

**BANK INDONESIA'S IT AUDIT GUIDELINES FOR PAYMENT SERVICE
PROVIDERS IN THE SME CATEGORY: AN INTEGRATED ISO 27001:2022
ANNEX A, AND CLOUD-BASED SOLUTION ARCHITECTURE DESIGN**

By

Suarjan
22451014

MASTER'S DEGREE

in

DATA SCIENCE CYBER SECURITY - 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 the Thesis Defense on 15 August 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.

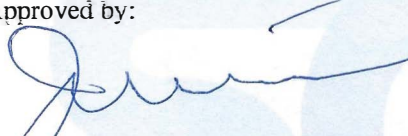

Suarjar

Student

28 AUGUST 2025

Date

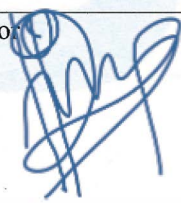
Approved by:


Dr. Ir. Moh. A. Amin Soetomo. S.T., M.Sc

Thesis Advisor

Aug 28th '25

Date


Dr. Ir. Heru Purnomo Iung, M.Eng

Thesis Co-Advisor

29 Aug 2025

Date

Dr. Maulahikmah Galinium S.Kom M.Sc

Dean of Faculty of Engineering and Information Technology

Date

Suarian

ABSTRACT

BANK INDONESIA'S IT AUDIT GUIDELINES FOR PAYMENT SERVICE PROVIDERS IN THE SME CATEGORY: AN INTEGRATED ISO 27001:2022 ANNEX A, AND CLOUD-BASED SOLUTION ARCHITECTURE DESIGN

By

Suarjan

Dr. Ir. Moh. A. Amin Soetomo, S.T., M.Sc, Advisor

Dr. Ir. Heru Purnomo Ipung, M.Eng, Co-Advisor

SWISS GERMAN UNIVERSITY

Indonesia's Small-Medium Enterprises (SMEs) face significant challenges complying with Bank Indonesia's (BI) stringent Payment Service Provider licensing requirements, including cybersecurity mandates (BI 23/6/PBI/2021). This study addresses these barriers by designing a cost-efficient cloud-based solution architecture that harmonizes with ISO 27001:2022 Annex A, and cloud-based to streamline compliance for resource-constrained SMEs. The framework helps prepare SMEs to face IT audits with guidelines that have been adjusted between Bank Indonesia requirements and ISO 27001:2022 Annex A control and replaces complex enterprise architectures with a lightweight, cloud-centric model, leveraging Indonesian cloud providers but still met the requirement from Bank Indonesia. Validation through SME pilot studies demonstrated a reduction in compliance costs compared to traditional approaches, achieved through open-source tools and hybrid cloud deployments. This research contributes to practical implementation guide for SMEs, and cloud-based solution architecture design met by Bank Indonesia requirement. By bridging regulatory complexity with SME realities, this work fosters inclusive growth in Indonesia's digital economy while advancing secure, scalable payment ecosystems.

Keywords: Bank Indonesia Regulations; Payment Service Providers (PSPs); Small-Medium Enterprises (SMEs); Solution Architecture Design; ISO/IEC 27001:2022 Annex A Controls.





DEDICATION

I dedicate this work to Allah SWT, my beloved mother and late father, my beloved wife, my beloved children, my beloved siblings, all my family, my friends, my leader and my company Tjakrabirawa.



ACKNOWLEDGEMENT

I would like to thank my beloved mother, my beloved wife, my beloved children, and my beloved siblings. With their prayers and encouragement, I was able to complete my education and this thesis.

I am also very grateful to Dr. Dr. Ir. Moh. A. Amin Soetomo, S.T., M.Sc., and Dr. Ir. Heru Purnomo Ipung, M.Eng., who have provided advice, support, and guidance throughout the process of this thesis.

I would also like to thank Amien Harisen, the leader of Tjakrabirawa, for providing me with support and resources throughout my education and for being a positive role model, both inside and outside of work. I also thank all my colleagues at Tjakrabirawa for their unwavering support.

Finally, I would like to express my gratitude to my colleagues, professionals, and friends, especially those in Batch 34 of MIT. Without you, this course would not have been as interesting.

TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	6
ACKNOWLEDGEMENT	7
TABLE OF CONTENTS	8
LIST OF FIGURES	11
LIST OF TABLES	12
CHAPTER 1 – INTRODUCTION	14
1.1 Background.....	14
1.2 Research Problem.....	19
1.3 Research Objective	21
1.4 Research Questions	21
1.5 Hypothesis	22
1.6 Research Scope and Limitation.....	22
1.7 Significance of Study	22
1.8 Thesis Structure	22
CHAPTER 2 – LITERATURE REVIEW.....	24
2.1 Small Medium Enterprise (SME).....	24
2.1.1 SME Regulation Peraturan Pemerintah No. 7/2021	27
2.1.2 PT XYZ	30
2.2 Bank Indonesia (BI)	31
2.2.1 Bank Indonesia Regulation No. 23/6/PBI/2021	32
2.2.2 Bank Indonesia Payment Service Provider Category	33
2.2.3 Bank Indonesia's Capability System Requirements for PSP	35
2.3 ISO/IEC 27001:2022	38
2.4 Badan Siber dan Sandi Negara Regulation No. 8 Tahun 2020.....	42
2.5 Cloud-Based Solutions Architecture	43
2.6 The Open Group Architecture Framework (TOGAF).....	45
2.7 System Analysis & Design (SAD)	47

