitoring. Guidance is provided by identifying the areas that require improvement, monitoring is provided by comparing the output of two subsequent capability maturity assessments.

Thus, the SOC-CMM created in this research supports the central hypothesis.

7.4 Final conclusion
In this chapter, the requirements for the SOC-CMM were evaluated. It was found that most requirements were met, with the exception of one optional requirement. Additionally, in this chapter the central hypothesis and the refined hypotheses were evaluated and fully or at least mostly supported. Thus, it becomes possible to answer the research question posed in paragraph 2.3: “How can the performance and improvement of a Security Operations Center be measured?”.

The answer to the research question is:

“By creating a self-assessment tool to determine strengths and weaknesses of the SOC based on capability and maturity levels, and using the output of this tool to determine next steps for improvement. Improvement can be tracked by regular self-assessment.”

With the research question answered, the hypotheses supported and the requirements satisfied, this research can be concluded.
8 Discussion
This final chapter provides a discussion of several elements in the research. Firstly, the research methodology is discussed. Secondly, the research participants are briefly discussed. Thirdly, the research results are discussed. Finally, potential directions for future research are presented.

8.1 Research methodology
The SOC-CMM was created using a design science approach. This paragraph discusses the application of that approach.

8.1.1 Application of design requirements
In paragraph 2.1.3, the design requirements as stated by Becker et al. are outlined. These requirements have been applied in this research and are discussed one by one.

R1: Comparison with existing maturity models
This requirement is an interpretation of guidelines 1 (Design as an Artefact) and 4 (Research Contributions) set by Hevner et al. It is argued that it is important that the artefact that is being created (in this case the self-assessment tool based on a maturity model) must be compared to existing models. There are no concrete artefacts such as the artefact created in this thesis for comparison. However, it is possible to compare the intermediate artefact (the assessment model) to existing models. The most likely candidates for comparison are the models presented by Schinagl et al. and Kowtha et al. Comparison to commercial models would be useful, but these models are proprietary and cannot be freely accessed.

Compared to the model presented by Schinagl et al., the SOC-CMM model uses different domains. There is a partial overlap, mainly with the technology and services domain from the SOC-CMM. This applies mainly to the areas ‘continuous monitoring’ and ‘intelligence’ from the Schinagl model. The areas ‘Business damage control’ has only a partial overlap in ‘forensic investigations’ and ‘response plans. The area ‘secure service development’ has no overlap with the SOC-CMM. This difference can be explained because of the fact that only a few participants in the research indicated that these activities were part of the SOC. In most cases, the activities were done by a department outside of the SOC.

Compared to the model presented by Kowtha et al., there is significant overlap with the activities model. However, the model by Kowtha et al. is aimed at characterising SOCs, not measuring maturity or capability.

From this brief comparison, it is clear that the SOC-CMM fills a gap in the research towards SOC maturity and capability.

R2: Iterative Procedure and R3: Evaluation
These requirements are an interpretation of Hevner guidelines 3 (Design Evaluation) and 6 (Design as a Search Process). Becker et al indicate that the solution must be “iteratively proposed, refined, evaluated and, if necessary, enhanced” [17]. Chapter 6 describes the evaluation process which was used in this thesis. The evaluation was performed in several iterations, and the output from each of those evaluations was used to further improve the artefact. Thus, these requirements are satisfied.
R4: Multi-methodological procedure
This requirement is an interpretation of Hevner guideline 5 (Research Rigor). Becker et al. indicate that using a variety of research methods yields the best results. In this thesis, the artefact was created using expert interviews (through workshops), literature study, survey and evaluation using different methods. With this combination of these different methods, this requirement is satisfied.

R5: Identification of Problem Relevance and R6: Problem Definition
These requirements are an interpretation of Hevner guideline 2 (Problem Relevance) and is an essential part of the research: the artefact must solve a relevant problem. The establishment of the problem relevancy was done in several ways:
- Using literature study by showing that a research gap exists in the area of SOC capability and maturity (see paragraph 1.2)
- Using expert interviews to confirm that this is indeed a relevant problem in which organisations are interested in (see paragraph 3.3). The willingness of participants to contribute to this thesis is also an important indicator.
- Using freely available information on the number of maturity assessments being carried out by a single commercial company (see paragraph 3.4)

The problem definition itself is presented in paragraph 1.3.

