
# Assessing Security Operations Centers Using the SOC-CMM

Author: Rob van Os
Date: 2022.06.01
SOC-CMM version: 2.2.x

# Table of contents

# 1 Foreword

The SOC-CMM came into existence as a master's thesis in 2016. After its initial release, it has grown from a thesis product into a mature and complete reference framework and methodology for assessing security operations centers. The SOC-CMM has seen world-wide adoption and is now considered to be a standard for assessing SOC strengths and weaknesses.

Over the years, the SOC-CMM has grown in size and complexity. This is a reflection of security operations centers, as they have grown in size and complexity as well. This also means that the task of performing a SOC-CMM assessment has become more complex. This has led to the release of a licensed & supported version, in addition to the free and unsupported version of the SOC-CMM. In this e-book, as part of the licensing, I explain the usage of the SOC-CMM. Helping you, the reader, to better understand the SOC-CMM and perform more effective assessments.

Because an assessment is more than simply going through a set of questions or comparing a state to a control objective. An assessment is about gaining a deep understanding of the SOC, the coherence between its elements, the identification of strengths and weaknesses and the way they are related. It's about overseeing the whole and determining where the possibilities for improvement are, in which order the improvements should be implemented, and the underlying issues that first need to be resolved. It's about determining the added value of the SOC to the organisation's cyber defense strategy and how it can be further improved. An assessment is seeing the SOC as a whole rather than the sum of its parts. When carried out correctly, assessments are a catalyst for growth and strengthening of your cyber defense.

The goal of the SOC-CMM has always been to empower teams in the journey towards higher maturity and capability. The license & support for the SOC-CMM, and this e-book as part of that, is the next step in helping security teams globally to implement more effective cyber defense, by guiding them in performing the best possible assessments.

With kind regards,
Rob van Os
June 1st, 2022

# 2 Introduction

Welcome to the e-book on assessing security operations centers using the SOC-CMM. In this e-book, guidance on utilising the SOC-CMM to assess a SOC is provided.

## 2.1 Purpose

This e-book provides guidelines and best practices for assessing security operations centers (SOCs) using the SOC-CMM. This document can be used as a reference guide during the assessment and for preparation purposes.

## 2.2 Intended audience

The intended audience of this e-book is:

- Security consultants that perform assessments to guide SOCs along their path to higher maturity and capability;
- Security analysts and engineers who wish to learn more about the broad aspects of security operations;
- SOC managers who wish to understand the SOC-CMM and its application in SOCs;
- SOC architects looking for reference material on SOC design;
- IT Auditors or SOC advisors seeking to understand how to use the SOC-CMM in SOC assessments.

## 2.3 Structure of this e-book

This e-book is structured in 3 sections. Section I (chapters 3 and 4) outlines the background of the SOC-CMM model and explains the basics of assessments and capability maturity levels. Section II (chapter 5 to 9) addresses the actual assessment, from proper preparation to best practices and pointers for each domain and aspect. The section closes with interpretation of results and determining next steps. Section III (chapter 10) covers advanced activities for the SOC-CMM.

## 2.4 License

# Section I

## Modelling & capability maturity levels

# 3 Background

The Security Operations Center Capability Maturity Model (SOC-CMM) is a model and self-assessment tool that can be used by SOCs to determine their capability maturity level. The SOC-CMM was initially created as a master's thesis product and is thus grounded in scientific research. The initial reason for creating the SOC-CMM was the lack of freely available or open-source assessment methodologies to determine capability maturity. Since its original release in 2016, the SOC-CMM has been updated, revised and extended to cover additional SOC topics and follow the latest developments in security operations.

## 3.1 Why perform a capability maturity assessment?

Determining the capability maturity level for a SOC is an important part of the growth path of any SOC as it will outline the strengths and weaknesses for the SOC. This assessment, when compared to a capability maturity target and/or an ambition for the SOC, is the basis for a gap analysis and a roadmap to more mature and capable security operations. In other words, assessments help the organisation to achieve the target operating model for security operations.

