NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Good Practice on assessing the maturity of a Security Operations Center (SOC) using the SOC Maturity Framework (SOC-MF)

Versie 1.2

Januari 2023

Christopher Nield MSc RE CISA CISSP CISM SSCP

Ing. Danny Schmidt MSc RE CISSP CISM

Tom Verharen MSc RE MHA CISA CISSP CDPSE

On behalf of the NOREA Knowledge group Cybersecurity

Good Practice on assessing the maturity of a SOC using the Security Operations Center Maturity Framework (SOC-MF)

This methodological guide has been published by NOREA, the professional organization of IT auditors in the Netherlands and may be used freely with due observance of the disclaimer and license conditions below. For questions and comments, please contact: NOREA, the professional organization of IT auditors PO Box 7984, 1008 AD Amsterdam Telephone: +3120-3010380 E-mail: norea@norea.nl.

More information can be found at: https://www .norea.nl.

Version control

Version	Date	Author	Comments
0.1	07-03-2022	NOREA knowledge group Cybersecurity	Initial version
0.2	10-4-2022	NOREA knowledge group Cybersecurity	Peer review comments
0.3	15-5-2022	NOREA knowledge group Cybersecurity	Professional practices committee NOREA comments (Vaktechnische Commissie)
0.4-0.9	16-5-2022 - 16-6-2022	NOREA knowledge group Cybersecurity	Update based on comments NOREA knowledge group Cybersecurity
1.0	17-6-2022	NOREA knowledge group Cybersecurity	V1.0 for open consultation purposes.
1.1	02-11-2022	NOREA knowledge group Cybersecurity	Feedback from consultation
1.2	09-12-2022	NOREA knowledge group Cybersecurity	Update based on comments from NOREA Professional practices committee (Vaktechnische Commissie)

Distribution

Version	Date	Comments
0.1	07-03-2022	Draft version submitted for peer review within NOREA Knowledge Group Cybersecurity
0.2	15-04-2022	Draft version submitted to NOREA professional practices committee (Vaktechnische Commissie)

1.0	17-6-2022	V1.0 released for consultation purposes
1.1	02-11-2022	Definitive version V1.1 released to NOREA professional practices committee (Vaktechnische Commissie)
1.2	05-01-2023	Definitive version V1.2 released on the NOREA website

Review and approval

Version	**Date**	**Reviewer / approver**
0.2	10-4-2022	NOREA knowledge group Cybersecurity
0.3	15-5-2022	NOREA Professional Practices Committee (Vaktechnische Commissie)
1.0	17-6-2022	Approved by the chair of the NOREA knowledge group Cybersecurity for distribution
1.1	02-11-2022	Approved by the chair of the NOREA knowledge group Cybersecurity for distribution
1.1	02-12-2022	NOREA Professional Practices Committee (Vaktechnische Commissie)

Index

1 Introduction

1.1 Purpose of this document

Structure

This good practice provides guidance to IT Auditors (RE's) and security professionals when auditing or advising on (the maturity of) a Security Operation Center (SOC) with regards to the protection of the enterprise, its partners and customer assets.

The document is organized as follows.

- Chapter 1: provides context on cyber security, the role of a SOC and this publication.
- Chapter 2: provides a theoretical framework on what defines a SOC.
- Chapter 3: describes the SOC-MF.

Context

In today's society, organizations and individuals increasingly communicate via (internet) connected automated systems where well-functioning IT is essential. The importance of and dependence on IT for companies and their customers continues to grow. Technology and information systems play a large role in supporting combatants as well as disrupting operations, critical infrastructure or supply chains. In addition, various (international) hacker groups are involved in cyberwars. A direct result of these factors is the impact of cyber security risks on societal functioning, which highlights the necessity to continue to be on and remain ahead of the curve. Therefore, cyber security needs to be prioritized depending on the organization risk-appetite. Risk-appetite effects the required maturity of the cyber resilience measures and varies per organization.

