

**DEVELOPING AN INTEGRATED SECURITY OPERATIONS FRAMEWORK TO
BRIDGE GOVERNANCE-OPERATIONS: A DESIGN SCIENCE APPROACH
SYNTHESIZING MULTI-FRAMEWORK AND INDONESIAN REGULATORY
FRAMEWORKS AT PT. BANK XYZ**

By

Adam Kalabadzi

22451044

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

January 2026

Revision after Thesis Defense on 2nd February 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.



Adam Kalabadzi

Student

15 Feb 2026

Date

Approved by:



Dr. Ir. Charles Lim, B.Sc., M.Sc.

Thesis Advisor

15/2/26

Date

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

Thesis Co-Advisor

Feb 15th '26 / 26 / 26

Date

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

Dean of Faculty of Engineering & Information Technology

Date

ABSTRACT

DEVELOPING AN INTEGRATED SECURITY OPERATIONS FRAMEWORK TO BRIDGE GOVERNANCE-OPERATIONS : A DESIGN SCIENCE APPROACH SYNTHESIZING MULTI-FRAMEWORK AND INDONESIAN REGULATORY FRAMEWORKS AT PT. BANK XYZ

By

Adam Kalabadzi

Dr. Ir. Charles Lim BSc., MSc, Advisor

Dr. Ir. Mohammad A Soetomo, DSc

SWISS GERMAN UNIVERSITY

Indonesian banks face a critical governance-to-operations gap where strategic cybersecurity frameworks define requirements but lack operational implementation guidance for security device management. This research develops the integrated Security Operations Framework (i-SOF) for banking sector security device operations using Design Science Research Methodology. Adapting established thematic analysis and qualitative synthesis methodologies, a systematic seven-step process synthesizes 14 source frameworks, including NIST CSF 2.0, ISO 27001, COBIT 2019, ITIL 4, TOGAF, DORA, and Indonesian regulations (POJK, SEOJK, PBI) into 100 operational criteria across 10 categories: Governance, Risk Management, Operations, Technical Controls, Monitoring, Incident Response, Resilience, Digital Trust, Third-Party Management, and Audit. The framework features a six-layer architecture explicitly translating governance requirements into operational procedures, RACI matrices, and KPIs. Demonstration at Bank XYZ through gap analysis, risk assessment, and management FGD validation confirms i-SOF addresses seven identified research gaps. The study concludes that integrated multi-framework approaches are more effective than single-framework implementations. i-SOF contributes as the first comprehensive framework specifically designed for banking security device operations, integrating more frameworks than prior studies while operationalizing Indonesian regulatory requirements.

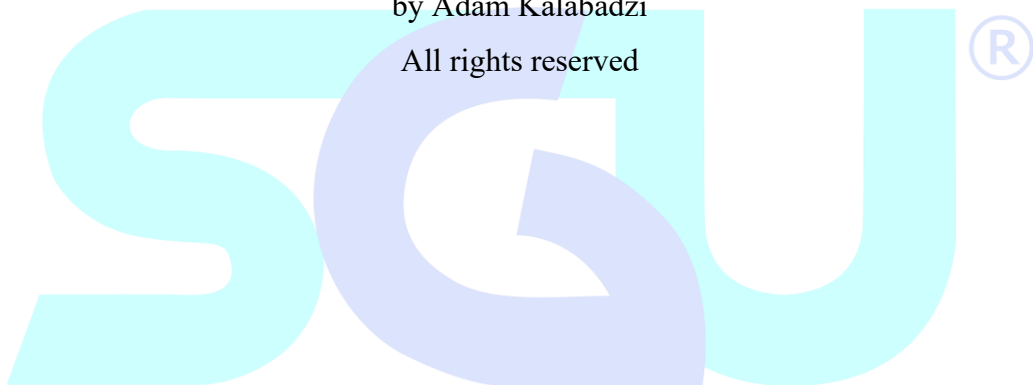
Keywords: Security Operations Framework, Multi-Framework Integration, Banking Cybersecurity, Governance-to-Operations Translation, IT Operation

Adam Kalabadzi

©copyright 2026

by Adam Kalabadzi

All rights reserved



DEDICATION

This thesis is dedicated to:

Allah SWT,

for the countless blessings, guidance, and strength throughout this journey.

My parents,

for your endless love, support, and prayers that have always been my source of strength.

Everything I have achieved is because of your sacrifices and guidance.

My beloved wife,

for your unwavering support, patience, and endless encouragement. I would not have gone through this without you by my side. Your sacrifices and belief in me have made this achievement possible.

My son and daughter,

for understanding and accepting the time I had to sacrifice from being with you to complete this study. May this work inspire you to always pursue knowledge and never stop learning.

Indonesia,

my homeland. May this work contribute to strengthening the cybersecurity posture of our nation's banking sector and support Indonesia's vision for a secure digital economy.

This is for all of you.

