

INFORMATION SECURITY MATURITY MODEL  
A BEST PRACTICE DRIVEN APPROACH TO PCI DSS COMPLIANCE

By

Semi Yulianto  
22013210

MASTER'S DEGREE  
In

INFORMATION TECHNOLOGY  
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY  
EduTown BSD City  
Tangerang 15339  
Indonesia

Revision after the Thesis Defense on 1<sup>st</sup> February 2016

## 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 company, except where due acknowledgement is made in the thesis.

Semi Yulianto

Student

Date

Approved by:

Benfano Soewito, BSc., MSc., PhD, Advisor

Thesis Advisor

Date

SWISS GERMAN UNIVERSITY

Charles Lim, BSc., MSc., Co-Advisor

Thesis Co-Advisor

Date

Dr. Ir. Gembong Baskoro, MSc.

Dean

Date

---

## ABSTRACT

### INFORMATION SECURITY MATURITY MODEL A BEST PRACTICE DRIVEN APPROACH TO PCI DSS COMPLIANCE

By

Semi Yulianto

Benfano Soewito, BSc., MSc., PhD, Advisor

Charles Lim, BSc., MSc., Co-Advisor

SWISS GERMAN UNIVERISTY



This research study proposes a practical information security maturity model (ISMM), which utilizes the use of quantitative and qualitative analysis, enhancing the PCI DSS to ISO/IEC 27001 mapping, emphasizes on the PCI DSS (specific) to ISO/IEC 27001 (generic) mapping and focuses on improving the quality of people, process and technology. This research study presents a practical approach to effectively identify the key success factors and the most common gaps in the PCI DSS compliance requirements and encourage the organizations to proactively improve their information security state by selecting the best security countermeasures (controls) to protect their information assets from the emerging cyber-attacks. The ISMM presented in this research study is a best practice driven model intended to be used by organizations regardless of type and size.

Extensive literature review were conducted and survey study approaches. Several ISMMs were selected, compared and analyzed. In order to validate the findings, three financial organizations in Indonesia were selected. The study was based on generic security controls adopted from the industry best practices by most of the organizations to protect their information asset. ISMM with four maturity level was proposed. The maturity level were: None, Initial, Basic and Capable.

The research main contribution is that the proposed model would help the organizations to save the time and efforts and provided as a tool to measure the maturity level of their information security state and come up with the best strategy to fully comply with PCI DSS.

*Keywords: PCI, PCI DSS, ISO/IEC 27001, compliance, compliant, maturity, model.*



## DEDICATION

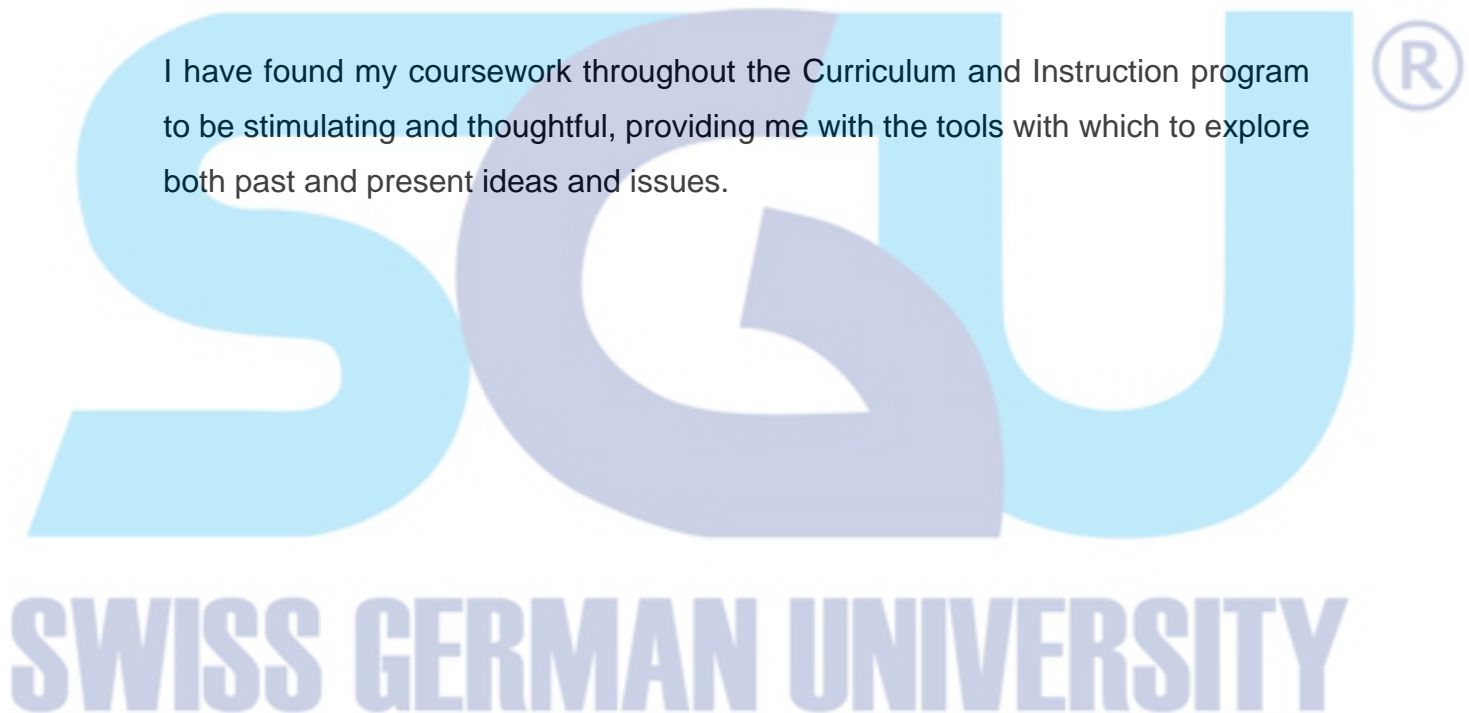
I dedicate this work to my beloved family who have prayed for me every day, my parents for all the support and encouragement, colleagues in MIT Swiss German University and especially my country Indonesia.



