

**DEVELOPING A LEVEL 1 SECURITY OPERATION CENTER ANALYST
COMPETENCY MATRIX (L1 SOC ACM) BY APPLYING MATURITY
APPROACH TO SUPPORT PERFORMANCE EVALUATION : CASE STUDY
ON PT XYZ**

By

Agung Setiaji
22351035

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 05 February, 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.

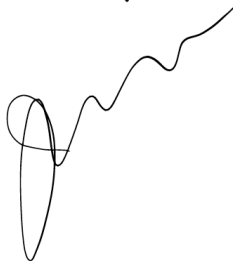


[Agung Setiaji]

Student

Date

Approved by:



[Dr. Ir. Mohammad Achmad Amin Soetomo M.Sc]

Thesis Advisor

Date

[Dr. Ir. Charles Lim BSc., M.Sc]



Thesis Co-Advisor

Date

[Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc]

Dean

Date

ABSTRACT

Developing A Level 1 Security Operation Center Analyst Competency Matrix (L1 SOC ACM) Based on Competency To Support Performance Evaluation : Case Study on PT XYZ

By

Agung Setiaji

Dr. Ir. Mohammad Achmad Amin Soetomo M.Sc, Advisor

Dr. Ir. Charles Lim BSc., M.Sc, Co-Advisor

SWISS GERMAN UNIVERSITY

The complex and dynamic nature of a SOC work environment necessitates that SOC analysts deliver optimal performance. To facilitate this, it is essential to implement a competency evaluation process focused on performance that aligns with the specific conditions of the SOC analyst's workplace. This research aims to develop a framework called L1 SOC Analyst Competency Matrix (L1 SOC ACM) for assessing the competency of L1 SOC Analyst in supporting the performance evaluation. This framework apply a maturity assessment approach that is assessed based on the level of capability in four dimensions of competence, namely professional competencies, personal competencies, social competencies and methodological competencies. In addition, weighting is applied to each competency to produce the level of importance of a competency. By using this framework, the L1 SOC Analyst competency assessment can be carried out more comprehensively and help the competency evaluation process more accurately in prioritizing competencies that must be improved. SOC XYZ was chosen as a case study in the implementation of this framework and matrix because it has a large enough structure and function so that all key competencies used in L1 SOC ACM can be tested. From the results of the implementation of this framework to SOC XYZ, it was found that L1 SOC ACM produced a high match rate

of capability (85%) and maturity (100%). This suggests that L1 SOC ACM are appropriate methods for the L1 SOC competency assessment of SOC XYZ.

Keywords: SOC analyst, Competency Framework, Skills Framework, Competency Assessment, Competency Matrix, Maturity Assessment, SOC Analyst Performance.

© Copyright 2025
by Agung Setiaji
All rights reserved

DEDICATION

This thesis is dedicated to my beloved family, whose unwavering support, encouragement, and sacrifices have been my greatest source of strength throughout this journey. To my parents, for their endless love and belief in my potential, and to my siblings, for always inspiring me to aim higher. To my academic mentors and advisors, who have guided me with their wisdom and expertise, shaping the foundation of this work. To my friends and colleagues, whose companionship and collaboration have been invaluable in overcoming challenges along the way. And to all those who have played a role, big or small, in helping me reach this milestone – this work is a testament to your support and belief in me.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my family, whose unwavering support, endless encouragement, and unconditional love have been my greatest source of strength throughout this journey. Without their patience and understanding, this thesis would not have been possible.

I am profoundly thankful to my academic advisors and mentors for their invaluable guidance, expertise, and constructive feedback throughout the research and writing process. Their dedication and commitment to my academic growth have inspired me to push beyond my limits and achieve my goals.

To my friends and fellow students who have shared this journey, your camaraderie, late-night discussions, and encouragement have been instrumental in navigating the challenges of this academic pursuit. I am truly grateful for the bond and memories we have created.

To my colleagues and peers at work, thank you for your support and understanding during this period. Your encouragement and willingness to share knowledge have significantly enriched my learning experience.

Lastly, I would like to extend my heartfelt appreciation to everyone who has contributed, directly or indirectly, to the completion of this thesis. Your assistance and motivation have been invaluable, and I am forever grateful for your support.

TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	6
ACKNOWLEDGEMENTS.....	7
TABLE OF CONTENTS.....	8
LIST OF FIGURES	12
LIST OF TABLES.....	15
CHAPTER 1 - INTRODUCTION.....	18
1.1. Background.....	18
1.2. Research Problem.....	21
1.3. Research Objective.....	24
1.4. Research Question.....	24
1.5. Hypothesis.....	25
1.6. Research Scope and Limitation.....	25
1.7. Significance of Study.....	26
1.8. Thesis Structure.....	26
CHAPTER 2 - LITERATURE REVIEW.....	27
2.1. National Cybersecurity Operation Services.....	27
2.2. PT XYZ.....	30
2.3. Related Regulations.....	32
2.4. Cyber Security.....	33
2.4.1. Cybersecurity Framework.....	33
2.4.2. Cyber Defense.....	34
2.5. Security Operation Center.....	35
2.5.1. SOC Governance.....	40
2.5.1.1. SOC General Arhitecture.....	40
2.5.1.2. SOC Operating Model.....	41
2.5.1.3. Standards & Guidlines.....	42

2.5.1.4.	Security Audit	43
2.5.1.5.	SOC Maturity	44
2.5.1.6.	SOC Performance Metrics	44
2.5.2.	People.....	47
2.5.2.1.	Roles and Responsibilities	48
2.5.2.2.	Skills and Knowledges	59
2.5.3.	Process	65
2.5.3.1.	Log Collection.....	65
2.5.3.2.	Detection & Analysis	66
2.5.3.3.	Containment, Eridication & Recovery	67
2.5.4.	Technology	67
2.5.4.1.	Security Information & Event Management (SIEM).....	68
2.5.4.2.	Intrusion Detection and Prevention System (IDPS).....	69
2.5.4.3.	Automation and Orchestration	70
2.6.	Security Operation Center Operational Challenges.....	71
2.7.	Performance.....	80
2.7.1.	Performance Management	81
2.7.2.	IT Performance Management	82
2.7.3.	SOC Analyst Performance Criteria.....	84
2.8.	Competency	86
2.8.1.	Competency Framework.....	87
2.8.2.	Competency Framework in Cybersecurity	90
2.8.3.	Competency Framework Dimension in Cybersecurity.....	96
2.8.4.	Competencies Capability Levels	99
2.8.5.	Competency Weights	104
2.8.6.	Competency Assessment and Methods.....	107
2.8.7.	Competency Matrix	108
2.8.8.	Methods for Competency Framework Development.....	110
2.8.9.	Validation Criteria and Methods for Competency Framework	114
2.9.	Maturity Model.....	116
2.9.1.	Maturity Model for IT Security	121
2.9.2.	Maturity Model for Security Operation Center	123
2.9.3.	Maturity Model for Competencies.....	125
2.9.4.	Maturity Model Structure	136
2.9.5.	Methods for Developing Maturity Model.....	136

2.10. Design Science Research Methodology	139
2.11. Related Works	141
2.11.1. Previous Studies on SOC Analyst Performance Evaluation	141
2.11.2. Previous Works on Cybersecurity Skills Framework	143
2.11.3. Previous Studies on Maturity Implementation for Competency Framework	145
CHAPTER 3 - RESEARCH METHODS	152
3.1. Research Method	152
3.2. Research Framework	152
3.3. Problem Identification	153
3.3.1. Literature Review	153
3.3.2. Expert Interview	154
3.4. Solution Design	154
3.4.1. Define Job Core Function and Job Description	154
3.4.2. Define L1 SOC Analyst Key Competencies and Competencies Details	155
3.4.3. Expert Review	156
3.4.4. Assigning Weighted on L1 SOC Analyst Key Competencies	156
3.4.5. Capability and Maturity Level Characteristics Development	157
3.4.6. Developing L1 SOC Analyst Competency Framework	158
3.4.7. Developing L1 SOC Analyst Competency Matrix	159
3.4.8. Developing Instrument for Competency Assessment	160
3.5. Validation and Evaluation	160
3.5.1. Validation and Evaluation Criteria	160
3.5.2. Evaluation and Validation Methodology	161
3.5.3. Expert In-Depth Interview	162
3.5.4. Apply L1 SOC Analyst Competency Matrix to SOC XYZ	162
3.5.5. L1 SOC ACM Evaluation and Update	164
CHAPTER 4 - RESULTS AND DISCUSSIONS	165
4.1. Problem Identification	165
4.1.1. Expert Review on Problem Statement	165
4.2. Solution Design	166
4.2.1. Define Job Core Function and Job Description	166
4.2.2. L1 SOC Analyst Key Competencies Identification	167
4.2.3. Developing L1 SOC Analyst Key Competencies Detail	169
4.2.4. Refining L1 SOC Analyst Key Competencies From Expert Review	175

