



Assessing Security Operations Centers Using the SOC-CMM

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

Licensed to support@soc-cmm.com

Copyright © 2022 by SOC-CMM

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior permission of the publisher. This e-book is issued on a personal license.

Table of contents

1	FOREWORD	5
2	INTRODUCTION	6
2.1	PURPOSE	6
2.2	INTENDED AUDIENCE	6
2.3	STRUCTURE OF THIS E-BOOK	6
2.4	LICENSE	6
3	BACKGROUND	8
3.1	WHY PERFORM A CAPABILITY MATURITY ASSESSMENT?	8
3.2	SOC-CMM MODEL	8
3.3	SOC-CMM4CERT	9
3.4	USE CASES FOR THE SOC-CMM	9
3.5	LICENSING & SUPPORT.....	10
3.6	COMMUNITY	10
4	MATURITY & CAPABILITY	11
4.1	MATURITY LEVELS.....	11
4.2	CAPABILITY LEVELS.....	12
5	PREPARING THE ASSESSMENT	15
5.1	CHOOSING THE RIGHT VERSION.....	15
5.2	DETERMINING CAPABILITY MATURITY TARGETS	15
5.3	DETERMINING SCOPE.....	16
5.4	PLANNING & RESOURCES	17
6	ASSESSMENT TYPES AND DATA COLLECTION METHODS	19
6.1	ASSESSMENT TYPES	19
6.2	DATA COLLECTION	19
6.2.1	<i>Organisational culture and data collection</i>	20
6.2.2	<i>Handling evidence</i>	20
6.2.3	<i>Taking notes</i>	20
6.2.4	<i>Avoiding bias</i>	21
6.3	REMOTE ASSESSMENTS	21
7	USING THE TOOL	22
7.1	REMOVING QUESTIONS FROM SCORING.....	22
8	SOC-CMM DOMAINS & ASPECTS	24
8.1	PROFILE	24
8.2	BUSINESS DOMAIN	24
8.2.1	<i>Business drivers</i>	24
8.2.2	<i>Customers</i>	24
8.2.3	<i>Charter</i>	24
8.2.4	<i>Governance</i>	24
8.2.5	<i>Privacy & Policy</i>	25
8.3	PEOPLE DOMAIN.....	25
8.3.1	<i>Employees</i>	25

8.3.2	<i>Roles & hierarchy</i>	25
8.3.3	<i>People management</i>	25
8.3.4	<i>Knowledge management</i>	26
8.3.5	<i>Training and education</i>	26
8.4	PROCESS DOMAIN	26
8.4.1	<i>SOC management</i>	26
8.4.2	<i>Operations & facilities</i>	26
8.4.3	<i>Reporting & communication</i>	26
8.4.4	<i>Use case management</i>	26
8.4.5	<i>Detection engineering & validation</i>	27
8.5	TECHNOLOGY DOMAIN	27
8.5.1	<i>SIEM tooling</i>	28
8.5.2	<i>IDPS tooling</i>	28
8.5.3	<i>Security analytics tooling</i>	28
8.5.4	<i>Automation & orchestration tooling</i>	29
8.5.5	<i>Other technologies</i>	29
8.6	SERVICES DOMAIN	29
8.6.1	<i>Security monitoring</i>	30
8.6.2	<i>Security incident management</i>	30
8.6.3	<i>Security analysis & forensics</i>	31
8.6.4	<i>Threat intelligence</i>	31
8.6.5	<i>Threat hunting</i>	31
8.6.6	<i>Vulnerability management</i>	32
8.6.7	<i>Log management</i>	32
8.6.8	<i>Other services</i>	33
9	RESULTS & NEXT STEPS	34
9.1	SOC-CMM RESULTS SECTION.....	34
9.2	INTERPRETING RESULTS	35
9.3	NEXT STEPS	36
9.4	SHARING RESULTS	36
10	ADVANCED ACTIVITIES	38
10.1	CUSTOMISING THE SOC-CMM	38
10.2	MIGRATING BETWEEN VERSIONS.....	38
10.3	COMPARING ASSESSMENT RESULTS	38
11	FINAL WORD	39
12	ABOUT THE AUTHOR	40

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 SOC's 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 SOC's;
- 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

This e-book is issued on a personal license and is part of SOC-CMM licensing & support. Publication or replication of this material without the explicit consent of the author is prohibited and punishable by law.

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 SOC's 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, SOC's are intended to be adaptive and responsive to change in the threat landscape. Thus, ongoing self-assessment is important for SOC's.

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).

