

**DESIGNING USER-CENTERED RISK MANAGEMENT FRAMEWORK TO  
ENHANCE SECURITY POSTURE AND SECURITY CONTROL MODEL IN  
SME**

By

Jahja Mayudin Kurniawan

22451049

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY  
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY

‘The Prominence Tower

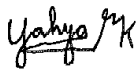
Jalan Jalur Sutera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

February 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.



Jahja Mayudin Kurniawan

Student

17-02-2026

Date

Approved by:



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

Thesis Advisor

Feb20th, 2026

Date



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

Thesis Co-Advisor

19-02-2026

Date

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

Dean of Faculty of Engineering and Information Technology

Date

## ABSTRACT

### DESIGNING USER-CENTERED RISK MANAGEMENT FRAMEWORK TO ENHANCE SECURITY POSTURE AND SECURITY CONTROL MODEL IN SME

By

Jahja Mayudin Kurniawan Students  
Dr. Ir. M. Amin Soetomo, M.Sc, Advisor  
Dr. Ir. Charles Lim, B.SC, M.Sc, Co-Advisor

SWISS GERMAN UNIVERSITY



Small and Medium Enterprises (SMEs) face growing cybersecurity risks while having limited resources and low readiness to implement ISO/IEC 27001. This research aims to design a user-centered risk management framework to improve security posture and enhance the effectiveness of security control implementation. The study applies Design Science Research Methodology (DSRM) by integrating ISO/IEC 27005 as the operational risk management standard and ISO 31000 as strategic guidance, supported by a Multi-Criteria Decision Analysis (MCDA) approach for security control prioritization.

The framework was demonstrated through a case study at PT Pulsabayar and evaluated using Focus Group Discussions and expert validation. The results indicate improved organizational understanding of risk assessment, structured risk prioritization, and effective mapping of risks to ISO/IEC 27001 Annex A controls. This research concludes that a user-centered and standards-aligned framework can strengthen cybersecurity governance and support SMEs in achieving incremental compliance and sustainable security improvement.

**Keywords:** Risk management, ISO/IEC 27001, ISO/IEC 27005, SME, security control, risk prioritization

© Copyright 2026  
by Jahja Mayudin Kurniawan Students  
All rights reserved



## DEDICATION

I dedicate this research project to my God, my Family, and my beloved country  
Indonesia



## ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to members of my committee for their support & patience. Their gentle but firm direction has been most appreciated. Dr. Ir. M. Amin Soetomo, M.Sc and Dr. Ir. Charles Lim, B.SC, M.Sc was particularly helpful in guiding me toward a research project. From the beginning, they are confident in my abilities to not only complete a degree but to complete it. It is through their invaluable contributions that this thesis and the entire research project have till this stage.

I would also like to thank my family for their moral support during my academic journey at SGU University. I proud that the time, patience, and sacrifices that enabled me to complete this thesis.

Lastly, I would like to express my appreciation to my team and colleagues at work, and my friends, especially Batch 35 MIT SGU, for their constant encouragement. I am also grateful to the many individuals who have supported me throughout research project, directly or indirectly.

## TABLE OF CONTENTS

|                                                            | Page |
|------------------------------------------------------------|------|
| <b>Contents</b>                                            |      |
| DEDICATION .....                                           | 5    |
| CHAPTER 1 - INTRODUCTION .....                             | 11   |
| 1.1 Background .....                                       | 11   |
| 1.2 Problem Statement .....                                | 12   |
| 1.3 Research Objectives .....                              | 13   |
| 1.4 Research Questions .....                               | 14   |
| 1.5 Hypothesis .....                                       | 14   |
| 1.6 Scope and Limitations .....                            | 14   |
| 1.7 Significance of The Study .....                        | 15   |
| 1.8 Thesis Structure .....                                 | 15   |
| CHAPTER 2 LITERATURE REVIEW .....                          | 17   |
| 2.1 Business, Industries and Challenges SME .....          | 17   |
| 2.2 The SME Organization .....                             | 18   |
| 2.3 Risk management .....                                  | 21   |
| 2.4 Related Works .....                                    | 34   |
| CHAPTER 3 RESEARCH METHODS .....                           | 38   |
| 3.1 Research Framework .....                               | 38   |
| 3.2 Research Design (Design Science Research Method) ..... | 38   |
| 3.3 Proposed Risk Management Framework .....               | 39   |
| CHAPTER 4 - RESULTS AND DISCUSSIONS .....                  | 50   |
| 4.1 Context Establishment .....                            | 50   |
| 4.2 Risk Identification .....                              | 51   |
| 4.3 Risk Analysis .....                                    | 53   |
| 4.4 Risk Evaluation .....                                  | 59   |
| 4.5 Risk Treatment .....                                   | 62   |
| 4.6 Evaluation .....                                       | 65   |
| 4.7 Validation .....                                       | 67   |
| 4.8 Result Summary .....                                   | 68   |
| 4.9 Limitation .....                                       | 69   |

|                                                                           |    |
|---------------------------------------------------------------------------|----|
| CHAPTER 5 - CONCLUSIONS AND RECCOMENDATIONS.....                          | 70 |
| 5.1 Conclusion .....                                                      | 70 |
| 5.2 Recommendations.....                                                  | 70 |
| 5.3 Future Works .....                                                    | 71 |
| Appendix A - Risk Register .....                                          | 74 |
| Appendix B - Forum Group Discussion on Prioritizing Security Control..... | 79 |
| Appendix C - Risk Control Prioritization Formula.....                     | 82 |
| Appendix D - Internal Stakeholder Evaluation Questionnaire .....          | 84 |
| Appendix E - Expert Profile and Questionnaire .....                       | 86 |
| Appendix F - Documentation of FGD & External Expert Validation .....      | 89 |
| Appendix G – Table Priority Score .....                                   | 92 |
| Appendix H – Table Likelihood Score .....                                 | 98 |



## LIST OF FIGURES

| Figures                                                          | Page |
|------------------------------------------------------------------|------|
| Figure 1.1 Fishbone diagram                                      | 13   |
| Figure 2.1 Organization structure                                | 20   |
| Figure 2.2 ISO 31000 Risk Management Principle                   | 24   |
| Figure 2.3 ISO/IEC 27005 The Risk Management Process (ISO, 2022) | 27   |
| Figure 2.4 Design Science Research Framework                     | 37   |
| Figure 3.1 Proposed Risk Management Framework                    | 38   |



## LIST OF TABLES

| Table                                          | Page |
|------------------------------------------------|------|
| Table 2.1 Comparison Risk Management Framework | 30   |
| Table 2.2 Literature review                    | 35   |
| Table 3.1 Likelihood                           | 43   |
| Table 3.2 Impact                               | 44   |
| Table 3.3 Risk level                           | 45   |
| Table 3.4 Risk treatment                       | 47   |
| Table 4.1 List of Asset                        | 51   |
| Table 4.2 Risk Level                           | 54   |
| Table 4.3 Risk Prioritization                  | 61   |
| Table 4.4 Control Prioritization               | 62   |

