

**DESIGNING INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK
FOR ENHANCE CYBER RESILIENCE MATURITY: A CASE STUDY ON THE
ONLINE APPLICATION OF BANK XYZ**

By

Guntur Pratomo
22451041

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

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.

Guntur Pratomo

Student

Date 15 February 2026

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. Maulahikmah Galinium S.Kom M.Sc

Dean of Faculty of Engineering & Information Technology

Date

The background of the abstract section features a large, light blue watermark of the letters 'SGU' with a registered trademark symbol (®) to the right. The word 'ABSTRACT' is centered over this watermark.

ABSTRACT

DESIGNING INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK FOR ENHANCE CYBER RESILIENCE MATURITY: A CASE STUDY ON THE ONLINE APPLICATION OF BANK XYZ

By

Guntur Pratomo

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

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

SWISS GERMAN UNIVERSITY

This thesis introduces the Risk Management-Cyber Resilience Maturity (RM-CRM) framework, integrating NIST RMF, STRIDE, NIST CSF 2.0, and NIST CREF for digital banking operations. The framework addresses gaps at Bank XYZ: unmeasurable cyber resilience, ad-hoc threat identification, compliance-driven controls, and inconsistent security implementation. Using design science methodology, the framework was validated through Focus Group Discussions with industry experts and Bank XYZ stakeholders. Application on

Bank XYZ's M-Banking platform demonstrates systematic threat identification, risk quantification, and maturity assessment across CREF goals. The framework aligns with Indonesian regulations (POJK, SEOJK, PBI, UU PDP), bridging international frameworks with local compliance requirements.

Keywords: cyber resilience, risk management, NIST CSF, STRIDE, digital banking, maturity assessment.





DEDICATION

This thesis is dedicated to:

Allah Subhanahu Wa Ta'ala

All praise belongs to You alone. Every word written, every obstacle overcome, and every moment of clarity throughout this journey has been by Your grace and mercy. You have been my source of strength when challenges seemed insurmountable, and my guide when the path forward appeared uncertain.

My Beloved Wife

For your unwavering patience during the countless late nights, your quiet encouragement when doubt crept in, and your steadfast belief in me even when I questioned myself. You carried the weight of our home so I could carry this academic burden. This achievement is as much yours as it is mine.

My Mother

For instilling in me the value of education, perseverance, and integrity. Your prayers have carried me further than any effort of my own ever could. Every sacrifice you made throughout my life has led to this moment.

My Late Father (Almarhum)

Though you are no longer here to witness this accomplishment, your voice still echoes in my heart urging me to work harder, to reach higher, and to never settle for mediocrity. I carry your dreams with me, and I hope this work honours your memory. Until we meet again, Papa.

"Indeed, with hardship comes ease." (Quran 94:6)

ACKNOWLEDGEMENTS

The completion of this thesis would not have been possible without the support, guidance, and encouragement of many individuals whom I wish to acknowledge.

First and foremost, I express my deepest gratitude to Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc, my thesis advisor, for his invaluable guidance, constructive feedback, and unwavering support throughout this research journey. His expertise in information technology and risk management has been instrumental in shaping the direction of this work.

I am equally grateful to Dr. Ir. Charles Lim, BSc., M.Sc, my co-advisor, whose deep knowledge in cybersecurity and critical insights challenged me to think more rigorously and approach problems from multiple perspectives. His patience in reviewing numerous drafts and his thoughtful suggestions have significantly strengthened this thesis.

I would also like to extend my appreciation to the faculty members of the Master of Information Technology programme at Swiss German University, whose stimulating coursework provided me with the theoretical foundation and analytical tools necessary to undertake this research.

My sincere thanks go to the management and staff of Bank XYZ for granting me access to conduct this case study and for their willingness to share valuable insights regarding their cyber resilience practices.

Finally, I thank my family and friends for their continuous encouragement and understanding throughout this demanding but rewarding endeavour.

TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR.....	Error! Bookmark not defined.
ABSTRACT.....	3
DEDICATION.....	6
TABLE OF CONTENTS.....	8
LIST OF FIGURES	13
LIST OF TABLES.....	14
CHAPTER 1 – INTRODUCTION	18
1.1 Background.....	18
1.2 Research Problem	23
1.2.1 Strategic Level Problem	24
1.2.2 Operational Level Problems	25
1.2.3 Technical Level Problem.....	26
1.2.4 Problem Synthesis	27
1.3 Research Objective	29
1.3.1 Research Objective Summary	31
1.4 Research Questions.....	31
1.4.1 Primary Research Question	32
1.4.2 Secondary Research Questions.....	32
1.5 Hypothesis.....	33
1.6 Research Scope and Limitation	34
1.7 Significance of Study	34
1.8 Thesis Structure	36
CHAPTER 2 - LITERATURE REVIEW	38
2.1. Role of Financial Institutions in Modern Company	38
2.1.1 Digital Transformation in Banking	39
2.1.2 Indonesia Banking Context	41
2.1.3 Financial Technology and Innovation	42
2.1.4 Emerging Challenges in Digital Banking.....	43
2.2 Summary of Bank XYZ.....	44
2.2.1 Digital Innovation as Core Business Strategy	45
2.2.2 The Cyber Resilience Imperative	45

2.2.3 Bank XYZ's Strategic Direction	47
2.2.4 Problem Identification and Research Scope	48
2.2.5 Digital Applications of Bank XYZ	53
2.2.6 Digital Application Architecture	56
2.2.7 The Necessity of System Understanding for Threat Identification	58
2.2.8 System Architecture	58
2.2.9 Data Flow Diagram	59
2.2.10 Role in Threat Identification	61
2.3. Assets	62
2.4 Threats	64
2.5 Vulnerabilities	64
2.6 Bank XYZ Risk Matrix	65
2.7 Risk Management	68
2.7.1 ISO 31000	69
2.7.2 NIST RMF	70
2.7.3 COSO ERM	72
2.7.4 FAIR (Factor Analysis of Information Risk)	73
2.7.5 ISO/IEC 27005	74
2.7.6 Critical Review of Risk Management Frameworks	75
2.8 Cyber Maturity	86
2.8.1 NIST CSF 2.0	87
2.8.2 CMMI (Capability Maturity Model Integration) for Cybersecurity	89
2.8.3 COBIT Maturity Model	91
2.8.4 ISO/IEC 21827 (SSE-CMM)	93
2.8.5 Cybersecurity Maturity Model Certification (CMMC)	96
2.8.6 Critical Review of Cyber Maturity	99
2.9 Cyber Resilience	106
2.9.1 NIST Cyber Resiliency Framework	108
2.9.2 MITRE Cyber Resilience Framework	112
2.9.3 Lockheed Martin Cyber Resiliency Level (CRL)	115
2.9.4 Critical Review of Cyber Resilience Frameworks	118
2.10 Threat Modelling	127
2.10.1 STRIDE	128
2.10.2 PASTA	129
2.10.3 DREAD	131
2.10.4 LINDDUN	133
2.10.5 Attack Trees	135
2.10.6 Critical Review of Threat Modelling Frameworks	136
2.11 Related Works	147
2.11.1 Comparative Analysis of Related Studies	156
2.11.2 Critical Analysis of Related Studies	164
2.11.3 Research Gap Summary and Integration Rationale	175
2.11.4 Design Science Research Alignment	180
CHAPTER 3 – RESEARCH METHODS	183