The UK National Cyber Security Centre (NCSC) defines Cyber security as "how individuals and organizations reduce the risk of cyberattack". Cybersecurity is directly linked to concepts such as cybercrime, data leakage, privacy protection, DDoS, phishing and hacking. In addition, we see that organizational aspects, outsourced responsibilities and human behavior are important in controlling cyber security risks. This is apparent from the increase in legislation and regulation surrounding the information security domain.

The NCSC in the Netherlands describes Cybersecurity as the whole of measures to prevent damage through the disruption, failure or misuse of ICT and, if damage does occur, to restore it. That damage may consist of the impairment of the availability, confidentiality or integrity of information systems and information services and the information stored in them.

Security Operations Center Maturity Framework (SOC-MF)

This framework focuses on the enterprise technical defense. To face and overcome cyber security threats, the deployment of a SOC is nowadays essential for companies. In the past, the initial concept of a SOC was mainly based on the reactive signaling of events. Over the years the SOC has evolved to include response, proactive research and the prevention of activities (MDEC, 2017). Gaining deeper insight into network usage and network operations, providing timely response and being able to provide accurate threat intelligence are the drivers for the continued development and operating effectiveness of a SOC. Considering the aforementioned developments and the role of the IT auditor as a trust provider, Good Practices on assessing SOC effectiveness should be shared. The SOC-MF was built for this purpose, primarily because existing frameworks or standards (i.e. ISO2700x, COBIT, CIS or NIST-CSF) do not support in-depth assessments of SOC operations, alignment and maturity.

The SOC-MF provides a scalable and in-depth framework on assessing SOC maturity and effectiveness to provide detailed insight in growth opportunities and gaps between the desired and assessed maturity.

The framework provides management with insight based on controls, whereby the design, existence and operational effectiveness can be tested. Using their inherent risk an organization can determine the desired state of the maturity of the SOC required for maintaining organization cyber security resilience. The framework provides an overview of the current maturity; based on gaps the organization can prioritize items for the SOC development roadmap. This Good Practice can also be used for IT assurance or specifically agreed on IT engagements.

NOREA and the establishment of this Good Practice

The Dutch Order of Register EDP-Auditors (NOREA) is the professional association for IT auditors in the Netherlands. Our members, IT Auditors, are closely involved with financial statements audits as well as providing assurance, or sometimes advice, regarding Information Technology and Information Systems directly to organizations.

The NOREA has several knowledge groups, such as Privacy, Algorithm & Assurance, Robotic Process Automation and Cybersecurity. The knowledge groups focus their products on audit/assurance professionals, but also target external audiences (such as buyers of IT (audit) services/products, politics, market parties, industry organizations, regulators, employers).

The Security Operation Center Maturity Framework (SOC-MF) was created by the NOREA knowledge group Cybersecurity.

2 Theoretical framework

The following paragraphs provide a high level overview on SOC functions, preconditions on assessing SOC effectiveness and additional in-depth resources.

2.1 Role and function of a SOC

The purpose of this paragraph is to give a broad overview of a SOC – this by definition means it is not exhaustive, nor is it meant to be an in-depth analysis of SOC operating (models). We assume readers to have a general understanding of a SOC's role, capabilities and core tasks.

NIST (2019) declares a SOC to be "*a combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects*".

In essence this means a SOC provides a centralized response on (possible) intrusions in enterprise networks. Majid and Ariffi (2019) expand on this, posing that through continual monitoring a SOC ensures system and information availability, integrity and confidentiality. Zimmerman (2014) and (Knerler et al., 2022b) complements this with SOC core tasks, being:

- Preventing cyber security incidents through:
  - Continual threat analysis;
  - Network and host vulnerability scanning;
  - Coordinated implementation of measures;
  - Security policy and architectural advice;
- Monitoring, detecting and analyzing possible intrusions in real time and using historical trend analysis based on security relevant data sources;
- Reacting on confirmed incidents by coordinating resources and effort on implementing suitable measures in a timely manner;
- Supplying situational awareness and reporting related to cyber security incidents and trends relating to threat actor behavior;
- Developing and applying Computer Network Defense technologies such as IDS's and data collection and analysis systems.

