

**DESIGNING SOC MATURITY IMPROVEMENT STRATEGIES BASED ON  
SOC-CMM EVALUATION AND NIST CSF ALIGNMENT: A PT XYZ CASE  
STUDY**

By  
Fildza Amalia Zhafira  
22451017

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

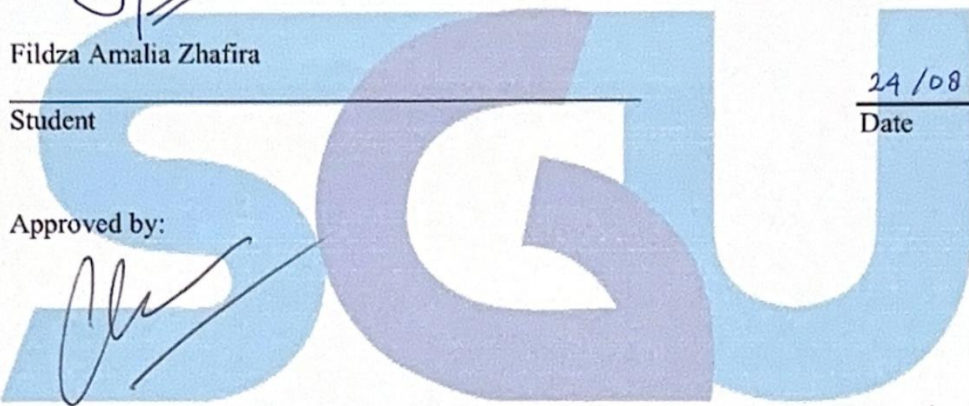


SWISS GERMAN UNIVERSITY  
The Prominence Tower  
Jalan Jalur Sutera Barat No. 15, Alam Sutera  
Tangerang, Banten 15143 - Indonesia

Revision after the Thesis Defense on August 13, 2025

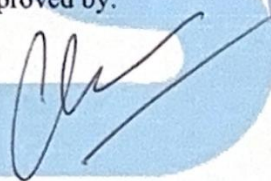
### STATEMENT BY THE AUTHOR

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.

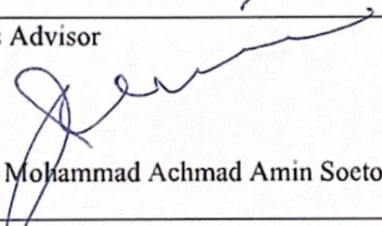


  
Fildza Amalia Zhafira  
\_\_\_\_\_  
Student

24/08/2025  
\_\_\_\_\_  
Date

Approved by:  
  
Dr. Charles Lim, B.Sc., M.Sc  
\_\_\_\_\_  
Thesis Advisor

25/8/25  
\_\_\_\_\_  
Date

  
Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc  
\_\_\_\_\_  
Thesis Co-Advisor

24/08/2025  
\_\_\_\_\_  
Date

Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc  
\_\_\_\_\_  
Dean of Faculty of Engineering and Information Technology

\_\_\_\_\_  
Date

## ABSTRACT

### DESIGNING SOC MATURITY IMPROVEMENT STRATEGIES BASED ON SOC-CMM EVALUATION AND NIST CSF ALIGNMENT: A PT XYZ CASE STUDY

By

Fildza Amalia Zhafira  
Dr. Charles Lim, B.Sc., M.Sc  
Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc

SWISS GERMAN UNIVERSITY

With the growing complexity of cyber threats, the role of the Security Operations Center (SOC) has become increasingly critical in ensuring the protection of enterprise information assets. Despite this importance, many SOC's still encounter challenges such as fragmented processes, lack of resource integration, and insufficient alignment with business strategies. This research explores the current state of SOC maturity at PT XYZ and proposes tailored improvement strategies by leveraging two well-established frameworks: the Security Operations Center Capability Maturity Model (SOC-CMM) and the updated version of the NIST Cybersecurity Framework (CSF 2.0). The study adopts a qualitative approach, involving an in-depth review of internal documents, guided interviews with stakeholders, and feedback sessions to validate the findings. Each domain defined by the SOC-CMM—Business, People, Process, Technology, and Services—was assessed using the Maturity Indicator Level (MIL) criteria. The results were then linked to the five functional pillars of the NIST CSF: Identify, Protect, Detect, Respond, and Recover, enabling a risk-oriented interpretation of the organization's security posture. The analysis reveals that the SOC is positioned between the early and developing stages of maturity, particularly needing improvement in procedural consistency, staff capabilities, and service cohesion. Based on this assessment, the study presents a set of actionable, phased recommendations designed to enhance the SOC's performance and strategic value. These insights offer a replicable framework for organizations aiming to strengthen their cybersecurity operations through globally recognized best practices.

