

**A GAT FRAMEWORK FOR CYBERSECURITY POSTURE ASSESSMENT
USING SELF-HOSTED LLM (LLAMA 3.1) : A GOVERNANCE-DOMAIN
PROOF OF CONCEPT AT XYZ GROUP**

By

DEDY RUSTANDI

20001504

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutra Barat No. 15, Alam Sutra

Tangerang, Banten 15143 - Indonesia

August 2026

Revision after the Thesis Defense on 7 August 2026

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.



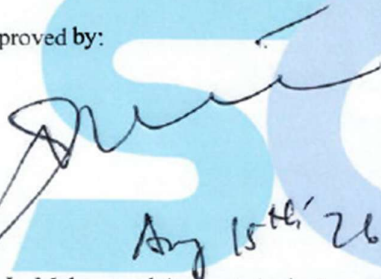
Dedy Rustandi

Student

14-Aug-2026

Date

Approved by:


Aug 15th '26

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

Thesis Advisor

14-Aug-2026

Date



Dr. Ir. Eka Budiarto, S.T., M.Sc.

Thesis Co-Advisor

15-Aug-2026

Date

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

Dean of Faculty of Engineering & Information Technology

ABSTRACT

A GAT FRAMEWORK FOR CYBERSECURITY POSTURE ASSESSMENT USING SELF-HOSTED LLM (LLAMA 3.1) : A GOVERNANCE-DOMAIN PROOF OF CONCEPT AT XYZ GROUP

By

DEDY RUSTANDI

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

Dr. Ir. Eka Budiarto, S.T., M.Sc.

SWISS GERMAN UNIVERSITY

XYZ Group currently relies on a manual, self-reported cybersecurity checklist that provides limited evidence of traceability, maturity differentiation, sector calibration, and linkage to Enterprise Risk Management (ERM). This research develops the GAT (Governance-Awareness-Technology) Framework, evidence-based assessment model using a graded FLPN (Fully-Largely-Partially-Not) rating scale, sector-differentiated Analytic Hierarchy Process weighting, and a self-hosted Retrieval-Augmented Generation pipeline. A Governance-domain proof of concept was executed across two subsidiaries with different sector, using Llama 3.1 8B for assessment and a cross-family judge model for faithfulness verification, validated through a practitioner focus group discussion. By assuming that Awareness and Technology Domain given same score 60, PoC result shows domain scores of 60 (Moderate) and 51 (Moderate) respectively, with RAGAS faithfulness of 0.84 and 0.82 against a 0.80 target, and an estimated 99% reduction in scoring time relative to the manual baseline. Practitioners endorsed the framework's architecture conditionally, identifying coverage gaps and traceability concerns requiring refinement. The findings indicate that LLM-automated, evidence-grounded cybersecurity posture assessment is a viable improvement over manual processes for the Governance domain, though accuracy and full three-domain deployment require further validation before enterprise-wide adoption. *Keywords: cybersecurity maturity assessment, retrieval-augmented generation, enterprise risk management, capability maturity model, RAGAS*



© Copyright 2026
by Dedy Rustandi
All rights reserved

DEDICATION

I dedicate this thesis to my family for the support given and the sacrificed through long nights and weekends. To my colleague at XYZ whose trust in this project gave it purpose beyond the page.



ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to Allah SWT for His blessings, guidance, and strength throughout my academic journey and the completion of this thesis.

I would like to extend my sincere appreciation to my advisor (Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc) and co-advisor (Dr. Ir. Eka Budiarto, S.T., M.Sc.) for their invaluable guidance, constructive feedback, patience, and continuous encouragement throughout this research. Thank you also to Dr. Charles Lim, B.Sc., M.Sc and Dr. Ir. Heru Purnomo Ipung, M.Eng for provide me feedback and invaluable suggestion during my work on Thesis. Their expertise, insights, and dedication have been instrumental in shaping this study and helping me navigate the challenges encountered during the research process.