R7: Targeted Presentation of Results and R8: Scientific Documentation
The last 2 requirements set by Becker et al. are an interpretation of Hevner guideline 7 (Communication of Results). These requirements have 2 elements:
- Presentation of results is a requirement regarding the functional appropriateness and the recognisability of that appropriateness by the organisations using the SOC-CMM. This requirement was addressed as part of the SQuaRE attribute profile and evaluated in the laboratory experiment. The results from the experiment were used to confirm the hypothesis.
- Documentation. Becker et al. indicate the relevance of describing the creation of the model by describing all steps that were taken and the methods that were applied. This thesis provides the scientific documentation for the SOC-CMM.

8.1.2 Action research
Basic Design Research does not go beyond the phases of identification, building and evaluation. When an Action Research (AR) component is added to DR (as described by Livari), then reflection and generalisation for purposes of refinement can be applied. In this research, multiple iterations of evaluation have been done to optimize the artefact. In total, there have been 3 rounds of evaluation. The first round was performed with a single participant to test the applicability of the tool to an organisation and additionally test the effectiveness of the tool. The second round was performed with a larger group of participants to determine applicability in a more diverse group of participants. Feedback from both rounds is used to improve the SOC-CMM and make it applicable for all SOCs. The last round was performed with a single participant to validate the optimisations.

These iterations can be considered part of an AR approach in sequence to the DR work performed in this research. However, it could also be argued that this is quite simply iterative evaluation as part of
DR. Lastly, it could be argued that the approach used has similarities to Action Design Research (ADR) as described by Sein et al. [93] where the iterative evaluation in larger groups can be considered part of guided emergence (principle 6 of Sein et al.) and generalisation (principle 7 of Sein et al.). However, since ADR is focussed on designing and building an artefact for a specific organisation, this methodology does not apply here.

As stated in the start of this chapter, this research is based on a DR approach. There are some elements that could be considered AR elements. However, there is no formal use of AR methodology in this research. Thus, the iterative evaluation and reflection should be considered part of the Evaluation phase of the DR methodology by Offermann et al. that is applied in this research.

8.1.3 Design theories
This research revolved around the creation of an IT artefact: the capability maturity measurement tool. This tool was created as a completely new artefact using literature studies, surveys and evaluation. It is possible that a different approach (such as the adaption of an existing tool or model) could have been more effective. Alternatively, a DR approach followed by AR (as described by Livari) could have been a better match than the current DR with iterative evaluation approach. In their paper “The Design Theory Nexus” [94], Pries-Heje and Baskerville opt for an approach in which different design theories are used to obtain an optimal result. While this approach does require more effort in the beginning of the research, the end result (artefact) could be created more efficiently and likely has a better scientific foundation. In retrospect, it is difficult to determine which approach would have yielded the best result given the amount of time available for this research. An approach in which expert interviews are used to quickly determine different design theories could have been a better starting point.

8.1.4 Research phases and steps
In this thesis, the work by Offermann et al. was used to outline the research process. During the course of the research, other similar methodologies were identified. For example, Peffer et al. [95] and the findings of Gregor and Jones [96] describe somewhat different steps from the work by Offermann et al. However, these methodologies are similar in general: the same phases at least are present. Additionally, the research by Mettler [97] that focusses on design science and maturity models presents a view based on 4 steps in the research (Define scope, Design model, Evaluate design, Reflect evolution). This view can easily be aligned with Offermann et al., where ‘define scope’ is addressed in the first phase, ‘define model’ in the second phase and both ‘evaluate design’ and ‘reflect evolution’ and the third phase. Because of the fact that the methodology of Offermann et al provides a very detailed approach, mapping and thus alignment with man other more high level approaches can be done easily. Thus, the chosen methodology is deemed both flexible and appropriate for this kind of research.