ACKNOWLEDGEMENT

First and foremost, I would like to express my deepest gratitude to Allah SWT for His countless blessings, guidance, and strength that have enabled me to complete this thesis. Without His grace, this accomplishment would not have been possible.

I wish to express my heartfelt gratitude to my advisor, Dr. Ir. Charles Lim, BSc., MSc., and co-advisor, Dr. Ir. Mohammad Amin Soetomo, DSc., for their invaluable guidance, insightful feedback, and continuous support throughout this research. Their expertise and encouragement have been instrumental in shaping the direction and quality of this thesis. I would also like to extend my sincere appreciation to Dr. Ir. Eka Budiarto, for his constructive feedback and valuable suggestions that have significantly improved the quality of this work.

My sincere gratitude goes to my superiors at Bank XYZ, whose encouragement and support made it possible for me to pursue this academic endeavour alongside my professional responsibilities. Their understanding and flexibility have been a source of inspiration and motivation throughout this journey.

To my beloved wife, your unwavering support, patience, and love have been my greatest strength. I would not have gone through this journey without you by my side. This accomplishment is as much yours as it is mine. To my son and daughter, thank you for your understanding and patience during the many hours I had to dedicate to this study. I hope this work inspires you to always strive for excellence and never stop learning.

Finally, I wish to acknowledge my colleagues and peers, whose constructive discussions and collaboration enriched this research. I hope this work contributes meaningfully to the advancement of cybersecurity practices in the Indonesian banking sector and supports our nation's journey toward a secure digital economy.

TABLE OF CONTENTS

	Page
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENT.....	6
TABLE OF CONTENTS.....	7
LIST OF FIGURES	23
LIST OF TABLES.....	25
CHAPTER 1 – INTRODUCTION	29
1.1 Background.....	29
1.2 `Research Problem.....	34
1.3 Research Questions	37
1.4 Hypothesis	37
1.5 Research Objectives	38
1.6 Research Scope and Limitations	38
1.7 Significance of Study	39
1.8 Thesis Structure	40
CHAPTER 2 - LITERATURE REVIEW	41
2.1 Introduction	41
2.2 Foundational Cybersecurity Concepts.....	43
2.2.1 Cybersecurity and Information Security.....	43
2.2.2 Security Operation Center and Security Operations (SecOps).....	44
2.2.3 Distinction Between SOC, and Security Operations	45
2.3 Review of Major International and National Cybersecurity Frameworks	46
2.3.1 NIST Cybersecurity Framework (CSF) 2.0.....	46
2.3.2 ISO/IEC 27001:2022 and ISO/IEC 27002:2022)	48

2.3.3	COBIT 2019	49
2.3.4	ITIL v4 (Information Technology Infrastructure Library)	54
2.3.5	TOGAF (The Open Group Architecture Framework)	58
2.3.6	NIST SP 800-37 (Risk Management Framework) and NIST SP 800-53 Revision 5	61
2.3.7	ISO/IEC 38500:2024 – Corporate Governance of Information Technology	63
2.3.8	ISO/IEC 20000-1:2018 – IT Service Management System Requirements	65
2.3.9	FitSM – Lightweight IT Service Management Standard	66
2.3.10	VeriSM – Service Management Approach for the Digital Age	67
2.3.11	Indonesian Banking Cybersecurity and IT Governance Regulations	69
2.3.11.1	POJK 11/POJK.03/2022	69
2.3.11.2	SEOJK 21/SEOJK.03/2017	70
2.3.11.3	SEOJK 29/SEOJK.03/2022	71
2.3.11.4	PBI No. 2 / 2024	73
2.4	Digital Trust and Resilience Frameworks	74
2.4.1.1	OECD Digital Security Governance & Digital Trust Principles	75
2.4.2	Digital Trust Ecosystem Framework (DTEF – ISACA)	77
2.4.3	EU Digital Operational Resilience Act (DORA)	79
2.4.4	Indonesia Digital Trust Framework	81
2.5	Gap Analysis, And Risk Prioritization Methodologies	83
2.5.1	Gap Analysis Methodology	83
2.5.1.1	Definition and Purpose	83
2.5.1.2	Types of Gap Analysis Approaches	83
2.5.1.3	Gap Analysis Indicators and Metrics	85
2.5.1.4	Gap Analysis Process	86
2.5.2	Risk Prioritization Approach in Information Security	86