I would like to express my heartfelt gratitude to my beloved family. To my wife, thank you for your unwavering support, understanding, patience, and encouragement throughout the demanding period of this study. To my children, thank you for being a constant source of motivation, joy, and inspiration. Your support has given me the strength to persevere and complete this academic milestone.

I would also like to thank my supervisors, colleagues, and cybersecurity practitioners within XYZ Group who generously contributed their time and expertise during the Focus Group Discussion (FGD) sessions. Their practical insights, professional perspectives, and constructive feedback played a vital role in validating and improving the proposed Governance–Awareness–Technology (GAT) Framework. Their participation significantly strengthened both the academic rigor and practical relevance of this research.

Finally, I would like to thank all lecturers, especially to friends, classmates, and everyone who has directly or indirectly contributed to the thesis.

May this research contribute to the advancement of cybersecurity governance assessment practices and provide value to both academic and professional communities.

TABLE OF CONTENTS

	Page
ABSTRACT.....	3
DEDICATION	5
ACKNOWLEDGEMENTS	6
TABLE OF CONTENTS.....	7
LIST OF FIGURES	12
LIST OF TABLES	13
CHAPTER 1- INTRODUCTION	15
1.1. Background	15
1.2. Problem Statement	17
1.3. Research Objective	21
1.4. Research Questions	22
1.5. Hypothesis.....	24
1.6. Significance of the Study	25
1.7. Research Scope and Limitation	25
1.8. Thesis Structure	27
CHAPTER 2- LITERATURE REVIEW	30
2.1. XYZ Organizational Context	30
2.1.1. Organizational Profile	30
2.1.2. Sub-Sector Profiles and Their Cybersecurity Implications.....	31
2.1.3. Regulatory Heterogeneity Across the ASEAN Portfolio.....	32
2.1.4. Current Cybersecurity Assessment State and Its Limitations.....	32
2.2. Enterprise Risk Management and Cybersecurity Risk Integration.....	35
2.2.1. Cybersecurity Posture Assessment in ERM Context.....	36
2.2.2. ERM-Derived Requirements for Posture Assessment	37

2.3.	Review of Existing Cybersecurity Assessment Frameworks	39
2.3.1.	NIST Cybersecurity Framework 2.0.....	39
2.3.2.	ISO/IEC 27001:2022	41
2.3.3.	CIS Controls Version 8	42
2.3.4.	C2M2, CTI and CCMF	43
2.3.5.	Comparative Summary of Frameworks	45
2.4.	Cybersecurity Maturity Modelling and Composite Scoring	46
2.4.1.	Five-Level Maturity Modelling Foundations.....	46
2.4.2.	Governance Domain Rubric Design	47
2.4.3.	Rubric Design Principle	48
2.4.4.	Composite Scoring Methodology	50
2.4.5.	FLPN Capability Rating Scale: Origins and Theoretical Basis	51
2.4.6.	Analytic Hierarchy Process for Domain Weighting	52
2.4.7.	Business Impact Factor Integration.....	53
2.5.	Gap Analysis: XYZ Current State vs. ERM Requirements	53
2.5.1.	Gap Analysis Methodology	53
2.5.2.	Gap Analysis Indicators and Their Selection Rationale	54
2.5.3.	Gap Analysis Results — XYZ Current State.....	56
2.5.4.	Root Cause Analysis	57
2.5.5.	Summary of Identified Gaps	58
2.6.	Mapping Gaps to Assessment Design Requirements (ADRs).....	58
2.6.1.	Derivation of Assessment Design Requirements.....	58
2.6.2.	ADR Summary Table	59
2.6.3.	Mapping Gaps to Assessment Design Requirements	60
2.7.	Mapping Gaps to Candidate Methods and Tools.....	61
2.7.1.	Method Selection Methodology.....	62