8.2 Research participants
This section briefly discusses the participants that have made contributions to the research.

8.2.1 Critical infrastructure
All the participants to the research are organisations that are part of critical infrastructure. Critical infrastructure is described as infrastructures “which affect all areas of daily life, include electric power, natural gas and petroleum production and distribution, telecommunications (information and
communications), transportation, water supply, banking and finance, emergency and government services, agriculture, and other fundamental systems and services that are critical to the security, economic prosperity, and social well-being of the nation.” [98]. It makes sense that organisations that are considered to be part of the critical infrastructure have a SOC capability (internal or outsourced). It is possible that SOCs outside of the critical infrastructure have a different setup than SOCs that are part of the critical infrastructure. However, no information could be found that indicates that this would be true. Thus, it is expected that the results from this research can be generalised to also apply to SOCs outside of the critical infrastructure.

8.2.2 Sample size
The laboratory experiment was carried out with a group of 5 participants that had different maturity levels to test the added value of the SOC-CMM at different maturity levels. It must be noted that in the work by Offermann et al., it is indicated that ‘sample sizes are considerable’. For this research, the sample size is not considerable. This has to do with the limited number of participants in the initial part of the research (the survey) and the fact that some of these participants were not candidates for inclusion into the laboratory experiment due to the nature of their SOC. Thus, the pool of potential participants was not very big. The time investment required for performing the assessment as part of the research process (knowing that this was not a final version) was another threshold for organisations to participate in this part of the research. Lastly, the size of the survey performed earlier in the research had a negative impact on the willingness of organisation to keep participating in the research. The sample size does not need to be a problem. Research by Nielsen and Landauer regarding usability engineering uses sample sizes of 3 groups of 5 participants, each being able to test 85% of usability problems [99, 100]. In this case, only a single group of 5 participants was used; this accounts for 85% of usability problems. It must be noted that other insights exists on this topic [101].

Also, the laboratory experiment was conducted in two rounds. The first round was done with the entire group of 5 participants. The second round was performed with a single participant to validate that the changes made to the tool resolved (most of) the issues. Individual evaluation of the final version with all participants or even multiple iterations of the tool would have been better. This is also described by Hevner [16] and Livari [21]. Again, restrictions regarding willingness and time made this impossible. Further research with larger sample sizes is recommended.

8.3 Research results
This section discusses the research results.

8.3.1 SOC maturity
The SOC-CMM is designed to provide added value to SOCs at all capability maturity levels. The laboratory experiment has verified that the SOC-CMM does provide added value at different maturity levels. However, most added value is perceived in SOCs where the gap between the current maturity level and the target maturity level is the biggest. Because of the fact that the SOC-CMM measures different aspects across different domains, individual aspects that need to be improved can be identified and prioritised.

An organisation that has a maturity level that is relatively close to the target maturity level may perceive little added value in terms of the ‘next steps’ that need to be taken. Even then, the
assessment can still have added value as ‘proof’ for operating on a certain maturity level, although it must be noted that for actual proof it would be better to have an independent party supervise the assessment process. Additionally, the assessment can serve as a checklist for and can also be used to have discussions about the activities within the SOC.

8.3.2 Results accuracy

The results accuracy was questioned by a participant in the laboratory. Because of the fact that the maturity model is a continuous model, inaccurate choices can be made in the detailed questions, while still getting an accurate result for the entire aspect. This behaviour is in the nature of the independent scoring that was implemented in the tool, consistent with AHP.

Presently, the correct answer depends on the knowledge of the person performing the assessment. The person first determines the optimal (fully) level for the question. Then, the current situation is compared to that optimal level to determine the right score. Thus, it is possible that results from assessments differ when executed at different times:

- Due to the fact that the SOC has evolved (legitimate difference)
- Due to the fact the advances have been made by the industry (legitimate difference)
- Due to the fact that the person performing the assessment has become more knowledgeable (illegitimate difference)

To counteract this potential inaccuracy, 2 important recommendations can be made:

1. Make notes as to why a certain score was chosen. This is not viable to do for all elements, but should at least be done for those elements that were most difficult to score. The amount of time spent on discussion is an important indicator (see next point)
2. Perform the assessment with a group of experts. The best understanding of what the ‘optimal’ level is for each of the questions comes from performing the assessment with a group of people. This also encourages discussion about certain aspects and may lead to valuable insights. This ‘side effect’ was also established in the laboratory experiment.

