

**DESIGN AND EVALUATION OF AN INTEGRATED RTBH–RBS GOVERNANCE-
AWARE MODEL FOR ILLEGAL TRAFFIC MITIGATION AT THE INDONESIA
INTERNET EXCHANGE (IIX)**

By

Muhammad Arif
22451067

MASTER’S DEGREE

in

MASTER PROGRAM IN INFORMATION TECHNOLOGY.
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sumatera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

January 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.

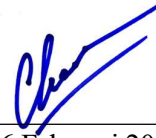
Muhammad Arif
Student



16 Februari 2026

Approved by:

Dr. Ir. Charles Lim, Msc., Bsc.
Thesis Advisor



16 Februari 2026

Dr. Ir. Mohammad Amin Soetomo, DSc
Thesis Co-advisor



16 Februari 2026

Acknowledged by:

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

Date

ABSTRACT

DESIGN AND EVALUATION OF AN INTEGRATED RTBH–RBS GOVERNANCE-AWARE MODEL FOR ILLEGAL TRAFFIC MITIGATION AT THE INDONESIA INTERNET EXCHANGE (IIX)

By

Muhammad Arif, Student

Dr. Ir. Charles Lim, Msc., Bsc., Advisor

Dr. Ir. Mohammad Amin Soetomo, DSc, Co-Advisor

SWISS GERMAN UNIVERSITY

This thesis addresses a governance gap in illegal traffic mitigation at the Indonesia Internet Exchange (IIX), where conventional Remote Triggered Black Hole (RTBH) practices can create unmanaged “zombie rules,” opaque decisions, and weak accountability. Using a three-phase Design Science Research (DSR) programme, Phase 1 derives governability requirements and workflow controls from operational failure modes and threat scenarios, including misuse, misconfiguration, and overbroad blocking risk. Phase 2 designs a sovereignty-aware, mandate-to-enforcement architecture that structures policy inputs into rule-based decisions and bounded enforcement under inter-domain constraints. Phase 3 integrates the Phase 1 workflow foundation and the Phase 2 architecture into an end-to-end RTBH–Rule-Based System (RBS) artefact and evaluates it using scenario-based walkthroughs, traceability and auditability checks, expert appraisal, and abuse-oriented analysis. The artefact introduces mandate verification, deterministic policy-to-rule translation, lifecycle controls such as Time-to-Live (TTL) with rollback, and evidence-first audit trails to make enforcement actions reconstructable and institutionally defensible. Results indicate improved controllability, traceability, and governance fitness compared with baseline manual RTBH practices, while explicitly documenting boundary conditions related to heterogeneous community propagation and member policies.

Keywords: RTBH, Rule-Based System, Internet Exchange Point, Design Science Research, Governance-Aware Mitigation.



© Copyright 2026
by Muhammad Arif, Student
All rights reserved

ACKNOWLEDGEMENTS

Alhamdulillahirabbil’alamin. All praise and gratitude be to Allah SWT, the Most Gracious and the Most Merciful, for His endless blessings, strength, and guidance, which enabled the author to complete this thesis entitled “Implementation and Evaluation of the Integrated RTBH–RBS Model for Illegal Traffic Mitigation in Indonesia Internet Exchange (IIX).” This thesis is submitted as a partial fulfillment of the requirements for the Master of Information Technology degree at Swiss German University.

The completion of this research would not have been possible without the support, mentorship, and encouragement of many individuals and institutions. I would like to extend my deepest appreciation to:

1. Dr. Ir. Charles Lim, M.Sc., B.Sc., my Thesis Advisor, for his invaluable patience, insightful guidance, and sharp technical critique throughout the research process.
2. Dr. Ir. Mohammad Amin Soetomo, D.Sc., my Co-Advisor, for his strategic direction and for constantly supporting me to finish the Thesis.
3. Dr. Eka Budiarto, S.T., M.Sc., Head of the Master of Information Technology Program, for his continuous encouragement, academic advice, and for facilitating a rigorous yet supportive learning environment for all graduate students.
4. The Management and Engineering Team of Indonesia Internet Exchange (IIX), for providing access to the operational context, data, and for their willingness to participate in the Focus Group Discussions. Their practical insights were the grounding force of this research.
5. My beloved family, for their endless prayers, sacrifices, and understanding during the many long nights and weekends spent on this research. Thank you for being my constant source of motivation.
6. My colleagues in the Master of Information Technology Class of 2024, for the shared knowledge, camaraderie, and moral support throughout our study journey.