2.5.2.1	ISO 31000:2018 Risk Management Framework	86
2.5.2.2	NIST Cybersecurity Framework 2.0 and Risk Management.....	87
2.5.2.3	COBIT 2019 Risk Optimization and IT Governance	88
2.5.2.4	Cybersecurity Maturity Assessment Approaches	88
2.5.2.5	Weighted Scoring Models and Multi-Criteria Decision Making.....	89
2.5.2.6	Cybersecurity Risk Management in Banking Sector	90
2.5.2.7	Comparison of Risk Prioritization Approaches	91
2.5.2.8	Synthesis and Research Gap	91
2.5.3	Risk Prioritization Approaches.....	92
2.5.3.1	Management-Driven Prioritization through Focus Group Discussion (FGD).....	92
2.6	Method for deriving categories and criteria from frameworks	94
2.6.1.	MECE Principle (Mutually Exclusive, Collectively Exhaustive)	95
2.6.1.1.	Definition and Origin	95
2.6.1.2.	Academic Foundation	96
2.6.1.3.	Application in This Research.....	96
2.6.2.	Thematic Analysis Methodology.....	96
2.6.2.1.	Definition	96
2.6.2.2.	Six-Phase Framework	97
2.6.3.	Inductive, Deductive, and Hybrid Coding Approaches.....	97
2.6.3.1.	Inductive Coding (Bottom-Up).....	97
2.6.3.2.	Deductive Coding (Top-Down)	98
2.6.3.3.	Hybrid Coding Approach.....	98
2.6.3.4.	Comparison of Coding Approaches.....	98
2.6.3.5.	Application in This Research.....	99
2.6.4.	Overview of the derivation process	99

2.6.5.	Step 1: Framework Selection.....	101
2.6.5.1.	Comparison Between Frameworks	101
2.6.5.2.	Selection Criteria.....	108
2.6.5.3.	Justification for Framework Selection	111
2.6.5.3.1.	Coverage of the Governance-to-Operations Spectrum	111
2.6.5.3.2.	Evidence from Empirical Studies.....	114
2.6.5.3.3.	Financial Sector Relevance	120
2.6.5.3.4.	Addressing Identified Research Gaps	121
2.6.5.3.5.	Complementarity Analysis	123
2.6.5.3.6.	Currency and Recency	124
2.6.5.4.	Justification for Standard and Guideline Selection.....	126
2.6.5.4.1.	Comparison of ISMS Standards	126
2.6.5.4.2.	Comparison of Control Catalogs and Guidelines.....	126
2.6.5.5.	Summary: Seven-Dimensional Justification.....	127
2.6.5.6.	Output of Step 1	131
2.6.6.	Step 2: Domain & Principles Extraction	131
2.6.6.1.	Extraction Approach	131
2.6.6.2.	Tools and Documentation	134
2.6.6.3.	Output of Step 2	134
2.6.7.	Step 3: Open Coding.....	134
2.6.7.1.	Hybrid Inductive–Deductive Approach	135
2.6.7.2.	Coding Process.....	135
2.6.7.3.	Output of Step 3	141
2.6.8.	Step 4: Thematic Grouping.....	141
2.6.8.1.	Thematic Grouping Process	141

2.6.8.2.	Themes Identified	143
2.6.8.3.	Convergence and Divergence Analysis	146
2.6.8.4.	Output of Step 4	148
2.6.9.	Step 5: Consolidation Into High-Level Categories.....	148
2.6.9.1.	Consolidation Process	148
2.6.9.2.	Consolidation Decisions	149
2.6.9.3.	MECE Validation.....	151
2.6.9.4.	Alignment with i-SOF Architecture.....	152
2.6.9.5.	Output of Step 5	153
2.6.10.	Step 6: Category-Based Framework Comparison.....	155
2.6.10.1.	Comparison Methodology.....	156
2.6.10.2.	Synthesis from Governance and Policy Comparison.....	159
2.6.10.3.	Gap Identified	161
2.6.10.4.	Interpretation for i-SOF	161
2.6.10.5.	Replicating the Comparison for All Categories.....	161
2.6.10.6.	Output of Step 6	162
2.6.11.	Step 7: Thematic Synthesis To Final Criteria	163
2.6.11.1.	Synthesis Methodology.....	163
2.6.11.1.1.	Synthesis Example: Governance and Policy Category	164
2.6.11.2.	Replicating Synthesis for All Categories	166
2.6.11.3.	Criteria Characteristics.....	166
2.6.11.4.	Validation of Criteria	167
2.6.11.5.	Output of Step 7	167
2.6.12.	Validation Of Derived Criteria	168
2.6.13.	Output: Consolidated Criteria For I-Sof Design	184