For getting truly accurate results, a formal baseline is required that describes all activities at different maturity levels. This allows for more informed decision as to the right answer to choose. As argued previously, the creation of such a baseline is outside of the scope of this research. Follow-up research could be done to establish a baseline that is independent of organisations and sectors.

8.3.3 SOC scope

As indicated by Schinagl et al., each SOC is unique. This means that the creation of any standard tool is very difficult: some elements may not be applicable to the SOC and some elements may be so unique that there is no literature or other SOC that is using that element. Thus, the element is not measured by default. Therefore, a general tool such as the SOC-CMM is unlikely to cover all activities of the SOC.

Thus, the added value of the assessment differs per SOC environment. In a larger organisation, where security functions are divided across different departments, the added value of a SOC capability maturity measurement in the strict sense can have limited added value in the services and technology domains. However, it must be noted that even though a security function is not formally part of the SOC, it can still be evaluated in the SOC-CMM. In this case, the assessment would be of a
‘virtual SOC’, comprising the actual SOC and a department that performs the specific security function.

### 8.3.4 Results comparison

Because of the fact that the tool is an instantiation of a continuous capability maturity model and the added fact that there is no dependency between elements under evaluation, it is possible that detailed items underlying an aspect change between evaluations, but that the overall result remains the same. Thus, it would seem that there was no change in the setup of the SOC based on the results, while in actuality, things have changed.

Consider the following example. The people management aspect consists of 7 detailed criteria. Table 8 shows these criteria.

<table>
<thead>
<tr>
<th>3</th>
<th>People Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Do you have a job rotation plan in place?</td>
</tr>
<tr>
<td>3.2</td>
<td>Do you have a career progression process in place?</td>
</tr>
<tr>
<td>3.3</td>
<td>Do you have team diversity goals?</td>
</tr>
<tr>
<td>3.4</td>
<td>Do you perform a periodic evaluation of SOC employees?</td>
</tr>
<tr>
<td>3.5</td>
<td>Do you have a 'new hire' process in place?</td>
</tr>
<tr>
<td>3.6</td>
<td>Do you measure employee satisfaction for improving the SOC?</td>
</tr>
<tr>
<td>3.7</td>
<td>Do you perform regular teambuilding exercises?</td>
</tr>
</tbody>
</table>

In the first assessment, team diversity goals may not be present yet, while team building exercises are carried out regularly. Thus, the score on this criterion decreases the overall aspect score. In the second assessment, team diversity goals may be present, but team building exercises may not have been executed (for whatever reason). Thus, the score for 3.3 increases while the score for 3.7 decreases. In such a case, the overall result for the aspect may be the same. This may be interpreted as a lack of change for this aspect, which is incorrect. Thus, a more detailed comparison is required in which all the elements can be individually compared. This would require a separate tool that is outside of the scope of the research.

### 8.4 Further research

In this chapter, some remarks have been made regarding further research. For example, further research can focus on the creation of a comparison tool to compare results from different assessments. But most importantly, further research can focus on the creation of a baseline for the assessments. This baseline would be the standard against which to measure and evaluate, thus providing a more accurate means of assessment. The creation of such a baseline could also be used to guide the transformation from the current continuous capability maturity model to a staged maturity model, which is more common in enterprise environments. A staged maturity model allows for alignment to existing maturity models such as CMMI. It must be noted that a staged maturity model is much harder to implement as a self-assessment. Thus, an external expert is likely required to perform the assessment.

---

**SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers**

© Copyright 2016, Rob van Os

Page 59 of 74
Also, additional research can focus on SOC operational performance. A mature and capable SOC can still operate inefficiently. This research has not focussed on these elements of performance. However, since the SOC is in essence an operational security unit, operational metrics regarding quantity (efficiency and effectiveness) and quality could be applied to determine how well the SOC is performing. Research could be done to determine and implement appropriate metrics. For example, the work by Savola [102] could be used as a starting point.