## ACKNOWLEDGEMENTS

I wish to thank the members of my committee for their support, patience and good humour. Their gentle but firm direction has been most appreciated. Greatest appreciation to Mr. Benfano Soewito, BSc., MSc., PhD (Advisor) and Mr. Charles Lim, BSc., MSc. (Co-Advisor) which were particularly very helpful in guiding me toward a better methodology in research study writing.

I have found my coursework throughout the Curriculum and Instruction program to be stimulating and thoughtful, providing me with the tools with which to explore both past and present ideas and issues.



## Table of Contents

STATEMENT BY THE AUTHOR .....	2
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENTS .....	6
Chapter 1 – Introduction .....	11
<b>1.1 Background</b> .....	11
<b>1.2 Problem Definition</b> .....	12
<b>1.3 Research Objectives</b> .....	14
<b>1.4 Significant of Study</b> .....	14
<b>1.5 Research Questions</b> .....	14
<b>1.6 Research Limitations</b> .....	15
<b>1.7 Hypothesis</b> .....	16
<b>1.8 Thesis Structure</b> .....	16
Chapter 2 – Literature Review .....	17
<b>2.1 Information Security Standards</b> .....	17
2.1.1 ISO/IEC 27001:2013 (ISMS) .....	17
2.1.2 Payment Card Industry Data Security Standards (PCI DSS) .....	20
2.1.3 COBIT (Control Objectives for Information and related Technology) .	21
2.1.4 PCI DSS v3.0 with ISO/IEC 27001:2013.....	22
2.1.5 PCI DSS v3.0 with COBIT 5.....	23
<b>2.2 Comparative Analysis of Information Security Models</b> .....	27
2.2.1 Information Security Management Maturity Model (ISM3) .....	27
2.2.2 NIST-PRISMA Information Security Maturity (ISM) .....	27
2.2.3 ISMS (Im) – Maturity Model.....	28
2.2.4 Other ISMMs .....	28
<b>2.3 Compliance Process</b> .....	30
<b>2.4 Related Works</b> .....	31
2.4.1 Standards and Frameworks .....	31
2.4.2 Information Security Maturity Models .....	32
2.4.3 The Proposed Model .....	34

Chapter 3 – Research Methodology .....	36
<b>3.1 Scope of Study</b> .....	36
<b>3.2 Research Process/Methodology</b> .....	36
<b>3.3 Method of Analysis</b> .....	41
3.3.1 Gap Analysis .....	41
3.3.2 SWOT Analysis .....	42
3.3.3 I/E Matrix Analysis.....	42
<b>3.4 Information Security Maturity Model (ISMM)</b> .....	42
3.4.1 Theoretical Approach .....	42
3.4.2 Experimental Considerations.....	46
3.4.3 Model Validity .....	47
Chapter 4 – Results and Discussion.....	51
<b>4.1 Data Source and Collection</b> .....	51
4.1.1 Organizations .....	51
4.1.2 Primary Dataset.....	52
4.1.3 Secondary Dataset.....	55
<b>4.2 Analysis and Results Comparison</b> .....	58
<b>4.3 Expert Panel Review</b> .....	60
Chapter 5 – Conclusion and Recommendations.....	63
<b>5.1 Conclusion</b> .....	63
<b>5.2 Recommendations</b> .....	64
<b>5.3 Future Work</b> .....	65
References .....	66
Glossary.....	73
APPENDIX A - Sample Questionnaires (ISO 2013).....	77
APPENDIX B - Expert Review Feedback Form .....	82
APPENDIX C - SWOT Analysis Example .....	88
APPENDIX D - Expert Panel Review Criteria .....	89
APPENDIX E - Curriculum Vitae.....	90