2.6.14.	Master Criteria List Summary.....	184
2.6.15.	Usage in Chapter 4 for contextualization.....	185
2.6.16.	Methodological Strengths And Limitations.....	187
2.6.17.	Section Summary	190
2.7	Framework Comparison	192
2.7.1.	Framework Comparison Based on Category	192
2.7.1.	Governance and Policy	194
2.7.2.	Risk Management	200
2.7.3.	Operations and Service Management	204
2.7.4.	Technical Controls and Architecture	207
2.7.5.	Monitoring and Detection.....	210
2.7.6.	Incident Response and Recovery	213
2.7.7.	Resilience and Continuity.....	219
2.7.8.	Digital Trust and Culture	221
2.7.9.	Third-Party and Supply Chain	224
2.7.10.	Audit and Compliance	227
2.7.11.	Synthesis: The Necessity of Multi-Framework Integration.....	233
2.8.	Previous Works and Critical Review	234
2.8.1.	Literature Search Methodology	235
2.8.2.	Framework Integration Studies.....	235
2.8.2.1.	The Insufficiency of Single Frameworks.....	235
2.8.2.2.	Governance-Operations Integration Patterns	236
2.8.2.3.	Operational Translation Attempts.....	237
2.8.2.4.	Architectural and Control-Level Integration.....	238
2.8.2.5.	Critical Synthesis: Integration Patterns and Gaps.....	238

2.8.2.6.	I-SOF Response to Framework Integration Gaps	239
2.8.3.	Security Operations Center and SecOps Research	240
2.8.3.1.	The Fragmentation Problem: Lack of Holistic SOC Definition	241
2.8.3.2.	Operational Practice Frameworks: Bridging Strategy to Execution	242
2.8.3.3.	Critical Synthesis: Convergence and Persistent Gaps.....	244
2.8.3.4.	i-SOF's Response to SecOps Research Gaps	246
2.8.4.	Banking and Financial Sector Cybersecurity Studies.....	246
2.8.4.1.	Sector-Specific Framework Application: Retail Industry Lessons.....	247
2.8.4.2.	Banking Sector Framework Integration: Service Delivery Focus	248
2.8.4.3.	Generic IT Governance Implementation Challenges.....	250
2.8.4.4.	Critical Synthesis: Banking Cybersecurity Framework Gap	251
2.8.4.5.	i-SOF's Banking Sector Contribution	252
2.8.5.	Digital Trust and Operational Resilience Research.....	253
2.8.6.	Maturity Model Studies	254
2.8.7.	Critical Comparison and Synthesis Across Research Streams	255
2.8.8.	Research Gaps Identification and i-SOF Contribution.....	263
2.9.	Consolidated Criteria for i-SOF Framework Design.....	266
2.9.1.	Introduction: From Framework Integration to Operational Criteria.....	266
2.9.2.	Criteria Organization: Ten Categories.....	268
2.9.3.	Master Criteria Table with Indonesian Regulatory Mapping	270
2.9.4.	Indonesian Regulation to Criteria Cross-Reference	292
2.10.	Maturity Models Synthesis for i-SOF Framework	296
2.10.1.	Introduction: The Role of Maturity Assessment in i-SOF.....	296
2.10.2.	Review of Existing Maturity Models.....	297
2.10.3.	Comparative Analysis of Maturity Models.....	300

2.10.4.	i-SOF Maturity Model Design	302
2.10.4.1.	Maturity Level Definitions for Security Operations	302
2.10.5.	10 Maturity Dimensions Aligned with i-SOF Categories.....	305
CHAPTER 3 - RESEARCH METHODOLOGY		307
3.1	Introduction	307
3.2	Design Science Research Methodology (DSRM)	307
3.3	Research Design Framework.....	310
3.4	Data Collection Methods.....	317
3.4.1	Document Review	317
3.4.2	Semi-Structured Interviews	318
3.4.3	Security Metrics Collection	319
3.4.4	Observation.....	320
3.5	Data Analysis Methods.....	321
3.6	Gap Analysis Methodology.....	321
3.6.1	Assessment Process	321
3.6.2	Maturity Scoring Methodology	322
3.6.3	Gap Prioritization Methodology	323
3.6.3.1	Weight Derivation and Justification	323
3.6.3.2	Scoring Criteria	324
3.6.3.3	Priority Classification	325
3.6.3.4	Assessment Scope and Limitations.....	325
3.6.3.5	Prioritization Application Example	326
3.6.3.6	Methodology Limitations.....	327
3.6.3.7	Management-Driven Prioritization Through Focus Group Discussion	327
3.7	i-SOF Framework Design.....	328

3.7.1	Framework Architecture Overview	328
3.7.1.1	<i>Layer 1 - Governance Layer</i>	329
3.7.1.2	<i>Layer 2 – Risk and Control Layer</i>	329
3.7.1.3	<i>Layer 3 - Operational Layer</i>	329
3.7.1.4	<i>Layer 4 - Technical Layer</i>	329
3.7.1.5	<i>Layer 5 - Resilience Layer</i>	330
3.7.1.6	<i>Layer 6 – Trust and Culture Layer</i>	330
3.7.1.7	<i>Cross Cutting Categories</i>	330
3.7.2	i-SOF Three-Level Architecture Model	330
3.7.2.1	Rationale for Three-Level Architecture	331
3.7.2.2	Three-Level Structure and Category Allocation	331
3.7.2.3	Level 1: Strategic (Direction and Governance)	331
3.7.2.4	Level 2: Tactical (Architecture and Controls)	332
3.7.2.5	Level 3: Operational (Day-to-Day Execution)	333
3.7.2.6	Strategic-to-Operational Bridge Mechanism	334
3.7.2.7	Alignment with Six-Layer Architecture	334
3.7.2.8	Practical Application	335
3.7.2.9	i-SOF Conceptual Security Operations Model	336
3.7.2.10	Category and Criteria Structure	339
3.7.2.11	Framework-to-Criteria Cross-Walk	340
3.7.2.12	Thematic Synthesis Process	342
3.7.2.13	Criterion Specification Template	343
3.7.3	i-SOF Framework Design Process	347
3.7.4	i-SOF Operational Deliverables	352
3.7.4.1	RACI Matrix for Normal Change Management	352