A SOC roadmap allows a SOC manager to determine key areas of the SOC to invest in. Recurring SOC assessments can subsequently be used to determine the progress of the SOC over time in terms of capability maturity. This helps SOC managers to prove that the investments into particular areas of the SOC yield the desired results, thereby demonstrating qualitative Return On Investment (ROI). Furthermore, SOCs are intended to be adaptive and responsive to change in the threat landscape. Thus, ongoing self-assessment is important for SOCs.

## 3.2 SOC-CMM model

At the core of the SOC-CMM assessment tool lies the SOC-CMM model. As with any model, the SOC-CMM represents a simplified and standardised view of Security Operations Centers. The model consists of 5 domains and 26 aspects tied to those domains. The SOC-CMM model is shown below (version 2.2).

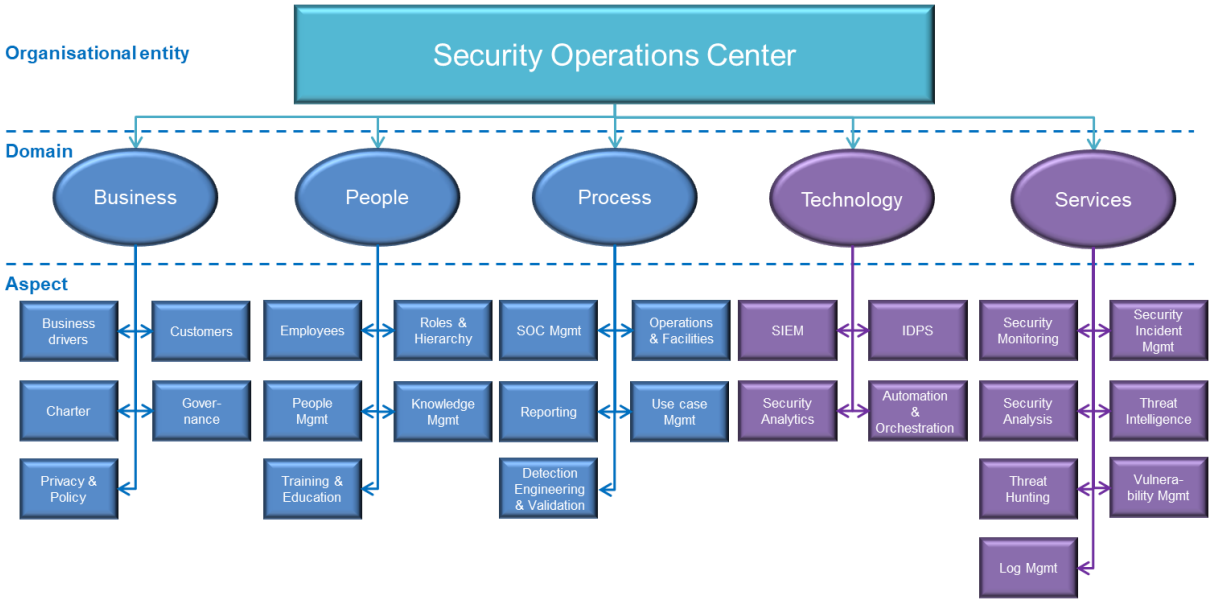


*Figure 1: SOC-CMM model*

In the figure above, 2 colours are used: blue and purple. The blue colour represents domains in which only maturity is measured. These domains (business, people and process) are considered obligatory in the assessment. For the other two domains (technology and services), both maturity and capability are measured. Because individual SOCs differ greatly when it comes to services delivered and technology used to deliver those services, the SOC-CMM has an option to define the assessment scope for these domains. This provides organisations to scope the assessment to the services that their SOC delivers, and the technologies used to support those services. It also enables assessors to perform a scoped assessment, aimed at a particular part of the SOC.

## 3.3 SOC-CMM4CERT

The SOC-CMM4CERT (short: 4CERT) is part of the SOC-CMM assessment suite. The 4CERT was created specifically for incident response teams. Thus, 4CERT uses a somewhat different model from the SOC-CMM. The 4CERT model is shown below.