3.1. Research Methodology	183
3.1.1 Phase 1: Literature Review.....	184
3.1.2 Phase 2: Gap and Comparative Analysis.....	185
3.1.3 Phase 3: Design and Development Framework.....	188
3.1.4 Phase 4: Validation and Evaluation.....	189
3.2. Research Framework	191
3.3. Research Instrument.....	194
3.3.1 Data Collection and Analysis	195
3.3.2 Instrument Limitations	195
3.4. Design RM-CRM.....	195
3.4.1 Overview RM-CRM.....	197
3.4.2 Organizational Context and Regulatory Alignment.....	204
3.4.3 System Categorization and Threat Identification	207
3.4.4 Integrated Threat Analysis and Risk Assessment	210
3.4.5 Control Selection and Resilience Design	213
3.4.6 Cyber Resilience Maturity Assessment.....	217
3.4.7 Expert Validation.....	220
3.4.8 Expert Evaluation	221
3.4.9 Consensus Thresholds and Quality Criteria	223
3.4.10 Validation and Evaluation Data Analysis.....	223
CHAPTER 4 – RESULTS AND DISCUSSION.....	224
4.1 Introduction.....	224
4.1.1 Case Study Context	224
4.1.2 Assessment Scope	224
4.1.3 Chapter Structure.....	225
4.2 Organizational Context and Regulatory Alignment	226
4.2.1 Internal Document Review	226
4.2.2 Stakeholder Identification Results.....	227
4.2.3 Compliance Objectives and Regulatory Mapping.....	227
4.2.4 Compliance Gap Analysis	228
4.2.5 Risk Appetite and Tolerance Definition.....	229
4.2.6 Maturity Assessment Criteria Establishment	229
4.2.7 Phase 1 Outputs Summary.....	231
4.3 System Categorization and Threat Identification	231
4.3.1 System Architecture and Asset Identification	232
4.3.2 Data Flow Diagram Analysis	233
4.3.3 Trust Boundary Identification	233
4.3.4 STRIDE Methodology Application.....	234
4.3.5 Identified Threats by STRIDE Category.....	234
4.3.6 Comprehensive Threat Summary	236
4.3.7 Threat Distribution Analysis	237
4.3.8 Phase 2 Outputs Summary.....	238
4.4 Integrated Threat Analysis and Risk Assessment.....	238
4.4.1 Risk Assessment Methodology	239

4.4.2 STRIDE-to-Domain Mapping	241
4.4.3 Likelihood Assessment Scale	242
4.4.4 Impact Assessment Scale	243
4.4.5 Risk Determination Matrix	243
4.4.6 Comprehensive Risk Register	243
4.4.7 Risk Distribution Analysis	247
4.4.8 Risk Distribution by STRIDE Category	247
4.4.9 Risk Distribution by RM-CRM Domain	248
4.4.10 Critical Risk Analysis	248
4.4.11 Phase 3 Outputs Summary	249
4.5 Control Selection and Resilience Design	250
4.5.1 Control Selection Methodology	250
4.5.2 RM-CRM Control Framework Overview	250
4.5.3 Domain 1: Governance & Strategy (GS)	251
4.5.4 Domain 2: Risk Intelligence (RI)	252
4.5.5 Domain 3: Defense & Protection (DP)	253
4.5.6 Domain 4: Detection & Monitoring (DM)	253
4.5.7 Domain 5: Incident Response & Recovery (IR)	254
4.5.8 Domain 6: Continuous Improvement (CI)	255
4.5.9 Comprehensive Control Register	256
4.5.10 Risk-to-Control Traceability Matrix	259
4.5.11 Indonesian Regulatory Compliance Summary	261
4.5.14 Phase 4 Outputs Summary	261
4.6 Cyber Resilience Maturity Assessment	262
4.6.2 Assessment Results by Domain	263
4.6.3 Dimension Score Summary	274
4.6.4 Maturity Tier Determination	275
4.6.5 Gap Analysis and Improvement Priorities	276
4.7 Expert Validation	277
4.7.1 Expert Panel Composition	277
4.7.2 Validation Methodology	278
4.7.3 Quantitative Validation Results	278
4.7.4 Qualitative Feedback Analysis	279
4.7.5 Framework Refinements Based on Expert Feedback	280
4.7.6 Overall Framework Validity Assessment	281
4.8 Internal Stakeholder Evaluation	282
4.8.1 Internal Stakeholder Panel Composition	282
4.8.2 Evaluation Methodology	283
4.8.3 Quantitative Evaluation Results	283
4.8.4 Qualitative Feedback Analysis	284
4.8.5 Integration Requirements	285
4.8.6 Overall Feasibility Assessment	286
4.9 Improvement Roadmap and Recommendations	287
4.9.1 Gap Analysis Summary	287
4.9.2 Improvement Initiatives	288

