

THESIS

**Development of Application Security Standard for Compliance to Information
Security Standard, PT. XYZ, Jakarta**

By

Irwin Lawrencius

2-2014-112

MASTER'S DEGREE

In

INFORMATION TECHNOLOGY
ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
EduTown BSD City
Tangerang 15339
Indonesia

January, 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 institution, except where due acknowledgement is made in the thesis. All used sources from external publications were cited without any exceptions.

Irwin Lawrencius Siagian, S.T

Student

Date

Approved by:

Dr. Lukas, M.AI

Thesis Advisor

Date

Charles Lim, M.Sc

Thesis Co-Advisor

Date

ABSTRACT**Development of Application Security Standard for Compliance to Information Security Standard: Case Study PT XYZ**

By

Irwin Lawrencius

2-2014-112

Dr. Lukas, M.AI, Advisor
Charles Lim, M.Sc, Co-Advisor

SWISS GERMAN UNIVERSITY

Application is a critical part on business process. Unfortunately, most of organization only concern with security control on infrastructure and general security control on logical access. There are many threats to application exist today that targeted the confidentiality, integrity, and availability of data especially on internet application. Security control on infrastructure and logical access is not enough to ensure the information or data is well protected on business process.

Application security becomes a very important aspect in order to defence or protecting sensitive data, assets, and reputation against threats to business process. To ensure the security on the application from design phase until production phase, it is needed a standard that contains a security requirements for application and it is called Application Security Standard.

To develop an application security standard, author using a hybrid threat modeling analysis process to identify and categorize threats on application. Also, with threat modeling analysis, security control against threats can be defined. Hybrid threat modeling is a combination and modification from some threat modeling process.

Keywords: Application, application security standard, hybrid threat modeling, threat, STRIDE, OWASP, data flow diagram



DEDICATION

I dedicate this thesis to my mom, who taught me the most important things in my life.



ACKNOWLEDGEMENTS

The author wishes to give thanks to God, my family especially my mother, Antonius Andy Wijaya, Kapat Parwono, Patria Indrajaya, Moh. Saleh M. Raub, Dr. Lukas, Charles Lim and the SGU Library for their continuous support in the development, writing, and completion of this thesis.

