

**DESIGNING AN INTEGRATED DATA PRIVACY RISK ASSESSMENT
FRAMEWORK TO IMPROVE DATA PRIVACY GOVERNANCE AT BANK
XYZ**

By

Retno Wulansari
22351006

MASTER'S DEGREE
in

DATA SCIENCE CYBER SECURITY
MASTER OF 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 February 04, 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.

Retno Wulansari

Student

18 February 2026

Date

Approved by:

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

Feb 18th '26

Date

Thesis Advisor

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

18 February 2026

Date

Thesis Co-Advisor

Acknowledged by:

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

Dean of Faculty of Engineering & Information Technology

Date

Retno Wulansari

ABSTRACT

DESIGNING AN INTEGRATED DATA PRIVACY RISK ASSESSMENT FRAMEWORK TO IMPROVE DATA PRIVACY GOVERNANCE AT BANK XYZ

By

Retno Wulansari

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

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

SWISS GERMAN UNIVERSITY

This study designs an integrated data privacy risk assessment framework for Bank XYZ's digital partnerships focused on vendor onboarding. The framework harmonies ISO/IEC 27001:2022, ISO/IEC 27701:2019, the Payment Card Industry Data Security Standard (PCI DSS) v4.0, and the Indonesian Personal Data Protection Law (Law No. 27/2022, UU PDP), and applies the National Institute of Standards and Technology Special Publication 800-30 Revision 1 (NIST SP 800-30 Rev.1). Using Design Science Research, evidence was collected through document review, interviews, and questionnaires. Findings show gaps in privacy governance accountability, evidence-based vendor due diligence, and ongoing monitoring of third-party processing. The study delivers a traceable risk register and prioritized recommendations in the form of policy and checklist improvements. It concludes that the artefacts enable a repeatable assessment process and strengthen third-party privacy governance.

Keywords: Data Privacy Risk Assessment, ISO27001, ISO27701, PCI DSS, NIST SP 800-30, UU PDP

© Copyright 2026
by Retno Wulansari
All rights reserved



DEDICATION

I dedicate this work to the country I love, Indonesia. May this contribution support a future where digital banking partnerships grow responsibly, with strong protection of personal data and the right to privacy, fostering a safer and more trustworthy digital society. I also dedicate this work to my family for their unwavering support during challenging times and throughout my health limitations, and to my best friends for constant encouragement and strength. This work is a small reflection of my gratitude and love for you.



ACKNOWLEDGEMENTS

I am deeply grateful to Allah SWT for His blessings, strength, and guidance throughout this journey, tells. While facing health limitations, I often felt close to giving up and doubted my ability to complete this work. Alhamdulillah, by His help, I was able to persevere and finish this journey.

I would like to express my sincere appreciation to my thesis advisors, Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc., and Dr. Ir. Charles Lim, M.Sc., for their patience, continuous guidance, and valuable insights, which were instrumental in shaping the direction and depth of this study. I also extend my gratitude to the faculty members of Swiss German University for their support and for enriching my academic experience.

My sincere thanks also go to the management and staff of Bank XYZ for their cooperation, valuable input during the data collection and evaluation activities. I also extend my appreciation to the expert participants who contributed their time in validating this study through the Focus Group Discussion.

On a personal note, I thank my mother, my beloved daughters, Zivana and Hilyah, and my closest friends for their prayers, unwavering support, encouragement, and motivation, which helped me remain strong and complete this journey.

Finally, I acknowledge all researchers and scholars whose work has contributed to the foundation of this thesis. Any errors or shortcomings in this research remain entirely my responsibility.