*Keywords: Cybersecurity Maturity, NIST CSF, SOC-CMM, SOC, Risk-Based Assessment*



## DEDICATION

To God Almighty, the constant light on my path, whose blessings, strength, and grace have guided me through every stage of this academic pursuit. With gratitude for this guidance, I extend this dedication to my life partner, whose unwavering support, encouragement, and sacrifices have been my anchor; to my dear friend, for the motivation and kindness that eased the way; and to my parents and sisters, whose love, support, and prayers have been a continuous source of strength.

In the same spirit, this thesis is also dedicated to the pursuit of knowledge and to the academic community that nurtures growth, innovation, and resilience. May it, in its own small way, contribute to advancing research in cybersecurity and to building a safer digital future.



## ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to Dr. Ir. Charles Lim, B.Sc., M.Sc. and Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc. as my thesis advisors, for their invaluable guidance, encouragement, and unwavering support throughout the course of this research. Their patience, wisdom, and constructive feedback have not only shaped this thesis but also enriched my academic and professional journey. It is because of their priceless contributions that this work has reached its completion.

I am profoundly thankful to my life partner, whose constant encouragement, understanding, and presence have been my greatest source of strength. Your unwavering support has carried me through the most challenging moments of this journey, and I could not have reached this milestone without you. To my beloved family, especially my two little sisters, thank you for your endless love, sacrifices, and prayers that have guided me through every step. Your faith in me has been both a comfort and a driving force, reminding me never to give up, even in the most difficult times.

I would also like to express my heartfelt appreciation to my close friend, for being a steady source of motivation, encouragement, and companionship throughout this process. Your presence has made this journey more meaningful and less daunting.

My sincere appreciation also goes to my supervisors, colleagues, and teammates at work, whose insights and encouragement greatly contributed to the progress of this research. To my friends in Batch 34 MIT SGU, thank you for the companionship, laughter, and solidarity that made this path less difficult and more memorable.

Finally, I extend my gratitude to all individuals—whether directly or indirectly—who have supported me in this endeavor. Each word of encouragement, shared knowledge, and gesture of kindness has played a meaningful role in bringing this thesis to fruition.

## TABLE OF CONTENTS

|                                                                               | Page |
|-------------------------------------------------------------------------------|------|
| STATEMENT BY THE AUTHOR.....                                                  | 2    |
| ABSTRACT.....                                                                 | 3    |
| DEDICATION.....                                                               | 5    |
| ACKNOWLEDGEMENTS.....                                                         | 6    |
| TABLE OF CONTENTS.....                                                        | 7    |
| LIST OF FIGURES .....                                                         | 10   |
| LIST OF TABLES.....                                                           | 11   |
| CHAPTER 1 – INTRODUCTION .....                                                | 12   |
| 1.1 Background.....                                                           | 12   |
| 1.2 Research Problem.....                                                     | 14   |
| 1.3 Research Objective.....                                                   | 16   |
| 1.4 Research Question.....                                                    | 16   |
| 1.5 Hypothesis.....                                                           | 16   |
| 1.6 Research Scope and Limitation.....                                        | 17   |
| 1.7 Significance of Study .....                                               | 17   |
| 1.8 Thesis Structure.....                                                     | 18   |
| CHAPTER 2 - LITERATURE REVIEW.....                                            | 19   |
| 2.1 ICT Company Profile .....                                                 | 19   |
| 2.2 The Strategic Importance of SOC in Modern ICT Organizations.....          | 20   |
| 2.3 The Evolving Cyber Threat Landscape .....                                 | 21   |
| 2.3.1 Key Characteristics and Trends in the Current Threat Landscape.....     | 21   |
| 2.3.2 Impact of Cyber Threats on Organizations .....                          | 23   |
| 2.3.3 Implications for Security Operations Centers (SOCs) .....               | 24   |
| 2.4 The Security Operations Center (SOC): Foundations and Core Components ... | 24   |
| 2.4.1 Definition of Security Operation Center .....                           | 24   |
| 2.4.2 Key Components of a SOC .....                                           | 25   |
| 2.4.3 Security Operation Center Operational Model.....                        | 31   |
| 2.4.4 SOC Capabilities and Tools .....                                        | 32   |
| 2.4.5 Key Challenges in Security Operation Center .....                       | 33   |
| 2.5 Critical Success Factors for SOC.....                                     | 34   |
| 2.6 Understanding SOC Maturity.....                                           | 36   |
| 2.7 Frameworks for Cybersecurity and Guiding SOC Maturity .....               | 39   |
| 2.7.1 NIST Cybersecurity Framework (NIST CSF).....                            | 40   |