4.3. Assigning Weightages to L1 SOC Analyst Key Competencies	176
4.4. Capability and Maturity Level Characteristics Development	178
4.5. Developing L1 SOC Analyst Competency Framework	181
4.6. Developing L1 SOC Analyst Competency Matrix.....	183
4.6.1. Defining L1 SOC Analyst Profile Based on Capability and Maturity Level	184
4.6.2. Determining Weighted Proficiency Rating for L1 SOC Analyst	185
4.6.3. Proposed L1 SOC Analyst Competency Matrix.....	186
4.7. Developing Assessment Instrument	191
4.8. Validation	192
4.8.1. Validation Participants.....	193
4.8.2. Validation Results.....	194
4.8.3. Key Findings.....	196
4.8.4. Changes Made.....	196
4.9. Implementation on SOC XYZ.....	197
4.9.1. Selection of Competency Assessors	197
4.9.2. Selection of L1 SOC Analyst Who Will Be Assessed.....	198
4.9.3. Implementation Result	198
4.9.3.1. Overall Matched Rate	198
4.9.3.2. Detailed Matched Rate Results	200
4.9.3.3. Implementation Feedbacks.....	209
4.9.4. Evaluation	209
4.9.5. Recommendations.....	210
CHAPTER 5 - CONCLUSIONS AND RECCOMENDATIONS.....	213
5.1. Conclusions	213
5.2. Recommendations and Future Works.....	214
APPENDIX A	216
APPENDIX B	235
APPENDIX C	242
APPENDIX D	273
REFERENCES	279
CURRICULUM VITAE.....	293

LIST OF FIGURES

Figures	Page
1. SOC Analyst Skills Challenges.....	19
2. Problem Identification	21
3. SOC incident response workflow (Falé et al., 2022)	54
4. Security Event Gateway	60
5. SOC Challenges and Problems Relationship	79
6. Capability Level and Maturity Level Relationship.....	84
7. Iceberg Competency Model	88
8. Onion Competency Model	89
9. Trapezium Competency Model.....	89
10. CIIISec Proficiency Level	102
11. Mapping of Cybersecurity Skills Framework Proficiency Level	103
12. Online AHP Calculator	106
13. AHP Application Input Form.....	106
14. AHP Application Result	107
15. Competency Matrix from (Glass & Metternich, 2020).....	109
16. Competency Matrix from (Thandlam Sudhindra & Blessing, 2021)	110
17. Competency Development Framework by (Batt et al., 2021)	112
18. Competency Development Framework by (Midhat Ali et al., 2021)	113
19. Competence claim categories and sub-categories by (Child & Shaw, 2023)	115
20. CMMI Framework Components.....	118
21. CMMI Framework Components Relationships	120
22. COBIT 2019 Maturity Level	121
23. C2M2 Maturity Level Criteria	122
24. ECDMM4.0 for I4.0 Adoption.	126
25. Maturity levels of Employee Competency Maturity Model	128

