

**Developing an Integrated Cybersecurity Audit Framework: Harmonizing  
Diverse Frameworks for Enhanced Specificity Guideline**

By

Ismail Choiri, S.T.  
22451023

MASTER'S DEGREE  
in

Data Science and Cybersecurity  
Master of Information Technology



SWISS GERMAN UNIVERSITY  
The Prominence Tower  
Jalan Jalur Sutera Barat No. 15, Alam Sutera  
Tangerang, Banten 15143 - Indonesia

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.



Ismail Choiri, S.T.

Student

24.08.2025

Date

Approved by:



Dr. Ir. Eka Budiarto, S. T, M Sc

25.08.2025

Date



Thata Apriatin, S.Kom., M Kom

24.08.2025

Date

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

Date

## ABSTRACT

### Developing an Integrated Cybersecurity Audit Guideline: Harmonizing Diverse Frameworks for Enhanced Specificity Guideline

By

Ismail Choiri, S.T.  
Dr. Ir. Eka Budiarto, S. T, M Sc , Advisor  
Thata Apriatin, S.Kom., M Kom, Co-Advisor

SWISS GERMAN UNIVERSITY

This thesis addresses the critical challenge of adapting generic audit practices to the specialized demands of cybersecurity within the Indonesian banking sector. It identifies significant deficiencies in existing audit Standard Operating Procedures (SOPs), particularly their lack of specific cybersecurity risk assessment methodologies and a dedicated Risk and Control Matrix (RCM). In response, a revised SOP is proposed, fundamentally transforming the audit process through the integration of a NIST SP 800-30 based risk assessment and the development and testing of a Cybersecurity Risk Control Matrix (C-RCM). Expert validation confirms this new framework's comprehensive alignment with global standards like NIST CSF, ISO 27001, and GIAS, demonstrating its high relevance to the practical needs of Indonesian banking institutions in navigating contemporary cyber threats and regulatory requirements. While implementation presents a moderate complexity, demanding investment in specialized expertise and technology, the long-term benefits of enhanced cybersecurity posture and operational resilience are substantial. This research concludes that the proposed SOP offers an indispensable pathway for Indonesian banks to transition from reactive compliance to a proactive, adaptive cybersecurity audit paradigm.

*Keywords: Cybersecurity Audit, NIST CSF, ISO 27001, Cybersecurity Compliance*



## **DEDICATION**

Dedication to my PT. XYZ and the Real Cybersecurity world.



## **ACKNOWLEDGEMENTS**

I would like to express my deepest gratitude to my beloved mother for her endless prayers and encouragement, and to my late father, whose guidance and values continue to inspire me every day. My heartfelt thanks also go to my younger sibling for their constant support, and to my wife and child, whose love, patience, and sacrifices have been the foundation of my journey.

I am also sincerely thankful to PT. XYZ, my professional home, for providing me with invaluable experience and insights into the real world of cybersecurity.

Special appreciation goes to my advisor, Dr. Ir. Eka Budiarto, S.T., M.Sc., for his unwavering guidance, critical insights, and encouragement throughout this research. I am equally grateful to my co-advisor, Thata Apriatin, S.Kom., M.Kom., for her thoughtful feedback and support that sharpened my work.

To all who have contributed directly or indirectly to this work, I extend my heartfelt thanks. This achievement would not have been possible without your support and belief in me.