2.7.2.	Method Selection Criteria	62
2.7.3.	Comparative Analysis of Candidate Methods	63
2.8.	Large Language Models for Automated Security Assessment.....	66
2.8.1.	Retrieval-Augmented Generation for Compliance Verification.....	67
2.8.2.	LLMs for Security Policy Automation	67
2.8.3.	Evaluation of RAG-Based Systems	68
2.8.4.	Previous Study of Security Assessment using LLM.....	68
2.8.5.	The reason of using Llama 3.1	70
2.9.	Summary and Theoretical Framework.....	73
2.9.1.	Theoretical Framework	74
CHAPTER 3-	RESEARCH METHODS	76
3.1.	Research Design.....	76
3.2.	GAT Framework Development Method.....	77
3.2.1.	Indicator derivation approach	78
3.2.2.	Maturity rubric development	78
3.2.3.	FLPN Capability Questionnaire Design Methodology.....	79
3.2.4.	Composite scoring construction.....	80
3.2.5.	GAT Framework End-to-End Flowchart	81
3.2.6.	FGD validation protocol	82
3.3.	GAT RAG Pipeline Architecture PoC.....	82
3.3.1.	System Architecture Overview	83
3.3.2.	Document Complexity Analysis	84
3.3.3.	Document Ingestion and Chunking	84
3.3.4.	Retrieval and Scoring Pipeline.....	85
3.3.5.	Gap Narrative Generation	86
3.4.	Scope and Limitations of the Proof of Concept.....	87

3.5.	Population and Sampling Method.....	89
3.5.1.	Subsidiary Population and Sampling	89
3.5.2.	FGD Participant Population and Sampling.....	90
3.6.	Data Sources and Collection	91
3.6.1.	Required Evidence Documents	92
3.6.2.	Organizational Metadata	93
3.6.3.	RAGAS Ground Truth Preparation.....	93
3.7.	Evaluation Methods	93
3.7.1.	SC1 — Assessment Efficiency	94
3.7.2.	SC2 — RAG Pipeline Quality (RAGAS Evaluation).....	94
3.7.3.	SC3 — Framework and Output Validation	95
3.8.	Validation Methodologies.....	95
3.8.1.	FGD Protocol	96
3.8.2.	FGD Data Analysis	97
3.8.3.	FGD Expert Qualifications and Questionnaire	97
3.8.4.	RAGAS Evaluation Procedure	98
3.9.	Success Criteria.....	99
3.10.	Research Timeline	101
CHAPTER 4-	RESULTS AND DISCUSSIONS.....	103
4.1.	GAT Framework Design.....	103
4.1.1.	Framework Architecture and Workflow	103
4.1.2.	GAT Framework Indicator Register and Standard Mapping.....	106
4.1.3.	Maturity Rubrics and FLPN Capability Questionnaires	112
4.1.4.	Composite Scoring Model	120
4.1.5.	SC3 - Framework Validation via FGD	121
4.2.	RAG Pipeline Implementation.....	127

4.2.1.	Deployed Architecture	127
4.2.2.	Pipeline Components and Configuration	128
4.2.3.	Web-Based Result Dashboard	133
4.3.	PoC Assessment Result.....	136
4.3.1.	PoC Execution Overview.....	136
4.3.2.	Knowledge Base Used in PoC	139
4.3.3.	SC1 — Assessment Efficiency Results	140
4.3.4.	SC2 — RAG Pipeline Quality (RAGAS) Results	145
4.3.5.	Indicator-Level Assessment Results	148
4.4.	Discussion	154
4.4.1.	Answering Research Questions	154
4.4.2.	Threats to Validity and Limitations	156
4.4.3.	Summary	157
CHAPTER 5-	CONCLUSIONS AND RECCOMENDATIONS	158
5.1.	Conclusions.....	158
5.2.	Recommendations.....	159
5.3.	Future Works and Roadmaps.....	160
APPENDIX.....		163
Appendix 1 –	GAT Full Register and Rubric Criteria	163
Appendix 2 –	FLPN Questionnaire (PoC Domain Only)	172
Appendix 3 –	LLM Prompt.....	194
Appendix 4 –	PoC Assessment Detail Result	196
Appendix 5 –	RAGAS Evaluation Score.....	197
Appendix 6 –	FGD Minutes of Meeting	199
GLOSSARY		204
REFERENCES		205

