

**KUBERNETES RISK MANAGEMENT: A FRAMEWORK TO ASSESS
KUBERNETES SECURITY RISK IN BANK XYZ**

By
HARTA DEDDY IRAWAN
22351036

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 Thesis Defense on 5 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.

HARTA DEDDY IRAWAN

Student

Date

Approved by:

Dr. Ir. Charles Lim BSc., MSc.

Thesis Advisor

Date

Dr. Ir. Mohammad A Soetomo, DSc

Thesis Co-Advisor

Date

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

Dean of Faculty of Engineering and
Information Technology

Date

ABSTRACT

KUBERNETES RISK MANAGEMENT: A FRAMEWORK TO ASSESS KUBERNETES SECURITY RISK IN BANK XYZ

By

HARTA DEDDY IRAWAN

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

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

SWISS GERMAN UNIVERSITY

This thesis introduces Kube-RMF, a risk assessment framework designed to address the unique security challenges of Kubernetes in cloud environments. Kubernetes, as a cornerstone of modern containerized application deployments, introduces complex security risks, particularly for small banks navigating digital transformation. The Kube-RMF framework integrates and extends established methodologies, such as OCTAVE Allegro and NIST SP 800-30, while focusing on Kubernetes-specific security concerns. It operates through four iterative phases: Preparation, Asset Identification, Risk Identification & Quantification, and Mitigation Planning. The framework's practical application is validated through a case study at Bank XYZ, an Indonesian financial institution utilizing Amazon Elastic Kubernetes Service (EKS). Results demonstrate Kube-RMF's capability to identify critical risks, prioritize vulnerabilities, and recommend actionable mitigation strategies, adhering to CIS Kubernetes Security Guidelines. This research bridges gaps in traditional risk frameworks, offering a tailored, iterative approach to Kubernetes-based cloud systems, especially for small and mid-sized financial institutions.

Risk Management Framework: kubernetes, aws eks, cloud risk, attack tree, risk analysis

© copyright 2025
by Harta Dedy Irawan
All rights reserved

DEDICATION

I dedicate this work to Almighty God, for His endless blessings, guidance, and strength
throughout this journey.

To my beloved wife, whose unwavering support, patience, and love have been my anchor and
inspiration. This achievement is as much yours as it is mine.

And to Indonesia, the country I deeply love, and its growing field of cybersecurity, may this
contribution help pave the way for a more secure and innovative future.

ACKNOWLEDGEMENT

I wish to express my heartfelt gratitude to my advisor, Dr. Ir. Charles Lim BSc., MSc., and co-advisor, Dr. Ir. Mohammad A 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 my superior at Bank XYZ, whose encouragement and support made it possible for me to pursue this academic endeavor alongside my professional responsibilities. Their understanding and guidance 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. This accomplishment would not have been possible without you by my side.

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, particularly in Indonesia.

Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	12
LIST OF FIGURES	15
LIST OF TABLES	17
LIST OF EQUATIONS	18
1. INTRODUCTION	19
1.1 Introduction	19
1.2 Problem Statement	24
1.3 Research Objective	25
1.4 Research Question	26
1.5 Hypothesis	26
1.6 Research Scope and Limitation	27
1.7 Significance of Study	27
1.8 Thesis Structure	28
2. LITERATURE REVIEW	29
2.1 Banking Business	29
2.1.1 Traditional Banking and its transformation	30