2.8	IT Infrastructure Library (ITIL).....	47
2.9	Payment Card Industry Data Security Standard (PCI DSS).....	49
2.10	Related Works.....	50
	CHAPTER 3 – RESEARCH METHODS	58
3.1	Research Framework	58
3.2	Literature Review	58
3.3	Standard Comparison	59
3.4	Gap Analysis.....	59
3.5	IT Audit Guideline Creation	59
3.6	Solution Architecture Design Creation.....	59
3.7	Implementation.....	61
3.8	Validation.....	61
	CHAPTER 4 – IMPLEMENTATION AND RESULTS	63
4.1	Standard Comparison	63
4.2	Gap Analysis.....	64
4.3	IT Audit Guideline Creation.....	65
4.3.1	Data confidentiality.....	66
4.3.2	System and data integrity	73
4.3.3	System and data two-factor authentication	76
4.3.4	Prevention of denial of transactions that have been carried out (non-repudiation)	78
4.3.5	System availability	79
4.3.6	The existence of systems and procedures for conducting audit trails.....	83
4.3.7	The existence of internal policies and procedures for the operation of information systems and human resources	85
4.3.8	The fulfillment of aspects of security and reliability of the system and/or network including networks provided by other parties.....	90
4.3.9	The existence of a Business Continuity Plan (BCP) that can guarantee the continuity of the implementation of fund management activities. The BCP includes preventive measures and disaster recovery plans in the event of an emergency or disruption that results in the main system for implementing fund management activities being unusable	91
4.4	Solution Architecture Design Creation.....	93
4.4.1	Planning.....	93
4.4.2	Analysis.....	94

4.4.3 Design	96
4.5 Implementation.....	98
4.5.1 Socialization.....	98
4.5.2 Monitoring.....	99
4.6 Validation.....	101
4.6.1 Participants selected for the validation	102
4.6.2 Questions.....	103
4.6.3 Validation result	104
CHAPTER 5 – CONCLUSIONS AND RECOMMENDATIONS.....	108
5.1 Conclusions	108
5.2 Recommendations	108
5.3 Future Works	109
APPENDIX A	110
APPENDIX B	111
APPENDIX C	112
APPENDIX D.....	114
GLOSSARY.....	115
REFERENCES	116
CURRICULUM VITAE	123

LIST OF FIGURES

Figures	Page
Figure 1.1 Fishbone Diagram of Challenges for SMEs in Complying with Bank Indonesia's PSP Requirements.....	20
Figure 2.1 SME total in Indonesia (31 December 2024) ("UMKM Indonesia," 2024)	24
Figure 3.1 Research Framework	58
Figure 3.2 SAD framework.....	60
Figure 4.1 PT XYZ cloud infrastructure diagram.....	95
Figure 4.2 PT XYZ improvement design.....	98
Figure 4.3 IT Audit findings	100
Figure 4.4 IT audit repor final statement	101
Figure 5.1 Gap analysis interview with PT XYZ IT Manager.....	110
Figure 5.2 Framework socialization with PT XYZ IT Team	111
Figure 5.3 Validation evidence with Riki Andi Nugraha	112
Figure 5.4 Validation evidence with Sri Hardianti Abdullah	112
Figure 5.5 Validation evidence with Aditya Rangga Putra	113
Figure 5.6 Multiple zone and redundancy implementations.....	114

LIST OF TABLES

Table	Page
Table 2.1 SME Criteria	28
Table 2.2 PSP categories	33
Table 2.3 PSP Services for each categories	34
Table 2.4 BI information system and security requirement	36
Table 2.5 Critical Review	53
Table 4.1 Standard and Framework Comparison	63
Table 4.2 Framework Comparison	64
Table 4.3 Gap analysis results	65
Table 4.4 Data Confidentiality	72
Table 4.5 System and Data Integrity	76
Table 4.6 System and Data Two-Factor Authentication	77
Table 4.7 Prevention of Denial of Transactions That Have Been Carried Out (Non-Repudiation)	79
Table 4.8 System Availability	82
Table 4.9 The Existence of Systems and Procedures for Conducting Audit Trails	85
Table 4.10 The existence of internal policies and procedures for the operation of information systems and human resources	89
Table 4.11 The Fulfillment of Aspects of Security and Reliability of The System and/or Network Including Networks Provided by Other Parties	90
Table 4.12 The Existence of a Business Continuity Plan (BCP) That Can Guarantee the Continuity of the Implementation of Fund Management Activities. The BCP Includes Preventive Measures and Disaster Recovery Plans in the Event of an Emergency or Disruption That Results In The Main System For Implementing Fund Management Activities Being Unusable	92
Table 4.13 Planning	93
Table 4.14 Cloud components	95
Table 4.15 Design improvement	96

Table 4.16 Questions.....	103
Table 4.17 Validation result	104