|                                         |                                                                                     |    |
|-----------------------------------------|-------------------------------------------------------------------------------------|----|
| 2.7.2                                   | COBIT 2019 .....                                                                    | 41 |
| 2.7.3                                   | SOC-CMM .....                                                                       | 42 |
| 2.7.4                                   | C2M2.....                                                                           | 43 |
| 2.7.5                                   | ISO/IEC 27001 .....                                                                 | 44 |
| 2.7.6                                   | ITIL .....                                                                          | 45 |
| 2.7.7                                   | CIS Controls .....                                                                  | 46 |
| 2.7.8                                   | MITRE ATT&CK .....                                                                  | 47 |
| 2.8                                     | Analytical Evaluation of Framework Suitability .....                                | 51 |
| 2.8.1                                   | Maturity and Granularity .....                                                      | 51 |
| 2.8.2                                   | Domain Coverage .....                                                               | 53 |
| 2.8.3                                   | Practical Suitability for the Case Study.....                                       | 54 |
| 2.8.4                                   | Scope of SOC-CMM Domains and Subcategories .....                                    | 55 |
| 2.9                                     | Scoring Method for SOC Maturity Assessment .....                                    | 56 |
| 2.9.1                                   | Maturity Indicator Levels .....                                                     | 56 |
| 2.9.2                                   | Link to Risk-Based Prioritisation .....                                             | 58 |
| 2.10                                    | Designing Effective Interview Questions .....                                       | 58 |
| 2.10.1                                  | Methodological Approach: Rationale for Semi-Structured, Role-Based Interviews ..... | 61 |
| 2.11                                    | Related Work .....                                                                  | 66 |
| CHAPTER 3 – RESEARCH METHODS .....      |                                                                                     | 71 |
| 3.1                                     | Research Design .....                                                               | 71 |
| 3.2                                     | Research Framework .....                                                            | 72 |
| 3.2.1                                   | Literature Review .....                                                             | 74 |
| 3.2.2                                   | Problem Identification .....                                                        | 74 |
| 3.2.3                                   | Maturity Assessment .....                                                           | 75 |
| 3.2.4                                   | Gap Analysis and Risk Identification.....                                           | 76 |
| 3.2.5                                   | Maturity Improvement Roadmap .....                                                  | 77 |
| 3.2.6                                   | Evaluation.....                                                                     | 78 |
| 3.2.7                                   | Validation .....                                                                    | 78 |
| 3.3                                     | Interview Question Structure.....                                                   | 79 |
| 3.4                                     | Reliability and Validity .....                                                      | 81 |
| 3.5                                     | Research Effectiveness Measurement Method.....                                      | 82 |
| 3.5                                     | Critical Success Factors for Roadmap Viability and Adoption.....                    | 83 |
| CHAPTER 4 – RESULT AND DISCUSSION ..... |                                                                                     | 85 |
| 4.1                                     | Problem Identification and Assessment Approach.....                                 | 85 |
| 4.2                                     | Scope of Assessment .....                                                           | 86 |
| 4.3                                     | Maturity Scores from Stakeholder Interviews.....                                    | 87 |
| 4.3.1                                   | Initial Maturity Evaluation Results – Management .....                              | 87 |
| 4.3.2                                   | Initial Maturity Evaluation Results – Manager .....                                 | 90 |
| 4.3.3                                   | Initial Maturity Evaluation Results – Engineer.....                                 | 93 |
| 4.3.4                                   | Initial Maturity Evaluation Results – Solution Architect.....                       | 95 |
| 4.4                                     | Capability Evaluation: Establishing the Foundation for Maturity Improvement .....   | 98 |