4.9.3 Implementation Roadmap	289
4.9.4 Governance and Monitoring Recommendations	290
4.9.5 Resource Requirements Summary	290
4.9.6 Strategic Alignment with Organizational Cyber Resilience Roadmap	291
4.10 Discussion	293
4.10.1 Achievement of Research Objectives.....	294
4.10.2 Framework Validation.....	296
4.10.3 Contributions and Limitations	296
4.10.4 Result Summary	298
CHAPTER 5 – CONCLUSIONS AND RECOMMENDATIONS	300
5.1 Conclusions.....	300
5.2 Recommendations.....	303
5.3 Future Works	303
GLOSSARY	307
APPENDIX A.....	313
APPENDIX 1 – FGD External	313
APPENDIX 2 – FGD Internal	315
APPENDIX B	318
APPENDIX 1 – Regulatory Compliance Mapping	318
APPENDIX 2 - Detailed Risk Assessment Justification Tables	321
REFERENCES	342
CURRICULUM VITAE.....	349

LIST OF FIGURES

Figures	Page
Figure 1. 1 Cyber Resilience Gap	18
Figure 1. 2 Recovery Time After Cybersecurity Incident	19
Figure 1. 3 Breach Detection	20
Figure 1. 4 Cyber Risk Comparison	21
Figure 1. 5 Regional Confidence	22
Figure 1. 6 Fishbone Diagram Problem	28
Figure 2. 1 Mobile Bank Apps	53
Figure 2. 2 Digital App Bank XYZ Architecture	56
Figure 2. 3 Data Flow Diagram Bank XYZ	57
Figure 3. 1 Research Methodology	183
Figure 3. 2 RM-CRM Research Framework	192
Figure 3. 3 RM - CRM Framework Overview	197
Figure 1 External Attendance (1).....	313
Figure 2 External Attendance (2).....	314
Figure 3 External Expert (1)	314
Figure 4 External Expert (2)	315
Figure 5 External Questionnaire	315
Figure 6 Internal Attendance	316
Figure 7 Internal Expert	316
Figure 8 Internal Evaluation Questionnaire	317

LIST OF TABLES

Table	Page
Table 1. 1 Summarizes the research problems identified at Bank XYZ.....	29
Table 1. 2 Presents the alignment between identified problems and research objectives:	31
Table 2. 1 Bank XYZ Digital Banking Context Summary	48
Table 2. 2 Fishbone Analysis: Identified Problem Categories at Bank XYZ	49
Table 2. 3 Research Scope: Problem to Objective Mapping	51
Table 2. 4 Risk Impact Matrix	65
Table 2. 5 Comparative Analysis Risk Management Frameworks	78
Table 2. 6 Comparative Analysis of Cyber Maturity Assessment Framework	100
Table 2. 7 Comparison Cyber Resilience Framework	120
Table 2. 8 Comparison Threat Modelling Frameworks	139
Table 2. 9 Comparative Analysis Related Works	157
Table 2. 10 Critical Analysis Comparison	164
Table 2. 11 Consolidated Research Gap Analysis	175
Table 2. 12 Framework Complementary Coverage Analysis	177
Table 2. 13 Framework Selection Rationale Summary	179
Table 2. 14 Consolidated Thesis Positioning Summary	180
Table 2. 15 DSR Phases Alignment with Research Methodology and RM-CRM Framework	181
Table 2. 16 Research Objectives Alignment with DSR and RM-CRM Framework	181
Table 3. 1 Gap Analysis Summary and RM-CRM Framework Response	187
Table 3. 2 RM-CRM Unified Assessment Domain Architecture	200
Table 3. 3 RM-CRM Framework Phases Overview	201
Table 3. 4 RM-CRM Maturity Tier Definitions	202
Table 3. 5 Stakeholder Identification Framework	204
Table 3. 6 Indonesian Banking Regulatory Requirements	205
Table 3. 7 Risk Appetite Dimensions	205
Table 3. 8 RM-CRM Maturity Tier Definitions	206
Table 3. 9 RM-CRM Assessment Dimensions	206
Table 3. 10 CIA Impact Level Definitions	208
Table 3. 11 Data Flow Diagram Element Types	209
Table 3. 12 STRIDE Threat Categories and Security Properties	209
Table 3. 13 STRIDE-per-Element Applicability Matrix	210
Table 3. 14 Likelihood and Impact Assessment Scales	211
Table 3. 15 Risk Determination Matrix (Likelihood × Impact)	212
Table 3. 16 Resilience Goal Impact Assessment with Domain Mapping	212
Table 3. 17 Unified Control Integration Framework	214
Table 3. 18 STRIDE-to-Domain Mapping Framework	215
Table 3. 19 Regulatory Alignment Framework	216
Table 3. 20 RM-CRM Assessment Dimensions	217
Table 3. 21 Control Sufficiency Assessment Scale	218