Lastly, additional research can focus on combining certain actors or threats with specific capabilities. Not all threats and actors are relevant for SOCs. By differentiating which threats can best be detected or mitigated by which capabilities, it becomes possible to create a truly risk-driven targeted profile that can be applied to measure the SOC. Documents such as the Cyber Security Assessment Netherlands (Dutch: Cyber Security Beeld Nederland, CSBN [103]) can be used to determine the risk profile for an organisation. The CSBN describes threats and resilience for sectors in the Netherlands.

For example, consider an organisation in which the main business driver for the SOC is the protection of Intellectual Property (IP). Depending on the sector in which the SOC is operating, the IP may be of interest to other countries. Thus, state actors could be the adversaries for this SOC. Because of the funding that state actors have, vulnerability management will likely be less effective against these attackers, as they are able to create their own zero-day attacks (attacks that exploit previously unknown vulnerabilities). It is also unlikely that such actors will be known in public threat intelligence sources. Lastly, the mode of operations for such actors will be to avoid detection at all costs to maximize the likelihood of obtaining IP. Standard security monitoring use cases will likely not have much effect. Thus, the focus of the SOC should be on detection of anomalies in the network, therefore making capabilities like subtle event detection very important. Also, data exfiltration detection is an important capability. Technologies and services that should be included in the profile for this SOC are SIEM, Security Analytics, Security Monitoring and Security Analysis. Threat Intelligence should be included, although the added value is debatable. By using this specific risk-based profile, the ability of the SOC to detect and respond to high-risk business threats can be assessed.

It must be noted that by focusing too much on specific SOC capabilities (which is basically a form of specialization), there is a risk of decreasing effectiveness in other areas. Thus, this should be evaluated with care. Because there is likely overlap between these profiles, it should be relatively easy to measure multiple profiles in a single assessment and determine the ability of the SOC to react to each of those threats.
9  A final word

With the completion of this thesis, a period of 4 years of intensive studying comes to an end. I started the Master Programme on Information Security in the fall of 2012, not knowing exactly what to expect from the distance education system or from the programme itself. Through its flexibility, the programme has enabled me to do all the studying in my own tempo and my own time. This has helped me in getting the most out of every subject and course. In retrospect, I would not have wanted to do it in any other way.

I would like to take this opportunity to express my gratitude to the following persons and organisations: Maung K. Sein. Thank you for your supervision and insightful comments that have guided me in the process of creating this thesis. I was unsure whether the creation of the SOC-CMM was at all possible with so limited scientific literature on the topic. You have guided me in the right direction.

All participants to this research. Naturally, none of this would have been possible without the willingness of the participants in this study. This willingness was heavily put to the test with the extensive survey. Still, the response rate was excellent. Thank you all for your participation and support in this research.

The participants to the laboratory experiment in particular. 5 organisations have taken the time and effort to test the SOC-CMM in their own SOC and share their findings to help improve the SOC-CMM and to obtain the best result possible. Thank you for your continued support.

And last but not least: my wife and family. These last 4 years have put a strain on me as well as my family. They have supported me throughout the entire journey. This would not have been possible without that support, so thank you very much for your patience and understanding. I will spend the next 4 years making up for everything.
Annex A: Literature study outcome

The following tables represent the outcome of the literature study on SOCs. For each domain, the number of times a particular normalised element was mentioned in the examined literature.

Table 9: Literature study outcome for the SOC people domain

<table>
<thead>
<tr>
<th>Role</th>
<th>Number of times mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Engineer</td>
<td>22</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>22</td>
</tr>
<tr>
<td>SOC Manager</td>
<td>17</td>
</tr>
<tr>
<td>Threat Analyst</td>
<td>17</td>
</tr>
<tr>
<td>Team leader</td>
<td>8</td>
</tr>
<tr>
<td>Security Architect</td>
<td>4</td>
</tr>
<tr>
<td>Security Incident Handler</td>
<td>4</td>
</tr>
<tr>
<td>Data Analyst</td>
<td>2</td>
</tr>
<tr>
<td>Security Specialist</td>
<td>2</td>
</tr>
<tr>
<td>Security Incident Manager</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Table 10: Literature study outcome for the SOC process domain