3.7.4.2	Key Performance Indicators (KPIs)	353
3.7.4.3	Process Step Summary with Artifacts and Controls	354
3.8	Success Criteria	357
3.9	Theoretical Foundation for Success Criteria	359
3.10	Validation Approach.....	360
3.10.1	Expert Review	360
3.10.2	FGD Validation	361
3.11	Ethical Considerations	363
CHAPTER 4 – RESULT AND DISCUSSION		364
4.1.	Introduction.....	364
4.2.	i-SOF Framework Overview	364
4.2.1.	Measurement Framework Design Rationale	364
4.2.2.	Maturity Level Definitions	366
4.2.3.	Maturity Dimensions Aligned with i-SOF Categories	368
4.3.	i-SOF Framework Results	371
4.3.1.	Framework Architecture Overview	371
4.3.2.	Category and Criteria Structure Results	375
4.3.3.	L3 Requirements and Implementation Guidelines	377
4.3.4.	Framework-to-Criteria Cross-Walk Results	380
4.3.5.	Thematic Synthesis Results	382
4.4.	Assessment Results and Gap Analysis	383
4.4.1.	Assessment Overview.....	383
4.4.2.	Overall Maturity Assessment	385
4.4.3.	Gap Analysis & Risk Assessment Results.....	388
4.4.3.1.	Residual Risk Profile	395

4.4.4.	Risk to Solution Mapping	397
4.4.5.	Detailed Risk Analysis — HIGH Priority	400
4.4.6.	Detailed Risk Analysis — MEDIUM Priority.....	401
4.4.7.	LOW Priority Risk Summary	402
4.4.8.	Systemic Risk Theme Analysis	403
4.4.9.	Regulatory Alignment Analysis	405
4.5.	Validation and Evaluation Results.....	406
4.5.1.	Framework Validation (Expert Review).....	406
4.5.1.1.	Expert Panel Composition	406
4.5.1.2.	Expert Validation Quantitative Results.....	407
4.5.1.3.	Expert Qualitative Feedback Analysis.....	410
4.5.1.3.1.	Key Strengths Identified by Experts	411
4.5.1.3.2.	Critical Concerns and Omissions Identified.....	411
4.5.1.3.3.	Improvement Recommendations.....	412
4.5.1.3.4.	Implementation Risks Identified	412
4.5.1.3.5.	Feedback Incorporation Summary	413
4.5.2.	Framework Evaluation (Internal FGD)	414
4.5.2.1.	Focus Group Discussion Overview.....	414
4.5.2.2.	FGD Quantitative Results	415
4.5.2.3.	FGD Qualitative Discussion	417
4.5.2.3.1.	Strengths Identified by Management	417
4.5.2.3.2.	Concerns and Limitations Raised.....	417
4.5.2.3.3.	Improvement Suggestions from Management	418
4.5.2.3.4.	Areas for Framework Expansion.....	418
4.5.2.3.5.	Management Validation of Gap Findings	419

4.5.2.3.6.	Management Commitment Summary	419
4.5.3.	Validation Conclusion	420
4.5.4.	Implementation Roadmap.....	421
4.5.4.1.	Prioritized Implementation Plan	421
4.5.4.2.	Resource Requirements.....	425
4.5.4.3.	Change Management Approach.....	425
4.5.5.	Validation Results Summary	426
4.5.5.1.	Success Criteria Evaluation	426
4.5.5.2.	Validation Conclusions.....	427
4.5.6.	Discussion.....	429
4.5.6.1.	The Value of Multi-Framework Synthesis.....	429
4.5.6.2.	Bridging Governance and Operations Through Architecture	430
4.5.6.3.	Implications of the Gap Analysis and Maturity Assessment and Regulation Compliance	432
4.5.6.4.	FGD and Expert Validation Insight	433
CHAPTER 5 – CONCLUSION		434
5.4.	Conclusion	434
5.1.	Recommendations.....	435
5.1.1.	Recommendations for Bank XYZ	435
5.4.2.	Recommendations for Banking Industry	435
5.4.3.	Recommendations for Regulators.....	435
5.4.4.	Recommendations for Academia.....	436
5.5.	Future Research Directions.....	436
REFERENCES		437
APPENDICES		446
APPENDIX A		446