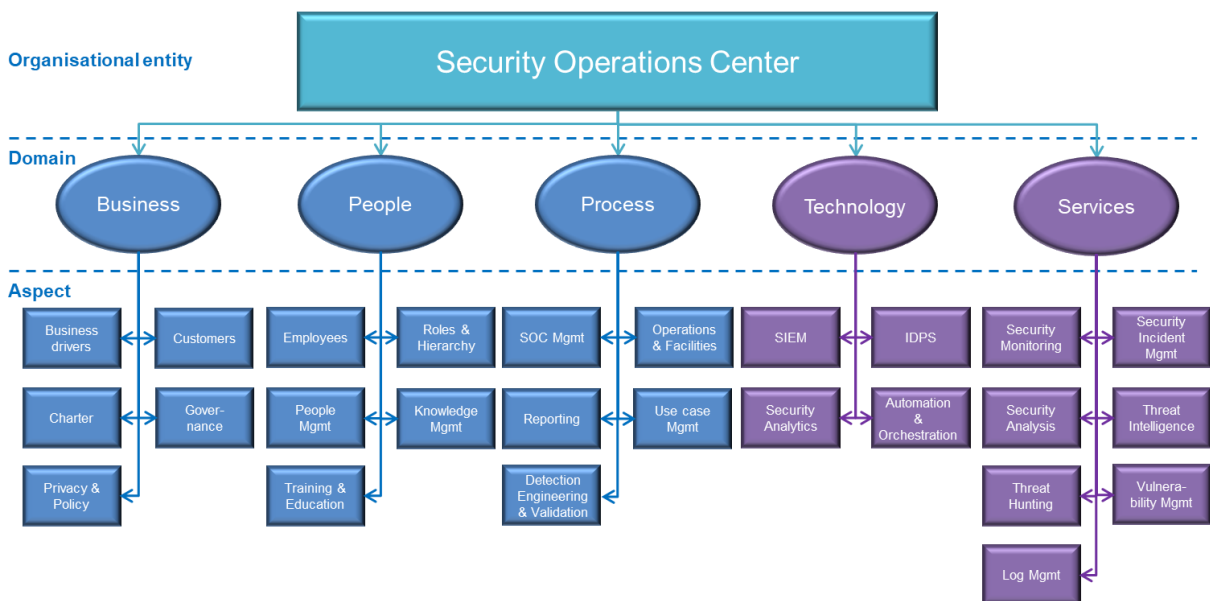


Figure 1: SOC-CMM model

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 SOC's 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.

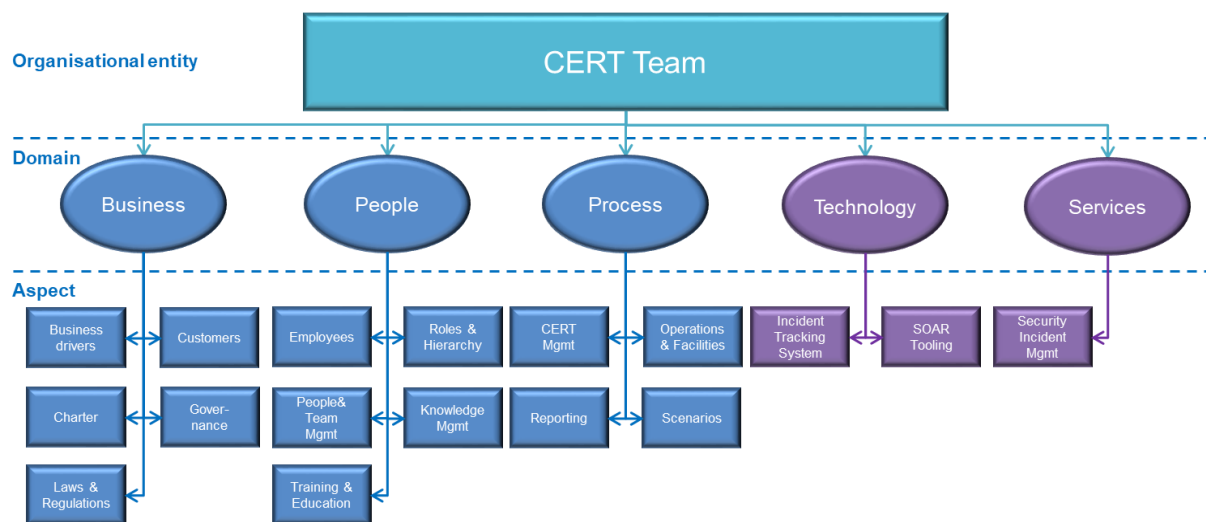


Figure 2: 4CERT model

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 SOC's within an organisation. Or to compare SOC's that work closely together. Note that the gold SOC-CMM license also includes benchmarking.
- To demonstrate RoI in SOC improvement. Regular assessment enables an organisation to track to progress of its SOC improvement roadmap. Note that this 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.