2.1.2	Digital Banking	31
2.2	A summary of Bank XYZ	33
2.2.1	Bank XYZ's Strategic Direction and Policies	34
2.2.2	Bank XYZ Risk Governance, Risk Management and Risk Assessment	36
2.2.2.1	Risk Appetite and Risk Tolerance	39
2.2.2.2	Key Risk Indicator	42
2.2.2.3	Risk Scenario	43
2.3	Banking Regulatory	46
2.3.1	Basel III and Its Adoption in Indonesia	47
2.3.2	Indonesian Regulations for Information Technology in General Banks	48
2.3.2.1	OJK Cyber Security Maturity Self Assessment	49
2.4	Technology Adoption in Digital Banking of Bank XYZ	50
2.4.1	Microservices in Digital Banking	50
2.4.2	The Role of Kubernetes in Microservices	51
2.4.3	The Role of Kubernetes in Bank XYZ	52
2.4.4	Containerization	53
2.4.4.1	Container Technology Architecture	53
2.4.4.2	Comparison Between Virtual Machines and Containers . . .	54
2.4.5	Kubernetes	55
2.4.6	Assets in Kubernetes	57
2.4.6.1	Control Plane Assets	57
2.4.6.2	Worker Node Assets	58
2.4.6.3	Workload Assets	58
2.4.6.4	Networking Assets	58
2.4.6.5	Storage Assets	58
2.4.6.6	Configuration Assets	59
2.4.7	Cloud Computing	60
2.4.8	Amazon Elastic Kubernetes Service (Amazon EKS)	62
2.4.8.1	AWS EKS Shared Responsibility Model	64
2.4.9	CIS Amazon Elastic Kubernetes Services Benchmark	64
2.4.10	AWS Organization, AWS Organizational Unit (OU) and AWS Accounts	65
2.4.10.1	AWS Organization	66

2.4.10.2	AWS Organization Unit	66
2.4.10.3	AWS Accounts	67
2.4.11	Cloud Architecture of Bank XYZ	68
2.4.12	DevOps	73
2.4.12.1	DevOps in Kubernetes Environments	73
2.4.12.2	DevSecOps	73
2.4.12.3	DevSecOps in Kubernetes Security	73
2.5	Security Risks in the Banking Sector	74
2.5.1	Risk in Containerization and Kubernetes Adoption	75
2.5.2	Security Risks in Containerized Environments	76
2.5.2.1	Container Risks	76
2.5.2.2	Image and Registry Risks	76
2.5.2.3	Orchestrator-Specific Risks	77
2.5.2.4	Host OS Risks	77
2.5.2.5	Mapping NIST SP 800-190 Risks to Kubernetes Environments	78
2.5.3	Security Risks in Kubernetes Environments	82
2.5.3.1	General Security Risk	82
2.5.3.2	Pod-Level Security Risks	83
2.5.3.3	Networking Vulnerabilities	83
2.5.3.4	Runtime Security Challenges	83
2.5.3.5	Threat Actors and Attack Vectors	84
2.5.3.6	OWASP Top 10 Kubernetes Risk	84
2.5.3.7	Case Studies in Kubernetes Security	86
2.5.3.8	Case Study 1: Cryptojacking Attack on Tesla's Kubernetes Infrastructure	86
2.5.3.9	Case Study 3: Bank XYZ's Kubernetes Deployment	87
2.5.4	Cloud Managed Kubernetes Services Security Risk	88
2.5.5	Security Risk in DevOps	90
2.6	Risk Management Framework	90
2.6.1	ISO27005	91
2.6.2	NIST SP 800-30	91
2.6.3	CRAMM	93

2.6.4	CORAS	94
2.6.5	OCTAVE Allegro	95
2.6.6	COBIT 5	97
2.6.7	Risk IT Framework	98
2.6.8	Cloud Octagon Model	100
2.6.9	Cloud Control Matrix	101
2.6.10	Kubernetes Common Configuration Scoring System KCCSS	102
2.6.11	Comparison of Industry Derived Risk Management Framework	103
2.6.12	ERMOCTAVE	104
2.6.13	Risk contagion based framework	106
2.6.14	CSCCRA (Cyber Supply Chain Cloud Risk Assessment)	107
2.6.15	Threat Modeling	109
2.6.15.1	STRIDE	109
2.6.15.2	PASTA	110
2.6.15.3	TRIKE	111
2.6.15.4	Cyber Kill Chain	111
2.6.15.5	MITRE ATT&CK	113
2.6.15.6	Attack Tree Analysis	115
2.6.16	Risk Flow Model	115
2.6.17	Quantitative Risk Assessment Metrics	117
2.6.17.1	Single Loss Expectancy (SLE)	119
2.6.17.2	Annual Rate of Occurrence (ARO)	119
2.6.17.3	Annual Loss Expectancy (ALE)	120
2.6.18	Measurement in Information Security: The ISO/IEC 27004:2016 Framework	120
2.6.19	Tools for Assessing Security in Kubernetes Environments	122
2.6.19.1	AWS Inspector	122
2.6.19.2	Kube-bench	123
2.6.19.3	Trivy	124
2.6.19.4	Kube-linter	125
2.6.19.5	Kube-hunter	125
2.6.19.6	Open Policy Agent (OPA)	126