APPENDIX B - CODEBOOK AND CODING, CATEGORY, CRITERIA AND FRAMEWORKS	446
B.1 Hybrid Coding Approach	446
B.2 Enhanced Codebook (Complete - 63 Codes)	447
GP - Governance and Policy (8 codes)	447
RM - Risk Management (9 codes)	447
B.3 Inductive Codes Detail	449
B.4 Digital Supplementary Materials Note	450
APPENDIX C: FRAMEWORK EXTRACTION	451
C.1 Framework Selection Summary	451
C.2 NIST CSF 2.0 Structure (129 Elements)	451
C.3 Indonesian Regulatory Coverage	452
APPENDIX D: i-SOF CRITERIA SPECIFICATIONS	453
D.1 Criteria Overview	453
D.2 Sample Criteria Specifications	453
D.2.1 GP - Governance and Policy Criteria	453
D.2.2 RM - Risk Management Criteria	454
D.3 RM – i-SOF Complete Four-Level Hierarchical Structure	454
APPENDIX E – i-SOF VALIDATION INSTRUMENTS	517
PART A: Success Criteria Summary	517
PART B: Template FGD Questionnaire (Internal Validation)	518
Session Information	518
Participant Requirements	518
Rating Scale	518
Section A: Framework Value and Strategic Alignment (Criterion 4: Adoption)	518
Section B: Implementation Feasibility (Criterion 4: Adoption)	519
Section C: Framework Quality (Criteria 2 & 5: Clarity & Completeness)	519
Section D: Gap Prioritization	519

Section E: Open-Ended Discussion Questions	519
PART C: Template Expert Review Questionnaire (External Validation)	521
Expert Profile.....	521
Rating Scale.....	521
Section 1: Comprehensiveness/Coverage (Criterion 1)	521
Section 2: Clarity and Usability (Criterion 2)	522
Section 3: Resilience and Architecture (Criterion 3)	522
Section 4: Completeness (Criterion 5)	523
Section 5: Best Practice Alignment & Innovation (Criterion 6)	523
Section 6: Implementation Feasibility.....	523
Section 7: Open-Ended Assessment.....	524
Section 8: Overall Assessment	524
PART D: FGD Internal	525
PART E: Detailed Expert Profiles	526
Expert 1: Pratomo Djati Nugroho, M.Kom, CCISO	526
Expert 2: Aa Iksan Aripin, CISSP	527
Expert 3: Mohammad Raditya Maliki Hansa, CISA, QIA.....	529
Expert 4: Goeroeh Andhi D., CISSP, CDCS, CHFI	531
APPENDIX F - GAP ANALYSIS DETAILED REPORT	534
GP - Governance and Policy.....	535
GP-02: Security Policy Framework	535
GP-03: Roles and Responsibilities (RACI)	537
GP-07: Performance Measurement and KPIs	539
GP-01: Leadership Commitment and Accountability.....	541
GP-05: Strategic Technology Planning	543
GP-08: Internal Audit of Security Operations	545
GP-09: Digital Maturity Assessment	547
GP-10: Board-Level Cybersecurity Reporting	549

TC - Technical Controls and Architecture	551
TC-02: Access Control and Authentication	551
TC-06: IT/Security Architecture Design	553
TC-09: Secure Development for Custom Rules/Scripts	555
TC-01: Secure Configuration Standards	557
TC-03: Network Segmentation and Zoning	559
TC-04: Encryption and Data Protection	560
TC-05: Patch Management for Devices	562
TC-07: Zero Trust Architecture Implementation	564
TC-08: Device Redundancy and Failover	566
TC-10: Physical Security for Device Infrastructure	568
MD - Monitoring and Detection	570
MD-07: Compliance Monitoring and Reporting	570
MD-08: Log Retention and Protection	572
MD-09: Metrics and KPI Tracking	574
MD-01: Security Event Logging	576
MD-02: Log Centralization and SIEM Integration	578
MD-03: Real-Time Monitoring Dashboards	580
MD-04: Anomaly Detection and Alerting	582
OS - Operations and Service Management	584
OS-01: Change Management for Security Devices	584
OS-03: Incident Management Procedures	586
OS-02: Configuration Management Database (CMDB)	588
OS-06: Knowledge Management and Documentation	590
APPENDIX G – DIGITAL FORMAT ARTIFACTS	592

APPENDIX H – SOP CHANGE MANAGEMENT – STANDARD	593
Table of Contents	593
1. Purpose and Scope	595
1.1 Purpose.....	595
1.2 What is a Standard Change?	595
1.3 Standard Change Categories	595
2. SME Validation Roles	596
2.1 Validation Sequence	596
2.2 Decision Flow	596
3. Roles and Responsibilities (RACI)	598
3.1 Key Differences from Normal Change	598
4. Service Level Agreements (SLA)	599
4.1 SLA Calculation.....	599
5. Process Steps with Artifacts and Controls	600
6. Performance Metrics (KPIs)	602
7. Escalation to Normal Change	602
8. References	602
9. Document Approval.....	603
APPENDIX I – MATURITY LEVEL DEFINITION 100 CRITERIA.....	604
CURRICULUM VITAE.....	620