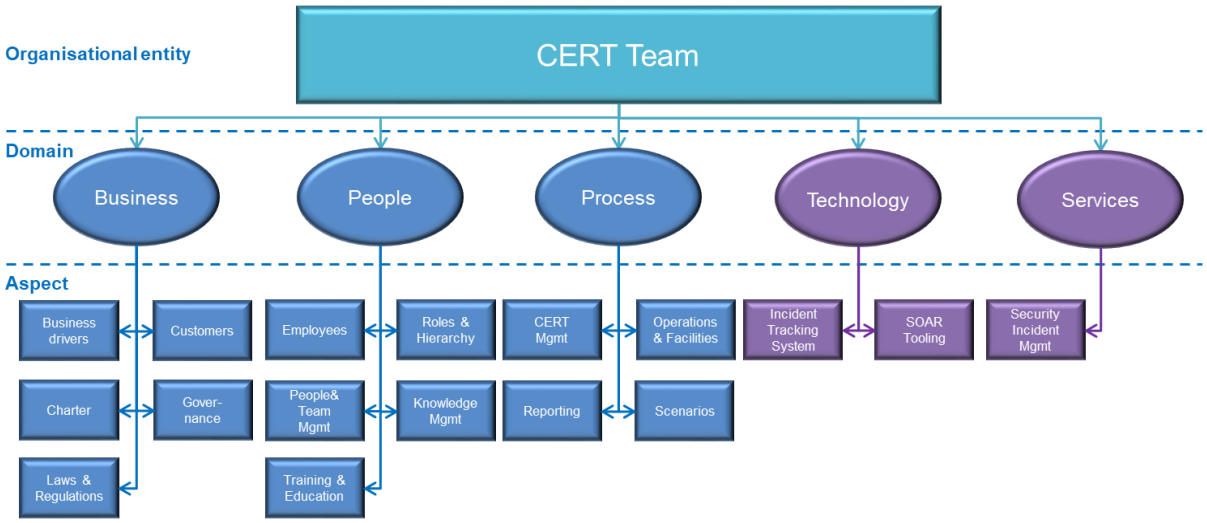


*Figure 2: 4CERT model*

The first 3 domains of the 4CERT model are very similar to the SOC-CMM, with the exception of scenarios rather than use cases in the process domain. The technology and services domains are very different. Where the SOC-CMM has 7 services in total, the 4CERT model only has a single service: security incident management. The technology domain has the two most relevant technologies for a security incident response team: an incident tracking system and Security Orchestration & Automated Response (SOAR), which is also part of the SOC-CMM. Some of the improvements introduced in 4CERT have been adopted in the regular SOC-CMM model as well, to minimise the difference in the first 3 domains. Note that the SOC-CMM4CERT only has an advanced version. The information in chapter 7 is written for the SOC-CMM, and is thus not fully applicable to the SOC-CMM4CERT. Since most elements are the same, chapter 7 should still be reviewed. All other chapters are relevant to both SOC-CMM and SOC-CMM4CERT.

## 3.4 Use cases for the SOC-CMM

The SOC-CMM was developed as a self-explanatory self-assessment tool for determining capability maturity levels in Security Operations Centers. However, there are several other use cases that the SOC-CMM is used:

- As a benchmarking tool to compare different SOCs within an organisation. Or to compare SOCs that work closely together. Note that the gold SOC-CMM license also includes benchmarking.
- To show RoI in SOC improvement. Regular assessment enables an organisation to track to progress of its SOC improvement roadmap. Note that his is not RoI in the financial sense, but rather RoI in the sense of the output of the effort and resources that were put into the improvement program.
- For formal SOC auditing and third-party assessment. While the SOC-CMM was initially designed for self-assessment, third-party assessment can be beneficial for the SOC. This allows external experts, with a more objective view on the SOC, to share their insights. Formal auditing can also be conducted. In this case, the assessment is still conducted by the organisation, but by an organisational entity (the audit department) that functions independent from the SOC. Note that the SOC-CMM is not an auditing framework, such as COBIT. However, the SOC-CMM is aligned with NIST-CSF, which is in turn aligned with COBIT and ISO27k standards.
- As a guideline for implementing a SOC. While the SOC-CMM was not designed as a model to build a SOC (modelling implies simplification), the aspects within the SOC-CMM can be used to create a SOC design, and the questions in the SOC-CMM can be used to shape those aspects in more detail. Although it is not recommended to build a SOC solely based on the SOC-CMM model, the SOC-CMM model can be used to provide guidance.