2.2 SOC effectiveness preconditions

Based on an overarching literature review four preconditions relate to SOC effectiveness and should be considered when assessing SOC maturity.

- Precondition 1: an effective SOC focuses on proactive asset protection through a combination of people, process and technology and performs both in a detective and corrective manner. This requires profound technical and network insight, structured processes and the use of advanced technologies.

- Precondition 2: an effective SOC evolves to match with the organizations needs and threat landscape developments. An effective SOC has a deep understanding of attack phases and uses this knowledge to give a proactive response.
- Precondition 3: SOC services should be aligned with Zimmerman's core tasks to be defined as a SOC; however, there is no limitation to the activities a SOC can perform. Therefore SOC services should always be aligned with the organizational strategic objectives, assets and its threat landscape and dictates SOC form and function. The IT landscape encompasses both internal and external IT (including partners and suppliers).
- Precondition 4: SOC effectiveness is influenced by factors outside of the SOC's direct area of influence. Governance alignment, management commitment and the ability and willingness to continually improve the SOC are important in attaining and maintaining SOC effectiveness.

3 Security Operations Center Maturity Framework (SOC-MF)

The following paragraphs describe the SOC CMM, the SOC-MF and considerations on its usage.

3.1 Relationship SOC-MF and SOC CMM

The SOC-MF is based on the SOC CMM (Security Operations Center Capability Maturity Model) by Rob van Os and uses five axis to increase insight in SOC operational capability maturity. The SOC-CMM is not an auditing framework, such as COBIT, but an empirically validated self-assessment tool. However, the SOC-CMM is aligned with NIST-CSF, which is in turn aligned with COBIT and ISO27k standards. SOC-MF and SOC CMM diverge with regards to auditability and objectivity.

3.2 SOC MF structure

SOC MF follows the SOC CMM-structure (domains, aspects, controls) and continues on this by adding control objectives, controls, testing of design and operating effectiveness practices to each aspect. Furthermore, one aspect has been added (outsourcing) to the Technology Domain to manage risks relating to partial or complete SOC outsourcing.

Domain	Aspects	
Business	Business Drivers Customers Charter	Governance Privacy
People	Employees Roles and hierarchy People management	Knowledge management Training and education

Process	SOC management Operations and facilities	Reporting Use case management
Technology	Security Information & Event Management (*SIEM*) Intrusion Detection and Prevention System (IDPS) Outsourcing	Security analytics Automation and orchestration
Services	Security monitoring Security incident management Security analytics Threat intelligence	Threat hunting Vulnerability management Log management

The SOC-MF uses control objectives, controls and quality attributes. The following quality attributes are used:

Quality attributes	Definition
Effectiveness	The extent to which an object is aligned with user demands and goals and whether an object contributes to organizational goals.
Availability	The extent to which business processes and organizational resilience maintained.
Integrity	The extent to which an object (data, IT service or IT tool) is in accordance with the desired design.
Confidentiality	The extent to which exclusively authorized persons or devices can use an object or access an object, using authorized procedures and limited privileges.
Timeliness	The extent to which information is available in a timely manner to contribute to SOC and organizational internal control.

3.3 Considerations in using the SOC-MF

- The SOC-MF can be used in assessing SOC design and operational effectiveness. Depending on the size of the SOC and its expected maturity, the SOC-MF can be too broad or in-depth.
- The SOC-MF needs to be tailored as part of the audit scoping. Not all controls are relevant to all SOC configurations, and some may be more relevant depending on the configuration or operational environment. For instance - if a SOC is partially or completely outsourced, control objectives relating to outsourcing and reporting should be included in the audit scope. Specific organizational context should be considered as well. If (for instance) use-case management is a formal process, it could be beneficial to expand the SOC-MF controls to include this process in full.
- The SOC-MF is a SOC specific, though generalized framework. It does not encompass all possible relevant SOC control objectives. Specific risks or controls should be included if the customer, auditor or auditee has reason to do so.

The SOC-MF does not report on SOC cyber security risk (mitigation). The framework provides insight on whether the SOC performs in a manner as guided by enterprise strategy as well as if relevant preconditions relating to SOC effectiveness are met.