Finally, I realize that this thesis is far from perfect. I welcome any constructive criticism and suggestions that may contribute to the further development of this research field. May this work provide benefits to the academic community, the industry, and the development of cybersecurity in Indonesia.

Tangerang, January 2026

Muhammad Arif



TABLE OF CONTENTS

STATEMENT BY THE AUTHOR	2
ABSTRACT	4
ACKNOWLEDGEMENTS	6
TABLE OF CONTENTS	8
LIST OF FIGURES	14
LIST OF TABLES	15
LIST OF PUBLICATIONS	16
CHAPTER 1. INTRODUCTION	19
1.1. Background	19
1.2. Research Problem.....	22
1.3. Research Objectives	24
1.3.1. Primary Objective	24
1.3.2. Supporting Objectives	25
1.4. Research Questions	29
1.5. Scope and Limitations	32
1.6. Significance of the Study	36
1.7. Research Roadmap	38
1.8. Hypotheses	41
1.9. Thesis Structure.....	44
CHAPTER 2. LITERATURE REVIEW	46
2.1. Introduction: Positioning the Literature Review in Design Science Research.....	46
2.2. Internet Exchange Points as Governance Sensitive Infrastructure	47
2.3. Illegal Traffic Mitigation: Technical Approaches and Governance Implications	51
2.4. Flow Specification (FlowSpec)	55
2.5. Scrubbing as a DDoS mitigation technique	57
2.6. DPI-based Filtering as a Mitigation Approach	60
2.7. Machine Learning–Based Automated Blocking	62
2.8. Cooperative/Collaborative Mitigation.....	65

2.9. Remotely Triggered Black Hole (RTBH): Practices, Limitations, and Critiques	68
2.10. Rule Based Systems as Governance and Decision Making Mechanisms	70
2.11. Governance, Accountability, and Auditability in Network Enforcement	73
2.12. Design Science Research in Information Systems: Foundations and Relevance	76
2.13. Evaluation in Design Science Research: From Performance to Design Validity	78
2.14. Previous Studies and Critical Review	81
2.14.1. Blackholing/RTBH at IXPs: Operational Practices and Risks.....	83
2.14.2. Orchestration and Rule Placement: Programmable Exchange Security.....	85
2.14.3. Governance and Decision-Making for Security Controls	87
2.15. Synthesis of Related Works and Identification of The Governance Gap.....	93
2.16. Research Gap and Design Opportunity	96
2.17. Implications of The Literature for The Proposed Research Framework	99
CHAPTER 3. RESEARCH METHODS.....	103
3.1. Research Framework.....	103
3.1.1. Framework Purpose and Scope	104
3.1.2. Evidence and Telemetry Inputs.....	105
3.1.3. Detection and Scoring Logic.....	106
3.1.4. Governance-Aware Rule-Based Decision Layer	107
3.1.5. Enforcement, Orchestration, and Collaboration Mechanisms.....	107
3.1.6. Evaluation Criteria and Success Conditions	108
3.1.7. Comparative Positioning of the Proposed Framework.....	109
3.2. Research Methodology.....	110
3.3. Analytical Methods	116
3.4. Data Collection Timeline	120
3.5. Instrument Development.....	124
3.6. Evaluation Method	128
3.7. Validation Methods	131
CHAPTER 4. RESULTS AND DISCUSSION - PHASE 1/PAPER 1.....	135
4.1. Chapter overview and Phase 1 positioning	135
4.2. Phase 1 problem focus and design objective (Phase 1 contribution statement).....	137
4.3. Phase 1 artefact: RTBH–RBS integrated architecture (blueprint).....	140
4.3.1. High-level architecture and data-to-enforcement flow.....	141
4.3.2. Policy interface: representing and operationalising policy inputs.....	142
4.3.3. Governance-by-design mechanisms embedded in the blueprint	143