2.7	Related Works	128
2.7.1	Functionality Comparison of Risk Management Frameworks	136
2.7.2	Threat Model Selection	138
2.7.2.1	Evaluation and Selection Criteria	138
2.7.2.2	Comparative Advantage Over Other Models	139
2.7.2.3	Attack Tree Analysis: A Hierarchical and Scalable Model	139
2.7.2.4	Limitations of Alternative Models	140
2.7.3	Comparison of Kubernetes Security Tool	142
2.8	Proposed Framework Kube-RMF	146
2.8.1	Kubernetes Configuration Testing and Validation Methodology	154
3.	RESEARCH METHODS	157
3.1	Research Methodology	157
3.2	Research Framework	159
3.3	Research Instrument	160
3.3.1	Data Collection and Analysis	160
3.3.2	Instrument Limitations	160
3.4	Development of Kube-RMF	160
3.4.1	Overview of Kube-RMF	161
3.4.2	Preparation Phase	161
3.4.2.1	Stakeholder Identification	162
3.4.2.2	Compliance Objectives	162
3.4.2.3	Risk Measurement Criteria	163
3.4.2.4	Risk Ranking Weight in Risk Measurement Criteria	166
3.4.3	Asset Identification	166
3.4.3.1	Asset Profiling	167
3.4.3.2	Configuration Analysis	172
3.4.4	Risk Identification & Quantification	172
3.4.4.1	Compliance Gap Analysis	173
3.4.4.2	Threat Analysis	176
3.4.4.3	Risk Analysis and Quantification	177
3.4.5	Mitigation Planning	180
3.4.6	Business Impact Analysis (BIA)	181

3.4.6.1	Key Risk Indicators (KRIs)	182
3.5	Tools and Techniques	183
3.5.1	AWS Inspector	183
3.5.2	Kube-bench	183
3.6	Evaluation	184
3.7	Validation	185
3.7.1	Focus Group Discussion (FGD) Framework Validation	185
4.	Results and Discussion	195
4.1	Introduction	195
4.1.1	Preparation Phase	195
4.1.1.1	Stakeholder Identification Process	195
4.1.1.2	Compliance Objective Process	196
4.1.1.3	Risk Measurement Criteria Process	196
4.1.2	Asset Identification Phase	197
4.1.2.1	Asset Profiling Process	197
4.1.2.2	Configuration Analysis	198
4.1.3	Compliance Gap Analysis	199
4.1.3.1	Staging Environment	199
4.1.3.2	Production Environment	200
4.1.3.3	Compliance Modifier Impact	200
4.1.3.4	Key Observations	201
4.1.4	Threat Analysis	202
4.1.4.1	Worker Node Exploitation	202
4.1.4.2	Control Plane Exploitation	204
4.1.4.3	Exploit Container Image Vulnerabilities	206
4.1.4.4	Misconfigured Network Policies	208
4.1.4.5	Lack of Centralized Policy Enforcement	209
4.1.4.6	Summary of Threats	210
4.1.5	Risk Analysis	212
4.1.5.1	Risk Distribution	212
4.1.6	Business Impact Analysis	213
4.1.7	Key Risk Indicator	217

4.1.8	Mitigation Strategies	219
4.1.9	Policy Development	219
4.1.10	Guideline Development	220
4.2	Framework Validation	221
4.2.1	FGD Results and Analysis	223
5.	CONCLUSION AND RECOMMENDATIONS	227
5.1	Conclusions and Implications	227
5.2	Recommendations	228
	REFERENCES	238
A.	Curriculum Vitae	239
A.	Appendix A.1: Kubernetes Security Policy	241
B.	Appendix B.1: Kubernetes Security Guidelines	243