3.4 Maturity scores

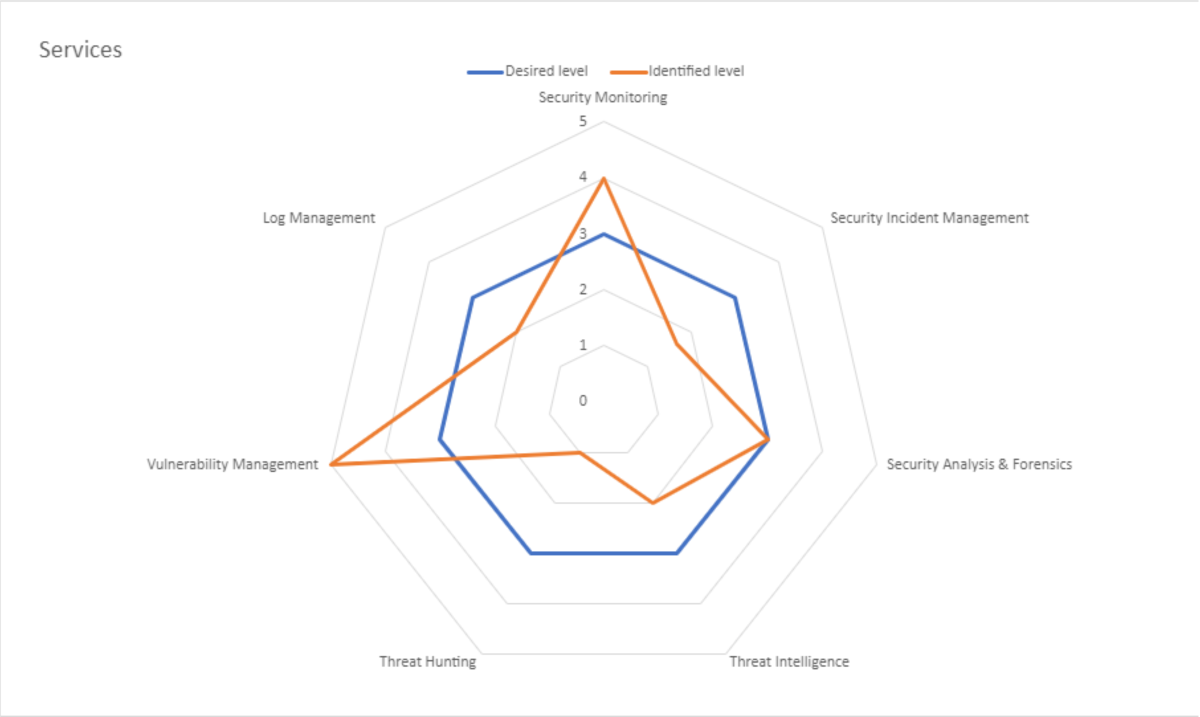
The SOC-MF uses maturity scores to show areas of excellence or possibilities for improvement. To ensure interpretation differences in maturity scores are as limited as possible, the SOC MF uses the COBIT 2019 maturity levels based on CMMI.

Each individual control is scored for its desired and assessed maturity, resulting in a maturity analysis using the following levels:

Incomplete	0
Initial	1
Managed	2
Defined	3
Quantitatively Managed	4
Optimizing	5

Full description of the maturity levels and their requirements are included in Appendix 1. Maturity levels are achieved by fulfilling the requirements per level, including all previous requirements – level 3 cannot be achieved without fulfilling level 2, 1 and 0 requirements etc.

Gaps between the assessed and desired maturity levels indicate areas of possible improvement and are reported on control level as well as aggregated domain-level scores. For instance, the below graphs encompasses both the desired and assessed maturity for the domain 'Services':



Downloading the SOC-MF.

The SOC-MF is contained in a separate Excel-document and contains the full framework. The SOC-MF can be downloaded from the NOREA website.

Citations

Knerler, K., Parker, I. & Zimmerman, C. (2022b). *11 Strategies of a World-Class Cybersecurity Operations Center*. MITRE.

