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 1st 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

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