List of Figures

1.1	Financial services leaders’ perspectives on cloud adoption, security, and compliance (Egnyte, 2024).	20
1.2	Bank XYZ’s Dual Banking Operations: Traditional vs. Digital	23
1.3	Security concerns in Kubernetes environments, highlighting misconfigurations (53%), general security concerns (46%), and vulnerability worries (28%) (RedHat, 2022a).	24
1.4	Fishbone Diagram - Kubernetes Security Risks at Bank XYZ	25
2.1	Cyber resilience inherent risk assessment 2023 of Bank XYZ	49
2.2	Cybersecurity maturity level-assessment 2023 of Bank XYZ	50
2.3	Container Technology Architecture (adopted from NIST SP 800-190 Souppaya et al. (2017))	54
2.4	Comparison of Virtual Machines and Containers (adopted from NIST SP 800-190 Souppaya et al. (2017))	55
2.5	Kubernetes cluster architecture by CNCF (2024)	57
2.6	Cloud Computing Models by NIST illustrated by Mell and Grance (2011)	60
2.7	EKS basic flow by AWS (b)	63
2.8	EKS Shared Responsibility Model by AWS (a)	64
2.9	Example of AWS Organization Design Diagram by AWS (2024c)	66
2.10	AWS Organization Unit example by AWS (2024b)	67
2.11	AWS Organization Design of Bank XYZ	70
2.12	AWS Intra Account Architecture Diagram of Bank XYZ	71
2.13	Inbound Internet AWS Cloud Architecture of Bank XYZ	71
2.14	Outbound Internet AWS Cloud Architecture of Bank XYZ	72
2.15	Multi DC AWS Cloud Architecture of Bank XYZ	72
2.16	OWASP Top 10 mapping to Kubernetes by Sysdig (2023)	85
2.17	ISO72005 process drawn by ISO	92

2.18	NIST SP 800-30 process drawn by Irsheid et al. (2022)	93
2.19	CRAMM process	94
2.20	CORAS process drawn by SINTEF Digital (2025)	95
2.21	OCTAVE Allegro process by Irsheid et al. (2022)	96
2.22	COBIT 5 principles by Irsheid et al. (2022)	98
2.23	Risk IT Risk Management Workflow by ISACA (2020)	100
2.24	Example of STRIDE illustrated by Jacob (2023)	110
2.25	Cyber Kill Chain threat model by Martin (2011)	112
2.26	MITRE ATT&CK tactics by Mitre	114
2.27	Basic attack tree model proposed by Schneier (1999)	115
2.28	Risk Flow Model: Relationship between management, assets, vulnerabilities, threats, controls, and risks illustrated by Maniscalch (2010).	116
2.29	Integration of Quantitative Risk Metrics in Risk Flow. The diagram demonstrates the relationships between management, assets, controls, threats, and risk metrics (SLE, ARO, ALE) by Maniscalch (2010).	117
3.1	Research Methodology	157
3.2	Kube-RMF Research Framework	159
3.3	Kube RMF Framework	161
3.4	Kube RMF Preparation Phase	162
3.5	Risk Heat Map Based on Impact and Likelihood	164
3.6	Kube RMF Asset Identification Phase	167
3.7	Kube RMF Preparation Phase	173
3.8	Kube RMF Preparation Phase	181
4.1	Attack Tree: Worker Node Exploitation	203
4.2	Attack Tree: Break Out of Containerized Environments	204
4.3	Attack Tree: Persistent Control Plane Access	205
4.4	Attack Tree: Abuse Excessive Permissions	206
4.5	Attack Tree: Exploit Vulnerabilities in Public Container Images	207
4.6	Attack Tree: Introduce Malicious or Backdoored Images	208
4.7	Attack Tree: Exploit Lack of Network Segmentation	209
4.8	Attack Tree: Exploit Configuration Drift	210