<table>
<thead>
<tr>
<th>Process</th>
<th>Number of times mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident Management</td>
<td>118</td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>90</td>
</tr>
<tr>
<td>Security Operations</td>
<td>59</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>40</td>
</tr>
<tr>
<td>Security Tooling Management</td>
<td>35</td>
</tr>
<tr>
<td>Security Reporting</td>
<td>29</td>
</tr>
<tr>
<td>Threat Management</td>
<td>24</td>
</tr>
<tr>
<td>Security Management</td>
<td>24</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>22</td>
</tr>
<tr>
<td>Policy &amp; Compliance Management</td>
<td>18</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>17</td>
</tr>
<tr>
<td>People Management</td>
<td>16</td>
</tr>
<tr>
<td>Forensics</td>
<td>16</td>
</tr>
<tr>
<td>Risk Management</td>
<td>15</td>
</tr>
<tr>
<td>Security Analysis</td>
<td>12</td>
</tr>
<tr>
<td>Log Management</td>
<td>12</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>12</td>
</tr>
<tr>
<td>IAM</td>
<td>11</td>
</tr>
<tr>
<td>Malware Analysis</td>
<td>11</td>
</tr>
<tr>
<td>Compliance Monitoring</td>
<td>10</td>
</tr>
<tr>
<td>Awareness &amp; Training</td>
<td>9</td>
</tr>
<tr>
<td>Patch Management</td>
<td>7</td>
</tr>
<tr>
<td>Technology</td>
<td>Number of times mentioned</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>BCM</td>
<td>7</td>
</tr>
<tr>
<td>Security Advisories &amp; Consulting</td>
<td>6</td>
</tr>
<tr>
<td>Fraud Management</td>
<td>3</td>
</tr>
<tr>
<td>Offensive Security</td>
<td>2</td>
</tr>
<tr>
<td>Public Relations</td>
<td>1</td>
</tr>
<tr>
<td>Strategic Security Advice</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>641</strong></td>
</tr>
</tbody>
</table>

Table 11: Literature study outcome for the SOC technology domain

<table>
<thead>
<tr>
<th>Technology</th>
<th>Number of times mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIEM Tooling</td>
<td>21</td>
</tr>
<tr>
<td>Security Analytics Tooling</td>
<td>20</td>
</tr>
<tr>
<td>IDPS Tooling</td>
<td>17</td>
</tr>
<tr>
<td>Log Management Tooling</td>
<td>8</td>
</tr>
<tr>
<td>Vulnerability Management Tooling</td>
<td>7</td>
</tr>
<tr>
<td>Reporting Tooling</td>
<td>5</td>
</tr>
<tr>
<td>Network Security Tooling</td>
<td>5</td>
</tr>
<tr>
<td>Physical Technology</td>
<td>4</td>
</tr>
<tr>
<td>Threat Intelligence Tooling</td>
<td>3</td>
</tr>
<tr>
<td>Packet Capture</td>
<td>3</td>
</tr>
<tr>
<td>Data Leakage Protection Tooling</td>
<td>3</td>
</tr>
<tr>
<td>Forensics Tooling</td>
<td>2</td>
</tr>
<tr>
<td>Ticket Management System</td>
<td>2</td>
</tr>
<tr>
<td>Packet Inspection Tooling</td>
<td>2</td>
</tr>
<tr>
<td>Change Management system</td>
<td>1</td>
</tr>
<tr>
<td>Desktop Management</td>
<td>1</td>
</tr>
<tr>
<td>Contextual Analysis Tooling</td>
<td>1</td>
</tr>
<tr>
<td>Database Security Tooling</td>
<td>1</td>
</tr>
<tr>
<td>Email Security Tooling</td>
<td>1</td>
</tr>
<tr>
<td>Identity Management</td>
<td>1</td>
</tr>
<tr>
<td>Anti-Malware tooling</td>
<td>1</td>
</tr>
<tr>
<td>Integration Tools</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>110</strong></td>
</tr>
</tbody>
</table>