Table 3. 22 Maturity Tier Mapping and Interpretation	218
Table 3. 23 RM-CRM Assessment Model Summary	219
Table 3. 24 External Expert Panel Composition Criteria	220
Table 3. 25 External Validation FGD Session Structure	221
Table 3. 26 Internal Expert Panel Composition	222
Table 3. 27 Internal Evaluation FGD Session Structure	222
Table 3. 28 Validation and Evaluation Quality Criteria	223
Table 4. 1 Chapter Structure Alignment with RM-CRM Framework Phases	225
Table 4. 2 Internal Document Review Summary	226
Table 4. 3 Identified Stakeholders and Framework Contributions	227
Table 4. 4 Regulatory Compliance Gap Analysis	228
Table 4. 5 RM-CRM Maturity Tier Definitions	229
Table 4. 6 Six Integrated Assessment Dimensions	230
Table 4. 7 M-Banking Asset Inventory by Functional Zone	232
Table 4. 8 Trust Boundaries and Data Flows	233
Table 4. 9 STRIDE-per-Element Applicability Matrix	234
Table 4. 10 Summary of Identified STRIDE Threats	236
Table 4. 11 Threat Distribution by STRIDE Category and Trust Boundary	237
Table 4. 12 Risk Measurement Input Mapping Framework	240
Table 4. 13 Evidence Source Triangulation Summary	240
Table 4. 14 STRIDE-to-RM-CRM Domain Mapping	241
Table 4. 15 Likelihood Assessment Scale	242
Table 4. 16 Impact Assessment Scale	243
Table 4. 17 Risk Determination Matrix (Likelihood × Impact)	243
Table 4. 18 M-Banking Application Comprehensive Risk Register	244
Table 4. 19 Risk Distribution by Priority Level	247
Table 4. 20 Risk Distribution by STRIDE Category	247
Table 4. 21 Risk Distribution by RM-CRM Domain	248
Table 4. 22 RM-CRM Control Framework Summary	250
Table 4. 23 Governance & Strategy Domain Controls	251
Table 4. 24 Risk Intelligence Domain Controls	252
Table 4. 25 Defense & Protection Domain Controls	253
Table 4. 26 Detection & Monitoring Domain Controls	254
Table 4. 27 Incident Response & Recovery Domain Controls	254
Table 4. 28 Continuous Improvement Domain Controls	255
Table 4. 29 RM-CRM Comprehensive Control Register	256
Table 4. 30 Critical and High Risk to Control Traceability Matrix	259
Table 4. 31 Regulatory Compliance Summary	261
Table 4. 32 Enhanced Control Sufficiency Assessment Scale with Evidence Requirements	263
Table 4. 33 Governance & Strategy Domain Assessment Results with Score Justification	263
Table 4. 34 Risk Intelligence Domain Assessment Results with Score Justification	265
Table 4. 35 Defense & Protection Domain Assessment Results with Score Justification	267
Table 4. 36 Detection & Monitoring Domain Assessment Results with Score Justification	269
Table 4. 37 Incident Response & Recovery Domain Assessment Results with Score Justification	271