## TABLE OF CONTENTS

|                                                             | Page      |
|-------------------------------------------------------------|-----------|
| STATEMENT BY THE AUTHOR                                     | 2         |
| ABSTRACT                                                    | 3         |
| DEDICATION                                                  | 5         |
| ACKNOWLEDGEMENTS                                            | 6         |
| TABLE OF CONTENTS                                           | 7         |
| LIST OF FIGURES                                             | 9         |
| LIST OF TABLES                                              | 10        |
| CHAPTER 1 – INTRODUCTION                                    | 11        |
| 1.1. Background                                             | 11        |
| 1.2. Research Problem                                       | 12        |
| 1.3. Research Objective                                     | 13        |
| 1.4. Research Question                                      | 14        |
| 1.5. Hypothesis                                             | 14        |
| 1.6. Research Scope and Limitation                          | 14        |
| 1.7. Significance of Study                                  | 15        |
| 1.8. Thesis Structure                                       | 15        |
| <b>CHAPTER 2 - LITERATURE REVIEW</b>                        | <b>17</b> |
| 2.1. Information Technology Audit                           | 19        |
| 2.3. NIST Cybersecurity Framework (CSF)                     | 21        |
| 2.4 ISO/IEC 27001 (Information Security Management Systems) | 24        |
| 2.5 Global Internal Audit Standards (GIAS) 2024             | 25        |
| 2.6 NIST Special Publication 800-30 Revision                | 26        |
| 2.7 Design Science Research (DSR)                           | 27        |
| 2.8 Mapping the Frameworks                                  | 28        |
| 2.9 Previous Studies                                        | 31        |
| 2.9.1 Clustered Landscape of Prior Work.                    | 31        |
| 2.9.2 What the Literature Gives and What It Misses.         | 32        |
| <b>CHAPTER 3 – RESEARCH METHODS</b>                         | <b>34</b> |
| 3.1. Gap Analysis                                           | 35        |
| 3.1.1 Activity Identification Process Walkthrough           | 35        |
| 3.1.2 Documentation Review                                  | 36        |
| 3.2. Design and Developing Artifact                         | 36        |
| 3.2.1 The Artifact Definition                               | 36        |

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| 3.2.2 Foundations Design Principles                                         | 37        |
| 3.3 Development Artifact Guideline                                          | 37        |
| 3.4 Artifact Evaluation                                                     | 38        |
| 3.4.1 Evaluation Method                                                     | 38        |
| 3.4.2 Evaluation Criteria and Specific Metrics                              | 39        |
| <b>CHAPTER 4 – Analysis and Result</b>                                      | <b>41</b> |
| 4.1 Gap Analysis                                                            | 41        |
| 4.1.1 Overview of the Current Audit Framework                               | 41        |
| 4.1.2 Detailed Gap Analysis Current and Ideal Cybersecurity Audit SOP       | 43        |
| 4.2 Designing and Developing Artifact Guideline                             | 46        |
| 4.2.1 Lack of Cybersecurity-Specific Audit Objectives and Scope Definition  | 46        |
| 4.2.2 Absence of a NIST SP 800-30 Cybersecurity Risk Assessment Methodology | 46        |
| 4.2.3 Missing Risk and Control Matrix (RCM) Development                     | 48        |
| 4.3 Artifact Evaluation                                                     | 52        |
| <b>CHAPTER 5 – Conclusion and Future Research</b>                           | <b>54</b> |
| 5.1 Conclusion                                                              | 54        |
| 5.2 Future Works                                                            | 55        |
| 5.3 Recommendation                                                          | 56        |
| REFERENCES                                                                  | 58        |
| Appendix                                                                    | 61        |
| CURRICULUM VITAE                                                            | 69        |

## LIST OF FIGURES

| Figures                                                          | Page |
|------------------------------------------------------------------|------|
| 1.1 Navigating Cybersecurity Challenges                          | 11   |
| 1.2 Fishbone Diagram                                             | 13   |
| 2.1 The top targeted industry groups.(Ensign InfoSecurity, 2024) | 17   |
| 2.2 Cybersecurity Architecture                                   | 18   |
| 2.3 NIST CSF 2.0                                                 | 22   |
| 2.4 ISO 27001                                                    | 24   |
| 2.5 Global Internal Audit Standards 2024                         | 25   |
| 2.7 Design Science Research                                      | 28   |
| 3.1 Research Framework                                           | 35   |
| 4.1 Existing Procedure                                           | 42   |
| 4.2 The Result Artifact Guideline                                | 52   |

## LIST OF TABLES

| Table                                                                     | Page |
|---------------------------------------------------------------------------|------|
| 2.1 The Mapping Framework                                                 | 12   |
| 2.2. Critical Review                                                      | 13   |
| 4.1 Gap Analysis                                                          | 46   |
| 4.2 Key Steps of a NIST SP 800-30 Based Risk Assessment                   | 49   |
| 4.3 Essential Components of a Cybersecurity Risk and Control Matrix (RCM) | 51   |
| 4.3 Essential Components of a Cybersecurity Risk and Control Matrix (RCM) | 51   |
| 4.3 Essential Components of a Cybersecurity Risk and Control Matrix (RCM) | 51   |