26. A Conceptual Framework for the Development of Debriefing Skills	130
27. GSD Scrum Maturity Level	131
28. Synopsis of Maturity Model by (Becker et al., 2009).....	138
29. Maturity Model Development Procedur by (Becker et al., 2009)	139
30. DSR Research Method by (Philipp Offermann et al., 2013)	140
31. Research Framework	153
32. Process of Defining L1 SOC Analyst Job Core Functions and Job Descriptions	155
33. Process of Defining L1 SOC Analyst Key Competencies and Details.....	156
34. Process of Developing L1 SOC Analyst Capability Level	157
35. Process of Developing L1 SOC Analyst Maturity Level.....	158
36. AHP Decision Matrix Result	177
37. Proposed L1 SOC Analyst Competency Framework	181
38. Assessment Instrument	191
39. Capability Matched Rate Result	199
40. Security Monitoring and Intrusion Analysis Matched Rate	200
41. Incident Management Matched Rate	201
42. Tools Proficiency Matched Rate.....	202
43. Data Vizualisation Matched Rate	202
44. Network Management Matched Rate	203
45. Stress Resilience Matched Rate	204
46. Time Management Matched Rate	205
47. Communication Match Rate	206
48. Team Work Match Rate	207
49. Analytical Mind Match Rate.....	207
50. Creative and Innovative Match Rate.....	208
51. Competencies Pairwise Comparison	233
52. Validation Evidence With Mr. Digit Oktavianto	235
53. Validation Evidence With Mr. Wahya Nuryanto.....	237
54. Validation Evidence With Mr. Andi Yusuf	239
55. ACP Implementation Documentation.....	273

56. AL Implementation Documentation	273
57. ANP Implementation Documentation.....	274
58. GPN Implementation Documentation.....	274
59. MSM Implementation Documentation	275

LIST OF TABLES

Table	Page
1. Problem Identification	21
2. SOC incident response workflow (Falé et al., 2022)	54
3. Security Event Gateway	60
4. SOC Challenges and Problems Relationship	79
5. Capability Level and Maturity Level Relationship.....	84
6. Iceberg Competency Model	88
7. Onion Competency Model	89
8. Trapezium Competency Model.....	89
9. CIISec Proficiency Level	102
10. Mapping of Cybersecurity Skills Framework Proficiency Level	103
11. Online AHP Calculator	106
12. AHP Application Input Form.....	106
13. AHP Application Result	107
14. Competency Matrix from (Glass & Metternich, 2020).....	109
15. Competency Matrix from (Thandlam Sudhindra & Blessing, 2021)	110
16. Competency Development Framework by (Batt et al., 2021)	112
17. Competency Development Framework by (Midhat Ali et al., 2021)	113
18. Competence claim categories and sub-categories by (Child & Shaw, 2023)	115
19. CMMI Framework Components	118
20. CMMI Framework Components Relationships	120
21. COBIT 2019 Maturity Level	121
22. C2M2 Maturity Level Criteria	122
23. ECDMM4.0 for I4.0 Adoption.	126
24. Maturity levels of Employee Competency Maturity Model	128
25. A Conceptual Framework for the Development of Debriefing Skills	130

26. GSD Scrum Maturity Level	131
27. Synopsis of Maturity Model by (Becker et al., 2009).....	138
28. Maturity Model Development Procedur by (Becker et al., 2009)	139
29. DSR Research Method by (Philipp Offermann et al., 2013)	140
30. Research Framework	153
31. Process of Defining L1 SOC Analyst Job Core Functions and Job Descriptions	155
32. Process of Defining L1 SOC Analyst Key Competencies and Details.....	156
33. . Process of Developing L1 SOC Analyst Capability Level	157
34. Process of Developing L1 SOC Analyst Maturity Level.....	158
35. AHP Decision Matrix Result	177
36. Proposed L1 SOC Analyst Competency Framework	181
37. Assessment Instrument	191
38. Capability Matched Rate Result	199
39. Security Monitoring and Intrusion Analysis Matched Rate	200
40. Incident Management Matched Rate	201
41. Tools Proficiency Matched Rate.....	202
42. Data Vizualisation Matched Rate	202
43. Network Management Matched Rate	203
44. Stress Resiliance Matched Rate	204
45. Time Management Matched Rate	205
46. Communication Match Rate	206
47. Team Work Match Rate	207
48. Analytical Mind Match Rate.....	207
49. Creative and Innovative Match Rate.....	208
50. Competencies Pairwise Comparison	233
51. Validation Evidence With Mr. Digit Oktavianto	235
52. Validation Evidence With Mr. Wahya Nuryanto.....	237
53. Validation Evidence With Mr. Andi Yusuf	239
54. Adit Chandra Prayuda Implementation Documentation.....	273
55. Anjeli Lutfiani Implementation Documentation.....	273

56. Arbain Nur Prasetyo Implementation Documentation	274
57. Galang Putra Nusantara Implementation Documentation	274
58. Mahar Surya Malaka Implementation Documentation	275