|                                                                              |                                                              |     |
|------------------------------------------------------------------------------|--------------------------------------------------------------|-----|
| 4.5                                                                          | Synthesizing the Findings: The Maturity Perception Gap ..... | 101 |
| 4.6                                                                          | Gap Score Analysis .....                                     | 102 |
| 4.7                                                                          | Mapping to NIST CSF Functions and Tier Estimation .....      | 105 |
| 4.8                                                                          | Initial Roadmap of Improvement .....                         | 107 |
| 4.9                                                                          | Evaluation.....                                              | 113 |
| 4.10                                                                         | Validation Expert.....                                       | 114 |
| CHAPTER 5 – CONCLUSION AND RECOMMENDATION .....                              |                                                              | 116 |
| 5.1                                                                          | Conclusion.....                                              | 116 |
| 5.2                                                                          | Recommendations .....                                        | 117 |
| REFERENCES .....                                                             |                                                              | 120 |
| Appendix A Questions for Management at SOC PT. XYZ.....                      |                                                              | 124 |
| Appendix A Result from Interview with Management at PT XYZ SOC .....         |                                                              | 127 |
| Appendix A Questions for Manager at SOC PT. XYZ .....                        |                                                              | 130 |
| Appendix A Result from Interview with Manager at PT XYZ SOC.....             |                                                              | 133 |
| Appendix A Questions for Engineer at SOC PT. XYZ .....                       |                                                              | 136 |
| Appendix A Result from Interview with Engineer at PT XYZ SOC .....           |                                                              | 138 |
| Appendix A Questions for Solution Architect at SOC PT. XYZ .....             |                                                              | 140 |
| Appendix A Result from Interview with Solution Architect at PT XYZ SOC ..... |                                                              | 142 |
| Appendix B Expert Validation.....                                            |                                                              | 144 |
| Appendix C Roadmap 3 Years.....                                              |                                                              | 146 |
| CURRICULUM VITAE – Author.....                                               |                                                              | 151 |

## LIST OF FIGURES

| Figures                                                                             | Page |
|-------------------------------------------------------------------------------------|------|
| Figure 1.1 The SOC's Proactive Lifecycle for Continuous Cyber Defense.....          | 13   |
| Figure 1.2 Fishbone Diagram for Research .....                                      | 15   |
| Figure 3.1 General Method for Research.....                                         | 72   |
| Figure 3.2 Research Framework .....                                                 | 73   |
| Figure 4.1 Chief's Assessment of SOC Maturity Across Five Domains.....              | 88   |
| Figure 4.2 Manager's Assessment of SOC Maturity Across Five Domains .....           | 91   |
| Figure 4.3 Engineer's Assessment of SOC Maturity Across Five Domains.....           | 93   |
| Figure 4.4 Solution Architect's Assessment of SOC Maturity Across Five Domains..... | 96   |
| Figure 4.5 Chart for Gap Between Current and Target. ....                           | 104  |
| Figure 4.6 Spider Web for All Domain Current and Target .....                       | 104  |
| Figure 4.7 Swimlane Chart for Three Years Roadmap.....                              | 109  |

## LIST OF TABLES

| Table                                                              | Page |
|--------------------------------------------------------------------|------|
| Table 1.1 Comparison of Framework .....                            | 49   |
| Table 2.1 SOC-CMM Model (SOC-CMM, 2024).....                       | 56   |
| Table 2. 2 Maturity Scoring .....                                  | 57   |
| Table 2.3 Comparative Type of Interview .....                      | 63   |
| Table 2.4 Comparative of Question Type.....                        | 65   |
| Table 2. 5 Comparison Related Works of SOC Maturity .....          | 68   |
| Table 3.1 Scoring based SOC-CMM .....                              | 75   |
| Table 3.2 Criteria of Expert .....                                 | 79   |
| Table 3.3 Question Structure .....                                 | 80   |
| Table 4.1 Category of Question.....                                | 86   |
| Table 4.2 Avg Domain Score Management.....                         | 88   |
| Table 4.3 Average Domain Score Manager.....                        | 90   |
| Table 4.4 Average Domain Score - Engineer .....                    | 93   |
| Table 4.5 Average Domain Score – Solution Architect.....           | 96   |
| Table 4.6 Capability Level SOC PT. XYZ .....                       | 100  |
| Table 4. 7 Mapping Problem .....                                   | 101  |
| Table 4.8 Gap Score for SOC PT XYZ .....                           | 103  |
| Table 4.9 Mapping SOC-CMM to NIST CSF .....                        | 106  |
| Table 4.10 Mapping Gaps, Risks, and Roadmap Priorities .....       | 112  |
| Table A.1 Question for Management.....                             | 126  |
| Table A.2 Answer of Interview Question for Management.....         | 129  |
| Table A.3 Question for Manager .....                               | 132  |
| Table A.4 Answer of Interview Question for Manager .....           | 135  |
| Table A.5 Question for Engineer .....                              | 137  |
| Table A.6 Answer of Interview Question for Engineer .....          | 139  |
| Table A.7 Question for Solution Architect.....                     | 141  |
| Table A.8 Answer of Interview Question for Solution Architect..... | 143  |
| Table C.1 Table Roadmap for 3 Years .....                          | 146  |