

**Evaluating Security Operations Center (SOC) Capability through Maturity
Level Assessment and Gap Analysis: A Case Study of PT. XYZ**

By
Mariano Joseph Tendean
22451026

MASTER'S DEGREE
in
MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

August 2025
Revision after the Thesis Defence on August 12th 2025

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Mariano Joseph Tendean

Student

Date

Approved by:

Dr. Eka Budiarto, ST, M.Sc

Thesis Advisor

Date

Dr. Charles Lim, BSc., MSc

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium, S.Kom., M.Sc.

Dean of Faculty of Engineering and
Information Technology

Date

ABSTRACT

Evaluating Security Operations Center (SOC) Capability through Maturity Level Assessment and Gap Analysis: A Case Study of PT. XYZ

By

Mariano Joseph Tendean

Dr. Eka Budiarto, ST, M.Sc , Advisor

Dr. Charles Lim, BSc., MSc , Co-Advisor

SWISS GERMAN UNIVERSITY

The increasing intensity and complexity of cyber threats demand a mature and effective Security Operations Center (SOC) to ensure an organization's resilience. This study aims to evaluate the capability maturity level of the SOC at PT. XYZ, a company operating as a Managed Security Service Provider (MSSP). The research adopts a mixed methods approach, combining qualitative data through observations and interviews with quantitative assessments using the Security Operations Center Capability Maturity Model (SOC-CMM).

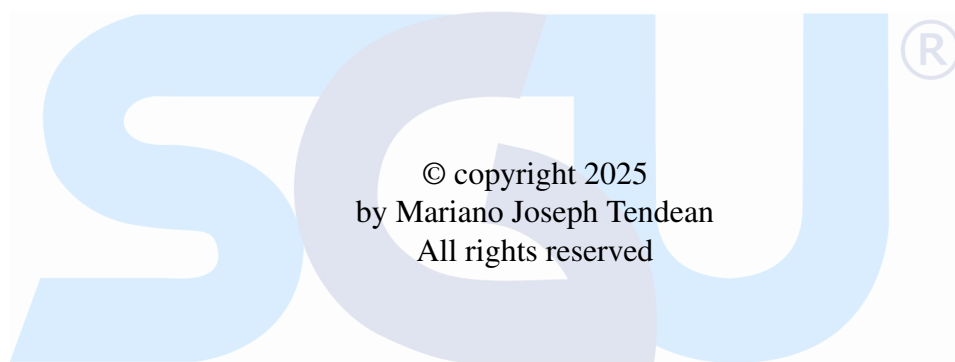
The study follows a structured framework consisting of five stages: literature review, problem identification, capability maturity assessment, gap analysis, and validation. The SOC-CMM tool was used to assess five process domains: SOC Management, Operations & Facilities, Reporting & Communication, Use Case Management, and Detection Engineering & Validation. The results show that the overall maturity level of PT. XYZ's SOC is at 1.87 out of 5, below the targeted level of 3. The largest gaps were identified in SOC Management and Detection Engineering, indicating a need for improvement in strategy, governance, and detection capabilities.

To strengthen these areas, the gap results were mapped to the COBIT 2019 framework to provide governance-aligned recommendations. The study concludes

with strategic recommendations focused on enhancing organizational structure, standardizing processes, developing incident playbooks, and integrating COBIT principles to support long-term SOC development. Validation through experts and internal stakeholders confirmed the accuracy and relevance of the findings. This research contributes to a structured understanding of SOC maturity and offers a practical roadmap for MSSPs seeking capability advancement.



Keywords: Security Operations Center, SOC-CMM, Capability Maturity, Gap Analysis, COBIT 2019, Cybersecurity, MSSP



DEDICATION

I would like to dedicate this research project to my God, my family, my beloved country Indonesia and my second home where I grow in knowledge, PT Alfa Siber Teknologi.



ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Dr. Eka Budiarto, ST, M.Sc and Mr. Dr. Charles Lim, BSc., MSc my thesis advisors, for their dedication, invaluable guidance, support, and encouragement throughout this research and the completion of this thesis. Their contribution has been instrumental in bringing this work to its current stage. I am profoundly grateful to my family, especially my parents, for their endless moral support during my studies at SGU. Your presence, prayers, and unwavering encouragement have meant everything to me. I also wish to thank my direct supervisors, my team at work, and my friends—especially the MIT SGU Class of 34—for their companionship and continuous support. Lastly, I extend my heartfelt appreciation to everyone who has contributed to this research, both directly and indirectly. Your support has truly made a difference.



Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	5
ACKNOWLEDGEMENT	6
TABLE OF CONTENTS	9
LIST OF FIGURES	10
LIST OF TABLES	11
1. INTRODUCTION	12
1.1 Background	12
1.2 Research Problem	14
1.3 Research Objective	16
1.4 Research Question	17
1.5 Hypothesis	17
1.6 Scope and Limitation	17
1.7 Significance of Study	18
1.8 Thesis Structure	19
2. LITERATURE REVIEW	20
2.1 The Role of Cybersecurity Technology Distributors in the Security Ecosystem	20
2.1.1 Distributor Function in Cyber Security	20

2.1.2	Cybersecurity Challenges	21
2.1.2.1	Business Challenges	21
2.1.3	Threat Landscape	22
2.1.4	Privacy and Data Protection	23
2.2	Ecosystem Security Operations Center (SOC)	24
2.2.1	Definition of Modern SOC: Purpose, Evolution, and Critical Urgency	24
2.2.2	Core Functions, Responsibilities, and Operational Model of the SOC	26
2.2.3	SOC Core Capabilities: People, Process, Technology, and Services	33
2.2.4	Factors Affecting the Effectiveness and Performance of SOC . .	35
2.3	Capability Maturity Models (CMM) for Process Improvement	37
2.3.1	Basic Concepts of CMM and Capability Maturity Model Integration (CMMI)	38
2.3.2	Understanding CMM/CMMI Maturity Levels and Their Significance	39
2.3.3	Benefits and Applications of CMM/CMMI in an Organizational Context	42
2.4	Assessing and Improving SOC Capabilities: Maturity Model and Methodology	43
2.4.1	Introduction to the SOC Specific Capability Maturity Model . .	43
2.5	Gap Analysis in the Context of SOC Maturity	45
2.5.1	Gap Analysis Indicators	46
2.5.2	Mapping With COBIT	47
2.6	Designing a Method for Stakeholder Interview Questions	49
2.6.1	Types of Interview Structures	49
2.6.1.1	Interview question method	51
2.6.2	Principles for Developing Interview Questions	52
2.7	Expert Selection Criteria for Validation	55
2.7.1	Mapping Questions to SOC-CMM Process Domain Aspects . .	56
2.8	Related Works	58

3. RESEARCH METHODS	68
3.1 Research Design	68
3.2 Research Framework	69
3.2.1 Literature Review	70
3.2.2 Problem Identification	70
3.2.2.1 Interviews Question Criteria Focus on SOC-CMM	
Proses Domain	71
3.2.3 SOC Capabilities Maturity Model Process Domain	73
3.2.4 SOC Gap Analysis	73
3.2.5 Validation	74
4. RESULTS AND DISCUSSIONS	75
4.1 Problem Identification	75
4.2 SOC Capability Maturity Assessment	76
4.3 Gap Analysis	77
4.3.1 Mapping with COBIT 2019 & Gap Result	78
4.4 Validation	79
4.4.1 Justification for Expert Selection	80
4.4.2 Results of Validation	82
5. CONCLUSIONS AND RECOMMENDATIONS	83
5.1 Conclusions	83
5.2 Recommendations	84
REFERENCES	94
A. Mapping Interview Questions to SOC Roles	95
B. Standard Operating Procedure & Incident Playbook	101

List of Figures

1.1

IBM Cost of Data Breach (Nawale, 2025)

12

1.2

Fishbone Diagram

16

3.1

Research Design (Creswell and Creswell, 2017)

69

3.2

Research Framework

70

A.1

Interview Expert

100



List of Tables

2.1	Comparison of Security Operations Center (SOC) Operational Models .	32
2.2	CMMI Maturity Levels Review (Incremental Representation)	41
2.3	Comparison of Frameworks	44
2.4	SOC-CMM Domains and Key Indicators	47
2.5	Mapping of SOC Gap Areas to COBIT 2019 Goals, Practices, and Activities	48
2.6	Comparison of Interview Types	50
2.7	Comparison of Interview Delivery Methods	53
2.8	Expert Selection Criteria for SOC-CMM Validation	55
2.9	Mapping of SOC-CMM Process Subdomains	57
2.10	Comparison of Related Works	61
3.1	SOC-CMM Process Domain Aspects	72
4.1	SOC-CMM Domain Scores	76
4.2	SOC-CMM Domain Current and Target Levels	77
4.3	SOC-CMM Domain and COBIT 2019 Focus Areas	79
A.1	Interview Questions Mapping	95
A.2	SOC Manager Interview Results	97
A.3	SOC Analyst Interview Results	99
A.4	Security Engineer Interview Results	99