LIST OF FIGURES

Figures	Page
Figure 1.1 Fishbone Diagram - Root cause of Inadequate Cybersecurity Posture Assessment at XYZ.....	20
Figure 2.1 Cybersecurity Posture Assessment in ERM context	36
Figure 2.2 NIST Cybersecurity Framework (National Institute of Standards and Technology, 2024)	39
Figure 2.3 NIST CSF 2.0 Structure (National Institute of Standards and Technology, 2024)	40
Figure 3.1 GAT Framework Development Method.....	77
Figure 3.2 GAT Framework End-To-End Flowchart	81
Figure 3.3 RAG Pipeline Development & PoC Execution Process.....	83
Figure 4.1 GAT Framework Architecture.....	105
Figure 4.2 GAT Framework High Level Assessment Workflow	106
Figure 4.3 Deployed Backend Architecture of the Governance Assessment Tool (GAT) Framework	127
Figure 4.4 FLPN Algorithm Workflow	131
Figure 4.5 LLM Prompt Workflow	132
Figure 4.6 Web Dashboard Screen	134
Figure 4.7 Sample of Assessment Result Screen.....	134
Figure 4.8 Evidence Display and Citation Screen	135
Figure 4.9 Gap Narrative Screen.....	136
Figure 4.10 Gap Narrative generated by LLM for G2 XYZ-RHQ.....	150
Figure 5.1 GAT-LLM Roadmap Plan.....	161

LIST OF TABLES

Table	Page
Table 2.1 XYZ Group Cybersecurity Characteristics and GAT Framework Design Implications.....	34
Table 2.2 Comparative Analysis of Cybersecurity Assessment Frameworks	45
Table 2.3 FLPN Rating Category	49
Table 2.4 Rubric Design Comparison Across Maturity Models.....	49
Table 2.5 Gap Analysis Indicators and Selection Rationale.....	54
Table 2.6 Gap Analysis Results: XYZ Current State vs. ERM Requirements.....	56
Table 2.7 Root Cause Analysis.....	57
Table 2.8 The Eight Assessment Design Requirements	59
Table 2.9 Method Selection Criteria.....	62
Table 2.10 Gap-Driven Method Comparison Matrix.....	63
Table 2.11 LLM and RAG Architecture Comparison for Security Assessment	69
Table 2.12 Comparison of Candidate Self-Hosted LLMs	71
Table 3.1 Subsidiary Sampling Criteria.....	89
Table 3.2 FGD Participant Composition and Criteria.....	90
Table 3.3 Evidence Documents per Subsidiary	92
Table 3.4 FGD Expert Qualification.....	97
Table 3.5 FGD Topics.....	98
Table 3.6 Success Criteria Definition	99
Table 3.7 Sixteen-Week Research Implementation Schedule	101
Table 4.1 Four Layer GAT Framework	104
Table 4.2 GAT Governance Domain Indicators	107
Table 4.3 GAT Awareness Domain Indicators.....	108
Table 4.4 GAT Technology Domain Indicators	108
Table 4.5 Standards Cross-Mapping for all GAT Indicators	109
Table 4.6 Indicator-to-ADR Traceability Summary	112
Table 4.7 GAT Maturity Levels.....	113
Table 4.8 G1 Information Security Policy Maturity Rubric.....	114
Table 4.9 Binary Question Distribution per Domain.....	116
Table 4.10 Question Categories per Maturity Level.....	117

Table 4.11 AHP Weight on Each Sector.....	120
Table 4.12 Five-band classification	121
Table 4.13 Configured parameter and justification	128
Table 4.14 PoC Execution Timeline	138
Table 4.15 XYZ-RHQ Knowledge Base List	139
Table 4.16 XYZ-ID Knowledge Base List	140
Table 4.17 Assessment Time Result.....	141
Table 4.18 Efficiency Compariosn between existing and GAT RAG Pipeline.....	143
Table 4.19 Faithfullness Score Results	145
Table 4.20 PoC Result - Per Indicator Maturity Scores & Evidence Citations	149
Table 4.21 Governance Indicator Domain Result.....	151
Table 4.22 Composite Score Summary	153