4.4. Phase 1 threat model (PASTA-inspired) for an active mitigation pipeline.....	144
4.4.1. Threat surface by component	145
4.4.2. Risk class framing and why it matters	147
4.5. Phase 1 operational threat scenarios and control objectives	148
4.5.1. Scenario 1: False trigger due to misclassification (DNS-like bursts)	148
4.5.2. Scenario 2: Overbroad blackholing on shared prefixes (collateral damage).....	149
4.5.3. Scenario 3: Configuration drift and malformed BGP community propagation ...	150
4.5.4. Scenario 4: Privileged insider misuse and abuse of authority	150
4.5.5. Scenario 5: Regulatory pressure leading to overblocking.....	151
4.5.6. Cross-scenario synthesis: what the scenarios establish for Phase 1	152
4.6. Mitigation plan: safeguards across technical, operational, and governance layers	152
4.6.1. Technical safeguards	152
4.6.2. Operational safeguards.....	154
4.6.3. Governance safeguards	155
4.7. Phase 1 deployment risk assessment (risk matrix).....	158
4.7.1. Deployment options and qualitative risk levels	158
4.7.2. Why bare-metal in the core is rated high risk	159
4.7.3. Why segregated VM or container deployment is rated medium risk.....	159
4.7.4. Why partner ISP deployment is rated medium risk	160
4.7.5. Why cloud-based deployment with secure peering is rated low risk	160
4.7.6. Phase 1 interpretation and Phase 2 carry-forward.....	161
4.8. Phase 1 evaluation plan (testbed and metrics) as a bridge to Phase 3.....	161
4.8.1. Testbed topology and rationale	162
4.8.2. Metrics defined for Phase 1 and later Phase 3 use	164
4.8.3. How Phase 1 uses the plan as a bridge.....	165
4.9. Phase 1 outputs and handover to Phase 2 (continuity).....	166
4.9.1. Phase 1 outputs as design artefacts	166
4.9.2. Handover mapping to Phase 2.....	167
4.9.3. Implications for Phase 2 architecture decisions	168
CHAPTER 5. PHASE 2: RESULTS AND DISCUSSION	170
5.1. Chapter introduction and Phase 2 scope	170
5.1.1. Context: why sovereignty-aware becomes architectural at IXPs.....	170
5.1.2. Phase 2 position in the three-phase programme.....	171
5.1.3. Research question focus for Phase 2.....	172
5.1.4. Chapter objectives aligned to Paper 2.....	172
5.2. Background and related work (design foundations).....	174
5.2.1. Digital sovereignty and critical internet infrastructure.....	174
5.2.2. IXPs as leverage points and risk amplifiers	175
5.2.3. Routing-based enforcement and mitigation techniques	175

5.2.4. Rule-based decision components and governance	176
5.2.5. Link to Phase 1 governance workflow model	177
5.3. Research gap and Phase 2 design requirements	178
5.3.1. Gap statement (end-to-end architecture missing)	178
5.3.2. Requirement sources and normalisation approach	179
5.3.3. Architecture quality objectives (Phase 2 targets; Phase 3 evaluation)	180
5.4. Phase 2 method (Design Science Research)	182
5.4.1. Method rationale	182
5.4.2. DSR framing (artifact-oriented output)	183
5.4.3. DSR lifecycle activities (Paper 2)	184
5.4.4. Evidence strategy (documents and scenarios)	186
5.5. The sovereignty-aware mitigation architecture (core contribution)	187
5.5.1. Overview of the layered model	187
5.5.2. Policy input layer (mandate formalisation)	188
5.5.3. Rule and decision layer (deterministic translation and verification gates)	188
5.5.4. Enforcement layer (RTBH-oriented execution with extensibility)	189
5.5.5. Observability and audit layer (evidence production)	190
5.5.6. Explicit attack surface considerations (BGP risks and rollback constraints)	190
5.6. Integration with Phase 1 governance and workflow model (technical embedding)	191
5.6.1. Purpose of integration	192
5.6.2. Interface mapping logic (workflow to architecture)	192
5.6.3. Multi-stakeholder coordination constraints (autonomy, shared services, and evidence boundaries)	195
5.7. Phase 2 evaluation approach (scenario-based, architectural)	196
5.7.1. Why scenario-based evaluation in Phase 2	196
5.7.2. Scenario set used in Paper 2	196
5.7.3. Evaluation criteria (five criteria from Paper 2)	197
5.7.4. Output of Phase 2 evaluation (fitness and unresolved boundaries)	198
5.8. Chapter conclusion and handover to Chapter 6	199
CHAPTER 6. PHASE 3 INTEGRATION & EVALUATION (RESULTS AND DISCUSSION)	203
6.1. Overview & Phase 3 positioning	203
6.1.1. Chapter 6 as primary validation	203
6.1.2. Evaluation scope and boundaries	204
6.1.3. RQ6 framing and validation logic	205
6.1.4. Planned validation artefacts	205
6.2. Phase 3 integration design (RQ5)	206
6.2.1. Integration mapping to Phase 3 artefacts	207