## 3.5 Licensing & support

The SOC-CMM is published under the CC BY-SA 4.0 license. This means that the SOC-CMM is open source and copy-left. Copy-left means that any derived products must be released under the same license. However, there are support options available for the SOC-CMM. This e-book is part of that support. SOC-CMM versions that are released to those who have purchased support (early access) are not open-source but have a copyright instead. Improvements introduced in the early access versions will ultimately make their way onto the open-source version of the SOC-CMM.

More on SOC-CMM support can be found on the license section of the SOC-CMM website.

## 3.6 Community

The SOC-CMM website includes a forum on which questions can be asked about the SOC-CMM, and discussion on the practical aspects of its application can be held. Bugs and issues can also be posted here. All activity in the area of SOC-CMM development has a separate section. If you wish to make a post on the forum, registration and account activation through a valid email address is required. Note that posts by new accounts will initially be moderated to avoid forum spam or malicious content on the forum.

# 4 Maturity & Capability

The SOC-CMM measures both maturity and capability of the SOC. Maturity is measured across all domains, capability measurement is limited to the technology and services domain and focuses on what the SOC can deliver. In short, capability deals with what the SOC is capable of delivering and maturity deals with how well things are organised. Although related, increasing maturity levels and capability levels can be done separately. Achieving a balance between capability and maturity is important for any SOC to avoid one of the two blocking progress and growth. A highly capable SOC with a low maturity level will ultimately suffer from lack of standardisation, documentation and formal organisational support for their capabilities.

Depending on your type or organisation, maturity and capability can have a different priority. For example, in organisations under formal supervision, maturity is much more important than organisations that do not have such supervision. Often, MSSPs initially focus on building capabilities and initiating service delivery, while maturity of the services and other domains has little focus. At some point, the MSSP will need to correct that discrepancy to achieve the desired balance. Note that there is no right or wrong: it depends on the type of organisation, the SOC goals, organisational culture, sector and, as mentioned, supervisory mechanisms in place.

## 4.1 Maturity levels

Both maturity and capability levels in the SOC-CMM are loosely based on the CMMI framework. The main difference between the CMMI levels and the SOC-CMM levels is that CMMI is much more formal and uses a staged maturity model. The SOC-CMM has no strict maturity levels and growth from one level to another is continuous. This means that it is possible for some elements to function on a lower maturity level and some on higher levels, while giving an adequate average score. For example, the business domain could have element function between level 1 and 2, and elements functioning between 2 and 4, averaging to a score slightly above 2. In CMMI, the maturity level would be set to 1, because not all elements function at level 2. In the SOC-CMM, the average scoring is maintained and elements that score below that average are considered to be candidates for improvement.

Finally, the SOC-CMM has 6 maturity levels (including non-existent) instead of 5. Figure 3 shows the maturity levels of the SOC-CMM.

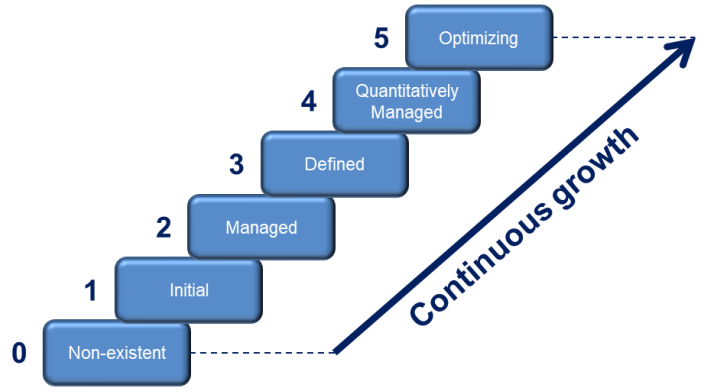


*Figure 3: Maturity levels in the SOC-CMM*

The SOC-CMM maturity levels are defined as follows:

0. **Non-existent**. Non-existing that the aspect under assessment has not been built yet. Most likely, the need for this aspect within the SOC has not yet been recognised by SOC management, or is in its initial building stage.
1. **Initial**. The 'initial' maturity level means that the contours of the aspect under assessment has been established and that the need for the aspect is recognised by SOC management. SOCs acting at the initial maturity level act mostly in an ad-hoc fashion and are characterised for their lack of documentation.
2. **Managed**. Where SOCs acting at the 'initial' maturity level act in an ad-hoc fashion, a SOC at the 'managed' maturity level has applied a basic level of standardisation to achieve a repeatable quality standard in service delivery.
3. **Defined**. The 'defined' maturity level is reached when more extensive documentation is available and used in a consistent fashion. The defined level can serve as an excellent basis for standardisation between aspects to create maturity consistency between aspects and domains.
4. **Quantitatively managed**. A SOC acting at the 'quantitatively managed' maturity level builds further on the standardisation initiated in the defined level and adds regular measurement, evaluation and formalised reporting to the SOC.
5. **Optimizing**. Acting on the 'optimizing' maturity level means that the aspect is subjected to continuous improvement, has been formally documented, approved and is regularly maintained, updated and refined. This maturity level takes significant effort to achieve and maintain.

Note that the maturity levels as described are generic for the SOC-CMM. More specific maturity definitions for specific aspects of the SOC-CMM can be created. For the services domain, service-specific maturity models may exist. For consistency in the assessment, it is recommended to assess the services using the SOC-CMM as well. Service-specific maturity models, such as the threat hunting maturity model [1] can be used for specific purposes. Such maturity model will likely use different maturity definitions and a different number of maturity levels and thus are not compatible with the SOC-CMM.

## 4.2 Capability levels

As indicated, the SOC-CMM is loosely based on the CMMI maturity and capability levels. The SOC-CMM also has 4 capability levels, from 0 to 3. Note that this has an effect on the scoring sheet of the SOC-CMM that may lead to misinterpretation. This is because the results for both maturity and capability are shown in the same spiderweb diagram, while they are actually at a different scale: 0 to 5 (maturity) and 0 to 3 (capability). Figure 4 shows the capability levels used in the SOC-CMM.

[1] Example: A Simple Hunting Maturity Model | Enterprise Detection & Response (detect-respond.blogspot.com)

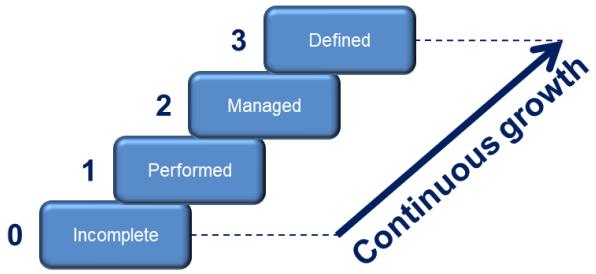


*Figure 4: Capability levels in the SOC-CMM*

The SOC-CMM capability levels are defined as follows:

0. **Incomplete**. This 'incomplete' capability level is reserved for capabilities that have not yet been established, or is in its initial stage of deployment. An incomplete capability will not perform adequately in reducing cyber risks to the organisation.
1. **Performed**. The 'performed' capability level means that this capability is in initial operation. The capability is deployed and operational, but requires additional development to function consistently and in a predictable fashion. A performed capability is not standardised or automated and is performed in an ad-hoc fashion.
2. **Managed**. The 'managed' capability level is reached when standardisation is applied and the capability is fully operational and delivering the desired quality results consistently. When capabilities act at the managed level, they consistently add value to the organisation in reducing cyber risk and are predictable (and therefor reliable) to the organisation.
3. **Defined**. The 'defined' capability level is the highest capability level. This level is reserved for capabilities that are complete in their scope (breadth) and implementation (depth). Capabilities at this level are also continuously optimised, improved and developed further to match trends in security operations.

As with maturity, specific capability models may exist for certain services. These capability models can be used to evaluate the service in more detail, but will not be compatible with the SOC-CMM. It is recommended use these models only when the SOC-CMM provides insufficient insight in particular capabilities and translate the results to the SOC-CMM assessment to provide a consistent overview of the whole SOC in your assessment results.