Majid, M. & Ariffi, A. (2019). Success Factors for Cyber security Operation Center (SOC) Establishment. Consulted from doi:10.4108/eai.18-7-2019.2287841 op 20 December 202

Malaysian Digital Economy Corporation (MDEC). (2017). Industry Guidance For Next Generation Managed Security Operating Centre. Consulted from https://mdec.my/media-centre/publications/ op 13 November 202

National Institute of Standards and Technologies. (2018). Framework for Improving Critical Infrastructure Cyber security: Version 1.1. Consulted from https://doi.org/10.6028/NIST.CSWP.04162

Van Os, R.M. (2016). SOC CMM : Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers.

Van Os, R. (2018). SOC CMM Whitepaper: Measuring Capability Maturity in Security Operations Centers.

Van Os, R. (z.j.) SOC CMM. Consulted from https://www.soc-cmm.com/ on 23 November 2022.

Zimmerman, C. (2014). Ten strategies of a world-class cyber security operations center. Consulted from https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf on 23 October 2020.

Appendix 1 Maturity scores SOC MF

Maturity levels are achieved by fulfilling the requirements per level, including all previous requirements. The SOC MF uses the COBIT 2019 maturity levels based on CMMI.

Dutch definition	English definition	Clarification	Level
Niet bestaand – Aan deze beheersingsmaatregel is geen aandacht besteed.	**Incomplete**– No or unknown attention has been given to this control.	N/A	0
Initieel – De beheersingsmaatregel is (gedeeltelijk) gedefinieerd maar wordt op inconsistente wijze uitgevoerd. Er is een grote afhankelijkheid van individuen bij de uitvoering van de beheersingsmaatregel.	**Initial** – The control is (partially) defined but is performed in an inconsistent manner with a large dependency on individuals relating to control execution.	• No or partial control executed • No or partial execution • No or partial documentation • No consistent execution	1
Herhaalbaar maar informeel – De beheersingsmaatregel is aanwezig en wordt op consistente en gestructureerde, maar op informele wijze uitgevoerd.	**Managed**– The control is implemented and performed with consistence and structure on a specific (part of the) process, but informally.	• Control execution is based on an informal but standardized procedure. The execution is not fully documented. • Still issues to resolve and address.	2
Gedefinieerd – De opzet van de beheersingsmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseerde wijze uitgevoerd. De vereiste effectiviteit van de beheersingsmaatregel is aantoonbaar en wordt getoetst.	**Defined** – The design of the control has been documented and is performed with structure and consistency. The required effectiveness of the control is demonstrable and assessed.	The control: • Is defined using risk-based considerations • Documented and formalized • Encompasses clear responsibilities and tasks • Reports on control design and operational effectiveness • Is reported using a risk-based frequency and proves control effectiveness over a longer period of time (>6 months) • Outcomes are reported to management	3
Beheerst en meetbaar – De effectiviteit van de beheersingsmaatregel wordt	**Quantitatively Managed**– The effectiveness of the	• Periodical (control) evaluation and follow-up is performed • Evaluation is documented	4

periodiek geëvalueerd. Daar waar nodig wordt de beheersingsmaatregel verbeterd of vervangen door andere beheersingsmaatregel(en). De evaluatie wordt vastgelegd.	control is periodically evaluated. The control is improved or replaced by other controls as necessary. The evaluation is documented.	• Evaluation responsibilities and tasks are documented • Evaluation frequency has been defined using the organization's threat profile (at least annually) • The evaluation includes operational incidents • Evaluation outcomes are reported to management	
Continu verbeteren – De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering van de effectiviteit van de maatregelen. Hierbij wordt gebruik gemaakt van externe data en benchmarking. Medewerkers zijn proactief betrokken bij de verbetering van de beheersingsmaatregelen	**Optimizing**– Controls are anchored in the integrated risk management framework, and control effectiveness is continually improved, by making use of external data and benchmarks. Employees are proactively involved in control improvement.	• Continual control evaluation to continually increase control effectiveness • Making active use of self-assessment and gap / root cause analyses • Benchmarking implemented controls using external data in comparison to other organizations	**5**