Table 4. 38 Continuous Improvement Domain Assessment Results with Score Justification	273
Table 4. 39 Maturity Assessment Summary by Dimension	274
Table 4. 40 Maturity Tier Mapping and Interpretation	275
Table 4. 41 Gap Analysis and Improvement Priorities	276
Table 4. 42 External Expert Panel Composition	277
Table 4. 43 Quantitative Validation Results by Dimension	278
Table 4. 44 Framework Strengths Identified by Expert Panel	279
Table 4. 45 Areas for Improvement and Framework Responses	280
Table 4. 46 Overall Framework Validity Assessment	281
Table 4. 47 Internal Stakeholder Panel Composition	282
Table 4. 48 Quantitative Evaluation Results by Dimension	283
Table 4. 49 Implementation Strengths Identified by Internal Stakeholders	284
Table 4. 50 Implementation Challenges and Mitigation Strategies	285
Table 4. 51 Integration Requirements for Bank XYZ Implementation	285
Table 4. 52 Overall Framework Feasibility Assessment	286
Table 4. 53 Maturity Gap Analysis Summary	287
Table 4. 54 Prioritized Improvement Initiatives	288
Table 4. 55 Phased Implementation Roadmap	289
Table 4. 56 Resource Requirements Summary	290
Table 4. 57 Strategic Alignment: CIO Improvement Targets and RM-CRM Assessment Findings	291
Table 4. 58 Strategic Alignment Summary	293
Table 4. 59 Research Objectives Achievement Summary	294
Table 4. 60 Maturity Assessment Key Findings by Domain	294
Table 4. 61 Combined Validation Results	296
Table 4. 62 Research Contributions Summary	297
Table 4. 63 Research Limitations and Mitigation Strategies	298
Table 4. 64 Chapter 4 Results Summary following RM-CRM Framework	298
Table 1 Glossary Table	307
Table 2 Indonesian Banking Cyber Resilience Regulatory Framework	318
Table 3 RM-CRM Control to Regulatory Requirement Mapping	318
Table 4 Key Regulatory Requirements and Addressing Controls	321
Table 5 Risk Assessment Justification — S-01: Account Takeover via Credential Theft	322
Table 6 Risk Assessment Justification — S-02: Session Hijacking	322
Table 7 Risk Assessment Justification — S-03: API Spoofing	323
Table 8 Risk Assessment Justification — S-04: Mobile App Spoofing	324
Table 9 Risk Assessment Justification — S-05: Man-in-the-Middle Attack	324
Table 10 Risk Assessment Justification — T-01: Transaction Tampering	325
Table 11 Risk Assessment Justification — T-02: Database Tampering	326
Table 12 Risk Assessment Justification — T-03: Configuration Tampering	326
Table 13 Risk Assessment Justification — T-04: Code Tampering (Mobile)	327
Table 14 Risk Assessment Justification — T-05: API Request Tampering	328
Table 15 Risk Assessment Justification — R-01: Transaction Repudiation	328
Table 16 Risk Assessment Justification — R-02: Authentication Repudiation	329

Table 17 Risk Assessment Justification — R-03: Admin Action Repudiation	330
Table 18 Risk Assessment Justification — R-04: Audit Log Tampering	330
Table 19 Risk Assessment Justification — I-01: Customer Data Breach	331
Table 20 Risk Assessment Justification — I-01: Customer Data Breach	332
Table 21 Risk Assessment Justification — I-03: Network Traffic Interception	332
Table 22 Risk Assessment Justification — I-04: Error Message Information Leakage.....	333
Table 23 Risk Assessment Justification — I-05: Insider Data Exfiltration.....	334
Table 24 Risk Assessment Justification — D-01: Volumetric DDoS Attack	334
Table 25 Risk Assessment Justification — D-02: Application-Layer DoS.....	335
Table 26 Risk Assessment Justification — D-03: Database Exhaustion.....	336
Table 27 Risk Assessment Justification — D-04: Account Lockout Attack.....	336
Table 28 Risk Assessment Justification — D-05: CBS Integration Disruption	337
Table 29 Risk Assessment Justification — E-01: SQL Injection Privilege Escalation.....	338
Table 30 Risk Assessment Justification — E-02: API Authorization Bypass	338
Table 31 Risk Assessment Justification — E-03: Privileged Credential Compromise	339
Table 32 Risk Assessment Justification — E-04: Insecure Direct Object Reference	340
Table 33 Risk Assessment Justification — E-05: Root/Jailbreak Exploitation.....	340