6.2.2. Enforceable boundaries and integration logic	208
6.2.3. Boundary conditions and assumptions (H4)	209
6.3. Integrated artefact specification	210
6.3.1. Artefact scope.....	210
6.3.2. Layered specification	211
6.3.3. Evidence-first artefacts.....	212
6.3.4. Lifecycle and authorization controls	213
6.3.5. Evaluation readiness for RQ5 and H1–H3–H5	214
6.4. Evaluation design & measurement plan	214
6.4.1. Claim-level validation rule.....	214
6.4.2. Scenario execution plan	215
6.4.3. Metrics and measurements	216
6.4.4. Preparing tests for H1–H6.....	217
6.5. Results I — Scenario Execution Evidence (Walkthrough and Measurable Traces) ...	218
6.5.1. Scenario A: Lawful intervention (walkthrough evidence)	219
6.5.2. Scenario B: Large-scale multi-participant attacks (walkthrough evidence).....	220
6.5.3. Scenario C: Abuse of authority attempt (walkthrough evidence)	220
6.5.4. Measured traces and boundary conditions	221
6.6. Results II — Traceability, Auditability, and Coherence Checks	222
6.6.1. Chain-of-custody test results.....	223
6.6.2. Coherence check results	224
6.6.3. Auditability and regulator-style reconstructability	224
6.6.4. Boundary conditions observed in checks	225
6.7. Results III — Governance Fitness and Cross-Role Expert Appraisal.....	226
6.7.1. Cross-role appraisal evidence and dimensions	226
6.7.2. Triangulation results and cross-role interpretability	228
6.7.3. Design refinements and rigor-cycle anchoring	228
6.7.4. Link to RQ6 and hypotheses	229
6.8. Results IV — Threat Modeling and Abuse Analysis of Governance Controls.....	230
6.8.1. Threat modeling scope and method	230
6.8.2. Abuse cases and observed control behavior.....	231
6.8.3. Evidence binding and reconstructability under abuse.....	232
6.8.4. Link to RQ6, H3, and H4.....	233
6.9. Phase 3 Synthesis and Implications.....	233
6.9.1. Extent of Validation Against RQ6	234
6.9.2. Cross-Phase Evidence Synthesis	235
6.9.3. Extracted Design Knowledge and Theory-Building Output.....	236
6.9.4. Boundary Conditions and What Remains Deferred.....	238
6.10. Practical Implications and Deployment Readiness	240

CHAPTER 7. CONCLUSIONS AND RECOMMENDATIONS.....	241
7.1. Thesis-Level Conclusions and Core Argument.....	241
7.2. Consolidated Findings Across the Research Programme.....	242
7.3. Addressing the Research Questions Through Thesis Contributions	244
7.3.1. Artefact Design: From Mitigation Action to Governed Enforcement	245
7.3.2. Demonstrating Improvement Using Governance-First Criteria.....	245
7.3.3. Making Actions Attributable and Non-Repudiable.....	246
7.3.4. Transparency and Explainability.....	246
7.3.5. Bounding Scope, Duration, and Reversibility.....	247
7.3.6. Governance-Aware Enforcement Across the Full Decision Lifecycle	247
7.4. Boundary Conditions and Scope of Validity.....	248
7.5. Recommendations and Future Work.....	248
REFERENCES	250
GLOSSARY OF TERMS.....	257
CURRICULUM VITAE.....	260
APPENDIX A VERBATIM FGD WITH EXPERT	262
APPENDIX B EXPERT SHORT BIO - FGD	294
APPENDIX C FIGURES AND TABLES.....	295