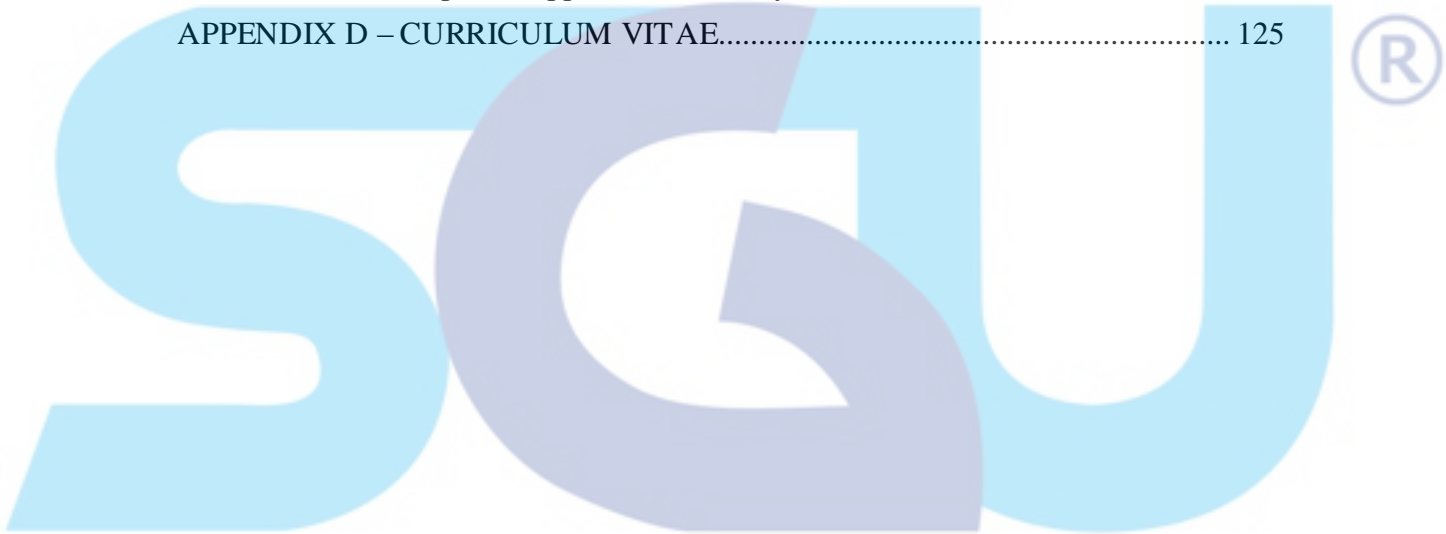


TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	5
ACKNOWLEDGEMENTS	6
TABLE OF CONTENTS	7
LIST OF FIGURES	10
LIST OF TABLES	11
CHAPTER 1 - INTRODUCTION	12
1.1 Background	12
1.2 Research Location	14
1.3 Research Problem	14
1.4 Research Objective	15
1.5 Research Questions	15
1.6 Research Scope	15
1.7 Significance Study	16
1.8 Thesis Structure	16
CHAPTER 2 – LITERATURE REVIEW	18
2.1 Information Security	18
2.1.2 Information Security Aspects	19
2.1.3 Information Security Principles	19
2.2. IT Risk	21
2.3. Risk Management	21
2.3.1 Risk Rating	22
2.1.3 Risk Rating Framework	22
2.4 Application Security	24
2.4.1 Application Security Key Principles	24
2.4.2 Application Security Standard	25
2.5 Application Security Framework	26
2.5.1 Threat Modeling	26
2.5.2 NIST SP 800-53 Information Security	27
2.5.3 Payment Application Data Security Standard (PA-DSS)	28
2.5.4 The Open Web Application Security Project (OWASP)	29
2.5.5 The Open Web Application Security Project – Application Security Verification Standard	30
2.5.6 Federal Information Security Law and Regulations	30
2.6. Information Security Law and Regulations	31

2.6.1 UU/ITE.....	31
2.6.2 Peraturan Bank Indonesia.....	33
2.7 Compliance.....	33
2.8 Related Works	34
2.8.1 Information Security Policy on Organization.....	34
2.8.2 Traditional Threat Modeling	34
2.8.3 Microsoft Threat Modeling Methodology	36
2.8.4 Secure Software Development Life Cycle	37
2.8.5 Advance Threat Modeling by OWASP.....	38
2.8.6 Research Discussion on Threat Modeling used on this Research.....	39
2.9 Theoretical Framework	42
CHAPTER 3 – METHODOLOGY.....	42
3.1 Research Methodology	42
3.1.1 Problem Identification	44
3.2 Investigation	44
3.2.1 Data Gathering.....	44
3.2.2 Data Analysis.....	45
3.2.3 Literature Review	46
3.2.4 In-Depth Interview	46
3.2.5 Threat Modeling.....	47
3.3 Design.....	50
3.3.1 Scoping Area	51
3.3.2 Application Security Standard Domain	52
3.4 Framework Mapping.....	54
3.5 Proposed Application Security Standard.....	55
3.6 Validation	55
CHAPTER 4 – RESULT AND DISCUSSION.....	56
4.1 Investigation	56
4.2 Analysis.....	56
4.2.1 Document Review	56
4.2.2 Hybrid Threat Modeling.....	56
4.2.3 In-Depth Interview	70
4.3 Focus Group Discussion.....	72
4.4 Proposed Application Security Standard.....	74
4.5 Validation	91
4.5.1. Application Security Standard Implementation	91

CHAPTER 5 – CONCLUSION AND RECOMMENDATION.....	95
5.1 Conclusion.....	95
5.2 Recommendation.....	96
5.3 Future Work.....	96
GLOSSARY.....	97
REFERENCES.....	99
APPENDICES.....	103
APPENDIX A – In-depth Interview.....	103
APPENDIX B – Focus Group Discussion.....	106
APPENDIX C – Proposed Application Security Standard.....	108
APPENDIX D – CURRICULUM VITAE.....	125



SWISS GERMAN UNIVERSITY