4.9 Risk Distribution by Priority Level

212

List of Tables

2.1	Risk Ranking Based on Impact	37
2.2	Risk Appetite and Risk Tolerance Levels define by (MAS, 2024)	40
2.3	Information Technology Complexity Based on Core and Supporting Applications define by (MAS, 2024)	41
2.4	Example Risk Scenarios for Kubernetes Mapped to Strategic Goals based on Bank XYZ Bank Business Plan 2024 - 2026	44
2.5	Risk Levels Based on Cyberattack Incidents defined in (MAS, 2024)	45
2.6	Risk Levels Based on Data Leakage Incidents defined in (MAS, 2024)	45
2.7	Assets in Kubernetes, summarizing the key components and their roles in the Kubernetes ecosystem.	59
2.8	Mapping NIST SP 800-190 Risks to Kubernetes Examples	79
2.9	Comparison Table between OCTAVE and OCTAVE allegro	96
2.10	Comparison Table between Industry Derived Risk Management Frameworks .	105
2.11	Comparison of Information Security Risk Management Models for Cloud Hosted Systems	135
2.12	Functionality Comparison of Risk Management Frameworks with a Focus on Kube-RMF	137
2.13	Comparison of Kubernetes Security Tools	143
2.14	Frameworks Main Process Mapping	153
2.15	Frameworks Sub Process Mapping	156
3.1	Risk Matrix Based on Impact and Likelihood	163
3.2	Asset Categorization	168
3.3	Criteria for FGD Participant Selection	186
3.5	Indicators Tied to Kube-RMF and Bank XYZ’s Needs	187
3.6	Mapping Indicators to Success Criteria	189
3.8	FGD Questions Based on Kube-RMF Indicators	190

4.1	Calculated Asset Values (AV) for Kubernetes Assets	198
4.2	Kube-bench Results Summary	199
4.3	Compliance Gap and Modifier for Identified Components	202
4.4	Summary of Kubernetes Threat Analysis	211
4.6	Exposure Factor (EF) Values for Kubernetes Risk Scenarios	213
4.7	AV, EF, and SLE for Kubernetes Assets (IDR)	214
4.8	Rationale for ARO Values	215
4.9	SLE, ARO, and ALE for Kubernetes Assets (IDR)	217
4.10	Key Risk Indicators (KRIs) for Kubernetes Security	218
4.11	Key Components of the Kubernetes Security Policy	220
4.12	Profiles of FGD Experts	221
4.5	Risk Analysis and Adjusted Risk Score (RSk) with Risk ID, Asset, and Environment	225
4.13	FGD Responses from experts	226

List of Equations

2.1 Annual Loss Expectancy (ALE) Formula	118
2.2 Single Loss Expectancy (SLE) calculation: $SLE = AV \times EF$	119
2.3 Annualized Rate of Occurrence (ARO) calculation: $ARO = \text{Number of Occurrences}$ / Time Period in Years	119
2.4 Annual Loss Expectancy (ALE) calculation: $ALE = SLE \times ARO$	120
3.1 Risk Rating Score (RRS) calculation: $RRS = \text{Impact Value} \times \text{Likelihood Value}$. .	164
3.2 Risk Rating (Rr) definition: $Rr = \text{Impact Ranking}$	166
3.3 Critical Asset Value (AV_{critical}) calculation: $AV_{\text{critical}} = \text{Revenue Dependency}$ (Downtime) + Operational Cost + Recovery Cost	170
3.4 Non-Critical Asset Value ($AV_{\text{non-critical}}$) calculation: $AV_{\text{non-critical}} = \text{Operational Cost}$ + Recovery Cost	170
3.5 Daily Revenue Dependency calculation: $\text{Daily Revenue Dependency} = (\text{Annual}$ $\text{Revenue} \times \text{Dependency Percentage}) / 365$	170
3.6 Revenue Dependency calculation: $\text{Revenue Dependency} = \text{Daily Revenue}$ $\text{Dependency} \times \text{Downtime Days}$	171
3.7 Compliance Gap (Cg) calculation: $Cg = (\text{Non-Compliant Controls} / \text{Total Controls}$ $\text{Assessed}) \times 100$	174
3.8 Compliance Modifier (Cm) calculation: $Cm = 1 + (Cg / 100)$	174
3.9 Adjusted Risk Score (RSk) calculation: $RSk = RRS \times Cm \times Rr$	178