Table 12: Literature study outcome for the SOC business & organisation domain

<table>
<thead>
<tr>
<th>Business / organisation aspect</th>
<th>Number of times mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>22</td>
</tr>
<tr>
<td>Mission, Vision, Strategy</td>
<td>15</td>
</tr>
<tr>
<td>Business Cases</td>
<td>9</td>
</tr>
<tr>
<td>Scope</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>50</strong></td>
</tr>
</tbody>
</table>
Annex B: Survey Introduction Page

Measuring Maturity in Security Operations Centers
Questionnaire

Introduction
This questionnaire is part of my master thesis research concerning the maturity of Security Operations Centers (SOCs). I am conducting this research as part of the master program Information Security at the Luleå University of Technology (LTU, Sweden). The questionnaire is a product of a literature review on the topic of SOC design and setup.

This questionnaire has 6 sections: a general information section, and 5 sections on the setup of your SOC: organization, business, people, process and technology. The terminology used in this questionnaire is explained in appendix A, references that were used to create this questionnaire can be found in appendix C. The process section is quite extensive, as is the level of detail throughout the questionnaire. This is because the research is not so much on the building blocks of the SOC, but the details of how each building block is set up. The more details your organisation can provide, the more complete the final result will become. For convenience and quick processing, most questions can be filled in using checkboxes, option buttons and dropdown items.

Parts I through IV (7 pages in total) can best be processed by the SOC Manager. Parts V and VI (22 pages in total) can best be processed by a senior SOC employee who has a lot of knowledge of the processes and procedures currently in place in the SOC. This person should be able to fill in these parts fairly quickly using the afore mentioned default options. It is highly recommended to print out appendix A (terminology) so that any unclear terms can quickly be looked up.

Although the results of this study must be made public, the information sent by individual organisations will be anonymised and aggregated. It will not be possible to deduce which organisation provided which results from the final report. Organisations will not be named, details answers to this questionnaire will not be disclosed, although some aggregate values or sectorial differences will be investigated.

For questions or comments or support regarding this questionnaire, please do not hesitate to contact me. Thank you for participating in this research. Your input is greatly appreciated.

With kind regards,
Rob van Os
Annex C: Laboratory experiment evaluation form

Evaluation form for the SOC CMM tool

Sheet 1: Introduction
Q1: Is the introduction sufficiently clear?
A:

Q2: Does the introduction provide sufficient information to perform the self-assessment?
A:

Sheet 2: Business domain
Q1: In your opinion, does the business domain section cover all relevant topics for this domain? If not, please specify what is missing in your opinion
A:

Q2: Are there questions asked that are difficult to interpret or ambiguous? If so, please specify which questions
A:

Sheet 3: People
Q1: In your opinion, does the people domain section cover all relevant topics for this domain? If not, please specify what is missing in your opinion
A:

Q2: Are there questions asked that are difficult to interpret or ambiguous? If so, please specify which questions
A:

Sheet 4: Process
Q1: In your opinion, does the process domain section cover all relevant topics for this domain? If not, please specify what is missing in your opinion
A:

Q2: Are there questions asked that are difficult to interpret or ambiguous? If so, please specify which questions
A:

Sheet 5: Technology
Q1: In your opinion, does the technology domain section cover all relevant topics for this domain? If not, please specify what is missing in your opinion
A:

Q2: Are there questions asked that are difficult to interpret or ambiguous? If so, please specify which questions
A:

Sheet 6: Services
Q1: In your opinion, does the services domain section cover all relevant topics for this domain? If not, please specify what is missing in your opinion
A:

Q2: Are there questions asked that are difficult to interpret or ambiguous? If so, please specify which questions
A:

Sheet 7: Results
Q1: Are the overall results in line with your expectations about SOC maturity?
A:

Q2: Are the overall results in line with your expectations about SOC capability?
A:

Q3: Are the domain maturity results in line with your expectations towards these domains? If not, please specify which domains deviated from your expectations and how (higher or lower)
A:

Q4: Are the domain capability results in line with your expectations towards these domains? If not, please specify which domains deviated from your expectations and how (higher or lower)
A:

General
Q1: In your opinion, how would you grade the visual aspect of the SOC-CMM self-assessment tool? (use: poor, reasonable, good, very good and provide some details to support your answer)
A:

Q2: In your opinion, how would you grade the ‘self-explanatory’ nature of the SOC-CMM self-assessment tool? (use: poor, reasonable, good, very good and provide some details to support your answer)
A:

Q3: In your opinion, how would you grade the time investment required to carry out the self-assessment? Please elaborate
A:

Q4: Has the self-assessment been valuable in determining strengths and weaknesses for the SOC? Please elaborate
A:
Q5: Has the self-assessment provided insight into the next steps that need to be taken to increase SOC maturity? Please elaborate
A:

Q6: Would you consider adopting the SOC-CMM as a standard for regularly assessing the progress of growth in your SOC? Please elaborate
A:

Any additional remarks or comments regarding the SOC-CMM tool (missing features, etc.):
Annex D: List of figures and tables

List of figures
Figure 1: Design Science Research steps, according to Offermann et al. ......................................................... 9
Figure 2: Modified Solution Design phase ...................................................................................................... 10
Figure 3: Design Evaluation Methods from Hevner et al. ................................................................................ 11
Figure 4: Number of elements identified per domain in the literature review .................................................. 18
Figure 5: Capability levels and maturity levels (source: CMMI® for Services, Version 1.3) .............................. 19
Figure 6: SOC sectors ..................................................................................................................................... 25
Figure 7: SOC age - number of years in production ....................................................................................... 26
Figure 8: SOC Maturity - Perceived (estimated or measured) maturity levels .................................................. 26
Figure 9: SOC size - number of monitored assets .......................................................................................... 27
Figure 10: SOC size - staffing (in FTE) ............................................................................................................ 27
Figure 11: SOC scope - reach ....................................................................................................................... 28
Figure 12: SOC process activities - aggregated view ..................................................................................... 29
Figure 13: SOC process activities - criticality of services ............................................................................. 30
Figure 14: SOC tools - tools and SOC roles .................................................................................................. 30
Figure 15: Simplified tooling view ................................................................................................................ 31
Figure 16: SQuaRE quality requirements - standard attribute profile ............................................................ 33
Figure 17: SQuaRE quality requirements - specific attribute profile ............................................................... 33
Figure 18: SOC Capability Maturity Assessment Model .................................................................................. 37
Figure 19: Survey results for security monitoring ........................................................................................ 38
Figure 20: Example output from CREST tool ................................................................................................ 41
Figure 21: Example output from the artefact (services domain) .................................................................... 41
Figure 22: NIST Cyber Security Framework compatibility visualisation ....................................................... 49

List of tables
Table 1: Number of maturity levels vs. number of times encountered ............................................................. 22
Table 2: MoSCoW prioritisation of requirements ............................................................................................ 36
Table 3: Maturity scoring mechanism ........................................................................................................... 39
Table 4: Maturity weighing mechanism ........................................................................................................ 39
Table 5: Mapping the artefact to NIST Cyber Security Framework ............................................................... 42
Table 6: Mapping evaluation questions to refined hypotheses ......................................................................... 45
Table 7: SOC-CMM requirements outcome .................................................................................................. 50
Table 8: People Management aspect ............................................................................................................ 59
Table 9: Literature study outcome for the SOC people domain ................................................................... 62
Table 10: Literature study outcome for the SOC process domain .................................................................. 62
Table 11: Literature study outcome for the SOC technology domain ............................................................ 63
Table 12: Literature study outcome for the SOC business & organisation domain ....................................... 63
Annex E: References


9. Ernst & Young, Security Operations Centers against Cybercrime, October 2013


30 Lehner, F., Zelewski, S., “Kann Wissenschaftstheorie behilflich für die Publikationspraxis sein?”, Wissenschaftstheoretische Fundierung und wissenschaftliche Orientierung der Wirtschaftsinformatik, 2007, pp. 71-120


100 Nielsen, J., “Why You Only Need to Test with 5 Users”, March 2000. Retrieved on 26-09-2016 from:
https://www.nngroup.com/articles/why-you-only-need-to-test-with-5-users/