LIST OF FIGURES

Figure 1.1 The Dual Role of the Internet Exchange Point (IXP).....	21
Figure 1.2. Fishbone Diagram: Root Causes of RTBH Governability Failure	24
Figure 2.1 Governance & Responsibility Swimlane Diagram: Actor Boundaries in IXP Mitigation	75
Figure 2.2 The Problem Space, Governance Gap, and Design Opportunity in IXP Mitigation	98
Figure 3.1 The Three-Cycle View of Design Science Research.....	112
Figure 3.2 The DSRM Process Model Adapted for Governance-Aware Mitigation	114
Figure 3.3 The Design Justification Arena: Synthesizing Inputs into Design Decisions	118
Figure 3.4 Research Timeline and Phasing: A 3-Semester DSR Trajectory.....	121
Figure 5.1 Phase 2 DSR activity-to-output map.....	185
Figure 5.2 Layered interaction of the sovereignty-aware architecture	187
Figure 5.3 Mapping governance workflow stages to architecture interfaces.....	193

LIST OF TABLES

Table 1.1 Research Objectives Mapping	27
Table 1.2 Research Questions–Phase–Chapter Placement Mapping	31
Table 1.3 Scope and Limitations	35
Table 1.4 Research Contribution and Validation Roadmap across Phases 1–3	39
Table 2.1. Internet Governance Actors and Leverage Matrix	48
Table 2.2 Governance-Centric Comparison of Mitigation Approaches	51
Table 2.3 Comparison of Governance Criteria in Conventional RTBH vs. RTBH–RBS Design	81
Table 2.4 Comparative summary table of previous studies	89
Table 3.1 Comparison of Related Frameworks and the Proposed Research Framework	110
Table 3.2. Research Instruments and Output Artefacts	124
Table 3.3. Artefact Traceability Matrix	127
Table 3.4. Evaluation & Validation Strategy Map	128
Table 3.5. Evaluation & Validation Strategy Map	131
Table 4.1 Summary of governance safeguards embedded in the RTBH–RBS mitigation pipeline	156
Table 4.2 Phase 1 IXP lane emulation elements	163
Table 4.3 Phase 1 metrics and measurement intent	165
Table 4.4 Phase 1 outputs as Phase 2 inputs	168
Table 5.1 Phase 2 scope and boundaries	172
Table 5.2 Design foundations and Phase 2 implications	177
Table 5.3 requirements and architectural realisation	181
Table 5.4 Layers, responsibilities, and artefacts	191
Table 5.5 Workflow stage, responsible actor, architecture component, evidence artefact produced	194
Table 5.6 Scenario-to-criteria coverage matrix	198
Table 5.7 Phase 2 outputs and Phase 3 validation targets	201
Table 6.1 Phase 3 validation strategy and evidence outputs	206
Table 6.2 Phase 1 controls mapped to Phase 2 layers and Phase 3 artefacts	207
Table 6.3 Integrated artefact specification and evidence outputs	211
Table 6.4 Claim-level validation rule, scenario coverage, and measurement evidence	217
Table 6.5 Scenario execution evidence bundles per scenario	218
Table 6.6 Metric extraction points per scenario	221
Table 6.7 Chain-of-custody evidence verification	223
Table 6.8 Reconstructability for regulator-style “why” questions	224
Table 6.9 Expert appraisal dimensions, role focus, and evidence inputs	227
Table 6.10 Threat scenarios, governance risks, and evidence-bound mitigations	232
Table 6.11 Phase 3 extracted principles and boundary conditions	234
Table 6.12 Sub-Chapter Mapping	239
Table 7.1 Thesis contributions and supporting evidence categories	243
Table 7.2 Governance-first pilot metrics and evidence outputs	245