LIST OF FIGURES

Figure 1. 1 Share of Attacks by Industry 2019 – 2024 (Adopted from IBM Report 2024 & 2025)	30
Figure 1. 2 Fish Bone Diagram.....	36
Figure 2. 1 ISO 27001 – PDAC – Cited from (Syafrietal et al., 2022).....	49
Figure 2. 2 Governance System Principles (ISACA, 2019a).....	51
Figure 2. 3 Design Factor Dashboard	53
Figure 2. 4 ITIL Distinct Practices – adopted from (Lopes et al., 2024).....	55
Figure 2. 5 TOGAF ADM – adopted from (The Open Group, 2022)	59
Figure 3. 1 Design Science Research Methodology	309
Figure 3. 2 Research Framework.....	311
Figure 3. 3 Research Framework - Phase 1: Input.....	312
Figure 3. 4 Research Framework - Phase 2: Process - 10 Categories, 100 Criteria	313
Figure 3. 5 Research Framework - Phase 3: Output	314
Figure 3. 6 Research Framework Low Level.....	316
Figure 3. 7 i-SOF Six-Layer Architecture	328
Figure 3. 8 i-SOF in Three Level.....	336
Figure 3. 9 i-SOF Conceptual Model.....	337
Figure 3. 10 Flow Process Change Management - Normal	356
Figure 3. 11 Flow Process Change Management – Standard	356
Figure 4. 1 i-SOF Six Layer Architecture.....	373
Figure 4. 2 i-SOF Three-Level Architecture Diagram.....	374
Figure 4. 3 i-SOF Conceptual Security Operations Model.....	375
Figure 4. 4 i-SOF Criteria Hierarchy: L1 → L2 → L3 → IG/TG	378
Figure 4. 5 Maturity Radar/Spider	387
Figure 4. 6 Gap Distribution by Category	387
Figure 4. 7 Gap Priority Distribution — pie chart: 1 HIGH, 15 MEDIUM, 17 LOWS	390

Figure 4. 8 Inherent Risk Heat Map.....	396
Figure 4. 9 Residual Risk Heat Map.....	396



LIST OF TABLES

Table 1. 1 Share of Attacks by Industry 2019-2023 (Adopted from IBM Report 2024 & 2025)	29
Table 2. 1 NIST CS Core Function and Category (National Institute of Standards and Technology, 2023)	47
Table 2. 2 Comparison of Risk Prioritization	91
Table 2. 3 FGD-based prioritization process	93
Table 2. 4 Advantages and disadvantages of FGD-based prioritization process	93
Table 2. 5 Braun and Clarke's Six-Phase Thematic Analysis Framework (adapted from Braun & Clarke, 2006; 2024)	97
Table 2. 6 Comparison of Qualitative Coding Approaches	98
Table 2. 7 Final Category Summary	100
Table 2. 8 Characteristics of Knowledge Source Types	102
Table 2. 9 Framework Comparison	103
Table 2. 10 Selected Sources	110
Table 2. 11 Complementarity Analysis of Selected Frameworks	123
Table 2. 12 Comparison of ISMS Standards	126
Table 2. 13 Comparison of Control Catalogs/Guidelines	127
Table 2. 14 Framework Selection Matrix	129
Table 2. 15 Code Register Example	139
Table 2. 16 Codebook Summary Sample	139
Table 2. 17 Code to Theme Mapping	147
Table 2. 18 Final Consolidated Categories	149
Table 2. 19 Category Consolidation	154
Table 2. 20 Framework Comparison for Category Governance and Policy	157
Table 2. 21 Literature Validation for Criteria	173
Table 2. 22 Final Consolidated Criteria by Categories	184
Table 2. 23 Methodological Strengths	187