TABLE OF CONTENTS

STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENTS.....	6
TABLE OF CONTENT.....	7
LIST OF FIGURES.....	9
LIST OF TABLES.....	9
CHAPTER 1 - INTRODUCTION.....	10
1.1 Background.....	10
1.2 Research Problem.....	14
1.3 Research Objective.....	15
1.4 Research Questions.....	15
1.5 Hypothesis.....	15
1.6 Research Scope and Limitation.....	15
1.7 Significance of the Study.....	16
1.8 Thesis Structure.....	16
CHAPTER 2 – LITERATURE REVIEW.....	18
2.1 Bank XYZ Overview.....	18
2.2 Digital Partnership in Banking Sector.....	19
2.3 Third Party Risk in Digital Banking Partnership.....	19
2.3.1 Cyber Security Risk Taxonomy.....	20
2.3.2 Data Privacy Risk and Personal Identifiable Information (PII) Risk.....	21
2.3.3 Third Party Risk and threats for banking.....	22
2.3.4 Impact on Organization.....	24
2.4 Mandatory Laws and Regulations on Personal Data Protection in the Banking Sector.....	25
2.5 Risk Assessment Frameworks for Data Privacy in Digital Banking Partnerships.....	27
2.5.1 ISO 31010:2019.....	27
2.5.2 OCTAVE Allegro.....	28
2.5.3 NIST SP 800-30 Framework.....	28
2.5.3.1 NIST Special Publication 800-30.....	28
2.5.3.2 NIST 800-30 Rev1.....	30
2.5.3.2 Likelihood Level Definition.....	32
2.5.3.2 Impact Definition.....	32
2.5.4 Comparison.....	33
2.6 ISO/IEC 27001: Information Security Management.....	34
2.7 ISO/IEC 27701: Privacy Extension for Third-Party Data Processor.....	35
2.8 PCI DSS v4.0.....	36
2.9 Framework Mapping for Integrated Data Privacy Risk Assessment in Digital Banking Partnership.....	37
2.10 Gap Analysis Approach.....	40
2.11 Domain and Indicator Mapping Approach.....	41
2.12 Design Science Research.....	43

2.13 Previous Study	44
CHAPTER 3 – RESEARCH METHODS	48
3.1 Research Design.....	48
3.2 Research Framework	49
3.2.1 Problem Identification	50
3.2.2 Data Collection	51
3.2.3 Gap Analysis.....	54
3.2.4 Framework Integration.....	55
3.2.5 Risk Assessment	55
3.2.6 Policy Development.....	55
3.2.7 Evaluation	56
3.2.8 Validation.....	56
3.3 Success Criteria.....	56
3.4 Expert Criteria.....	58
CHAPTER 4 – RESULT AND DISCUSSIONS	60
4.1 Data Collection Result	60
4.1.1 Integrated Domain Framework and Indicator Baseline	60
4.1.2 Summary of Document Review Result.....	63
4.1.3 Summary of Interview Result	63
4.1.4 Summary of Questionnaire Result	64
4.2 Gap Analysis Result.....	62
4.3 Framework Integration Result	67
4.3.1 Consolidation Domain Result.....	68
4.3.2 Integrated Privacy Risk Assessment Requirements.....	69
4.4 Risk Assessment	70
4.4.1 Threat Identification.....	71
4.4.2 Vulnerabilities Identification	71
4.4.3 Risk Scenario Formulation	72
4.4.4 Risk Level and Determination	72
4.4.5 Risk Assessment Result	75
4.4.5.1 Risk Evaluation.....	75
4.4.5.2 Control Recommendation	76
4.5 Policy Design Recommendation.....	78
4.5.1 Privacy Management Policy Design Recommendation.....	79
4.5.2 Third-Party Security Assessment Checklist Design Recommendation	81
4.6 Evaluation Result.....	82
4.7 Validation Result	84
CHAPTER 5 – RESULT AND DISCUSSIONS	87
5.1 Conclusions.....	87
5.2 Recommendations.....	88
5.3 Future Work.....	90
REFERENCES	92
GLOSARRY	97
LIST OF APPENDICES.....	98
CURRICULUM VITAE.....	113

LIST OF FIGURES

Figure 1.1 Data Breach in Indonesia from 2020-2025.....	11
Figure 1.2 Type of Data Breach 2021 to 2024.....	12
Figure 1.3 Fishbone Diagram	14
Figure 2.1 Risk Assessment NIST SP 800-30	30
Figure 2.2 Risk Assessment NIST SP 800-30 Revision 1	31
Figure 2.3 DSR Adoption Mapping.....	44
Figure 3.1 Research Design	48
Figure 3.2 Research Framework	50

LIST OF TABLES

Table 2.1 Risk Assessment Methodology Comparison	33
Table 2.2 Framework Mapping for Integrated Data Privacy Risk Assessment.....	38
Table 2.3 Domain Mapping for Indicator Development.....	42
Table 2.4 Previous Study	45
Table 4.1 Integrated Domain Framework.....	60
Table 4.2 Indicator Derivation	62
Table 4.3 Questionnaire Results	64
Table 4.4 Gap Analysis Result	66
Table 4.5 Consolidated Domain Result	68
Table 4.6 Integrated Privacy Risk Assessment Requirements.....	69
Table 4.7 Likelihood Definition	72
Table 4.8 Impact Definition	73
Table 4.9 Risk Level Matrix	73
Table 4.10 Risk Scale	71
Table 4.11 Risk Evaluation Result.....	75
Table 4.12 Control Recommendation	78
Table 4.13 Proposed Governance Instrument	79
Table 4.14 Policy Structure Component.....	80
Table 4.13 Expert Validation Feedback.....	85