Table 2. 24 Limitation and Mitigations	188
Table 2. 25 High Level Framework Overview by Categories	193
Table 2. 26 Framework Comparison by Governance & Policy Category	197
Table 2. 27 Framework Comparison by Risk Management Category	202
Table 2. 28 Framework Comparison by Operations and Service Management Category	206
Table 2. 29 Framework Comparison by Technical Control and Architecture Category	209
Table 2. 30 Framework Comparison by Monitoring and Detection Category	212
Table 2. 31 Framework Comparison by Incident Response and Recovery Category	217
Table 2. 32 Framework Comparison by Resilience and Continuity Category	220
Table 2. 33 Framework Comparison by Digital Trust and Culture Category	223
Table 2. 34 Framework Comparison by Third-Party and Supply Chain Category	226
Table 2. 35 Comparison by Audit and Compliance Category	231
Table 2. 36 Critical Comparison Across Previous Works	255
Table 2. 37 Summary Gaps on Previous works	264
Table 2. 38 Category Overview	270
Table 2. 39 Shows the Master Criteria to Build i-SOF	271
Table 2. 40 Indonesia Regulation mapping to i-SOF Criteria	292
Table 2. 41 Comparison of Maturity Model Level	300
Table 2. 42 Maturity Dimension Aligned with i-SOF Categories	305
Table 3. 1 Research Methodology	308
Table 3. 2 Maturity Level Definition	322
Table 3. 3 Decimal Scoring Guidelines	322
Table 3. 4 Weight Derivation Justification	323
Table 3. 5 Regulatory Impact Scoring Criteria	324
Table 3. 6 Operational Impact Scoring Criteria	324
Table 3. 7 Remediation Urgency Scoring Criteria	325
Table 3. 8 Priority Classification Thresholds	325
Table 3. 9 Assessment Scope Based on RACI Accountability	326
Table 3. 10 Prioritization Calculation Example - TC-08 (Device Redundancy)	326
Table 3. 11 Strategic Level Categories (30 Criteria)	332

Table 3. 12 Tactical Level Categories (30 Criteria)	332
Table 3. 13 Operational Level Categories (40 Criteria)	333
Table 3. 14 Mapping Between Three-Level and Six-Layer Architectures	334
Table 3. 15 Comparison of i-SOF Architectural Views	338
Table 3. 16 i-SOF Category Structure Summary	339
Table 3. 17 Criteria Catalog - Governance and Policy (GP) Category	340
Table 3. 18 Framework Cross-Walk Summary	341
Table 3. 19 Cross-Walk Example - GP-02 Security Policy Framework	341
Table 3. 20 Thematic Synthesis Statistics.....	342
Table 3. 21 i-SOF Criterion Specification Template Structure	344
Table 3. 22 Complete Criterion Specification Example - TC-08 Device Redundancy and Failover	345
Table 3. 23 RACI Matrix - Normal Change Management for Security Devices	352
Table 3. 24 i-SOF Security Operations KPIs.....	353
Table 3. 25 Process Steps Summary - Normal Change Management	354
Table 3. 26 Success Criteria Foundatoin	360
Table 4. 1 Design Requirements for i-SOF Measurement Framework	365
Table 4. 2 i-SOF Maturity Level Definitions.....	366
Table 4. 3 Decimal Scoring Guidelines	367
Table 4. 4 Maturity Dimensions Aligned with i-SOF Categories	368
Table 4. 5 Criterion-Specific Maturity Levels — TC-08 Device Redundancy and Failover	371
Table 4. 6 Mapping Between Three-Level and Six-Layer Architectures	372
Table 4. 7 i-SOF Category Structure Summary	375
Table 4. 8 Criteria Catalog — Governance and Policy (GP) Category	376
Table 4. 9 L3 Requirements and Implementation Guidelines Statistics	378
Table 4. 10 OS-01 Change Management for Security Devices	379
Table 4. 11 Implementation Guideline Types.....	380
Table 4. 12 Framework-to-Criteria Cross-Walk Summary	381
Table 4. 13 Cross-Walk Example — GP-02 Security Policy Framework.....	382
Table 4. 14 Thematic Synthesis Statistics.....	382

Table 4. 15 Assessment Scope.....	384
Table 4. 16 Assessment Results Summary by Category.....	385
Table 4. 17 Complete Gap Prioritization Results	388
Table 4. 18 Risk Assessment Register	391
Table 4. 19 Residual Risk Profile	395
Table 4. 20 Risk-to-Solution Mapping	397
Table 4. 21 Detailed Risk Analysis — RISK-TC-08.....	400
Table 4. 22 LOW Priority Risk Summary	403
Table 4. 23 Risk-to-Regulation Compliance Matrix.....	405
Table 4. 24 Expert Panel Composition	406
Table 4. 25 Expert Validation Results — Detailed Scores by Question	408
Table 4. 26 Expert Validation Results — Summary by Dimension	410
Table 4. 27 Expert Feedback Incorporation.....	413
Table 4. 28 FGD Participant Composition	414
Table 4. 29 FGD Evaluation Results — Detailed Scores	415
Table 4. 30 FGD Evaluation Results — Summary by Section.....	416
Table 4. 31 Combined Validation Summary.....	420
Table 4. 32 Phase 1 Remediation Plan.....	422
Table 4. 33 Phase 2 Remediation Plan.....	422
Table 4. 34 Phase Remediation 3.....	423
Table 4. 35 Phase 3 Remediation Plan.....	423
Table 4. 36 Implementation Roadmap Gantt Chart	424
Table 4. 37 Resource Requirements by Implementation Phase.....	425
Table 4. 38 Success Criteria Achievement Summary.....	426