ANALYSIS OF INFORMATION TECHNOLOGY GOVERNANCE AND SECURITY USING COBIT 5 AND PCI DSS FOR POLICY IMPROVEMENTS : CASE STUDY OF PT XYZ IN IT SERVICES AREA

By
Thata Apriatin
21951012

MASTER'S DEGREE
in
MASTER OF INFORMATION TECHNOLOGY
ENGINEERING AND INFORMATION TECHNOLOGY

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

February 2021
Revision after thesis defense on 28 January 2021

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.

Student Date

Approved by:

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

Thesis Advisor Date

Dr. Ir. Heru. P. Ipung. M. Eng

Thesis Co-Advisor Date

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

Dean of Faculty of Engineering and Information Technology Date

ABSTRACT

ANALYSIS OF INFORMATION TECHNOLOGY GOVERNANCE AND SECURITY USING COBIT 5 AND PCI DSS FOR POLICY IMPROVEMENTS: CASE STUDY OF PT XYZ IN IT SERVICES AREA

By

Thata Apriatin

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

Dr. Ir. Heru P. Ipung, M. Eng,

SWISS GERMAN UNIVERSITY

Information and Communication Technology has experienced developments in all aspects of life. PT XYZ as a dedicated cloud service provider must ensure that the service has passed the right to information technology security governance and also meets international standards.

The purpose of this study is to analyses whether the information technology governance at PT XYZ is appropriate and can follow reliable compliance. In this case the researcher uses the Payment Card Industry - Data Security Standard (PCI DSS) and Cobit 5 compliance methodology.

In the process, researchers used COBIT 5 (APO01.08 Maintain compliance with policies, APO03.02 Define reference Architecture, APO12.01 Collect Data, DSS01.03 Monitor Infrastructure, DSS05.05 Manage physical access to IT assets) .

process mapping assistance to support PCI DSS compliance requirements. Data collection techniques used to compile this research are the results of observations, interviews in this case in focus group discussion forums and literature studies. The results of this study are to produce better policies and procedures so that they are more comprehensive in accordance with international compliance standards and increase the company's credibility as a cloud service provider.

Keywords: COBIT 5,Cloud, Compliance, Standard, PCIDSS.

DEDICATION

I would like to dedicate this research project to my beloved Mom, my Husband, my Son, and my beloved country Indonesia and my second home where I grow in knowledge, IT Services Operations

ACKNOWLEDGEMENTS

Praise God Almighty, for the presence of plenty of mercy and his grace, so that the writer can complete the thesis with the title "ANALYSIS OF INFORMATION TECHNOLOGY GOVERNANCE AND SECURITY USING COBIT 5 AND PCI DSS FOR POLICY IMPROVEMENTS: CASE STUDY OF PT XYZ IN IT SERVICES AREA" is submitted as the final requirement in accomplishing master's degree at Swiss German University.

Thank you very much to my Mother and my beloved late father, my Brothers, my Sisters, my Family Pesantren Lungsemut for praying and all the support during my study at Swiss German University. To my husband and sons (Ferry and Sigi) who always provide encouragement in the preparation of the thesis and also thanks for their attention to the author, my sister Vinda and my niece Amoy who have been willing to accompany and inspire.

The author's appreciation and gratitude give to Mr. Dr. Ir. Moh. A.Amin Soetomo, M. Sc, as Advisor and Dr. Ir. Heru P. Ipung, M. Eng, as the Co Advisor who helped write this thesis. And thanks to Mr. Dr. Charles Lim, and Mr. Eka Budiarto who has given enthusiasm for writing during his lectures at Swiss German University, and all the lecturers in the Swiss German University Cybersecurity class who have provided guidance during the lecture period.

Thank you to all students of class B-25 Business Cybersecurity and Cybersecurity, especially Pejuang 25 who always give an injection of enthusiasm when enthusiasm is down, thank you for your solidarity so far.

My best friends (Samuel, Imam, Juliardi, Arhemy Shelly, Wiliambuyung, Hansen, Santoso Song, Tedi, Monika, Alm Revino) who are always bothered by giving other views about what I have compiled in this thesis and colleagues in IT Services, especially Cloud and Security team.

Finally, the writer realizes that the writing of this thesis is still far from perfection. Therefore, the authors ask for suggestions and constructive criticism for its perfection and hopefully it will benefit us all. Amen.

Table Of Content

STATEMENT BY THE AUTHOR 2
ABSTRACT 3
DEDICATION 5
ACKNOWLEDGEMENTS 6
LIST OF FIGURES 9
LIST OF TABLES 9
CHAPTER 1 – INTRODUCTION 10
1.1 Background 10
1.2 Problems Statement 12
1.3 Research Objective 14
1.4 Research Question 14
1.5 Scope and Limitation 14
1.6 Hypothesis 15
1.7 Significance of study 15
1.8 Thesis Structure 16
CHAPTER 2 – LITERATURE REVIEW 17
2.1 Theoretical Perspective 17
2.2 Cloud Services and Model 17
2.2.1 Cloud Customer identification 20
2.3 IT Governance for Service Provider 20
2.4 Security and Compliance Issue 22
2.5 HIPAA 22
2.5.1 FISMA 24
2.5.2 ISO 27001 25
2.5.3 PCI DSS 27
2.5.4 COBIT 5 29
2.5.5 Measurement stages 31
2.6 Previous Research Review 32
2.6.1 Cloud Security Compliance. 32
2.6.2 Security Threat and Control Models 33
2.6.3 Compliance Approach for cloud services 35
2.6.4 PCI DSS for Cloud Service Provider 35
2.6.5 Mapping Cobit 5 with PCI DSS 37
2.6.6 Related Work 37
2.6.7 Comparison of Compliance 38

2.6.8 Previous Study Journal 52
CHAPTER 3 – RESEARCH METHODS 53
3.1 Research Methodology 53
3.2 Research Framework 54
3.2.1 Finding 55
3.2.2 Data Preparation 55
3.2.3 Data Analysis 56
3.2.4 Evaluation 56
3.2.5 Validation 56
3.2.6 Deployment 56
3.3 Flow Model Produce 57
CHAPTER 4 – RESULT AND DISCUSSION 59
4.1 Determination 59
4.1.1 Focus Group Discussion 59
4.2 Mapping the enterprise Goals in COBIT 5 60
4.3 Mapping Enterprise Goals to IT Goals 63
4.3.1 Focus Group Discussion 65
4.3.2 Analysis 66
4.3.2.1 Procedure of Assessment 66
4.3.2.2 Evaluation 66
4.3.3 Improve security Policy 67
4.3.3.1 Produce Security Policy 68
4.3.3.2 Determination of Audit gaps process 68
CHAPTER 5 – CONCLUSIONS AND RECOMMENDATIONS 71
5.1 Conclusions 71
5.2 Recommendations 72
GLOSSARY 72
REFERENCES 73

LIST OF FIGURES

FIGURE 1 1 FISHBONE DIAGRAM 13

FIGURE 2 1 FISMA AUDIT FRAMEWORK.....25
FIGURE 2 2 ISO 27001 METHOD 27
FIGURE 2 3 FIVE CONCEPTS OF IT GOVERNANCE.....30
FIGURE 2 4 COBIT FRAMEWORK (ISACA, 2012)[30].....31
FIGURE 2 5 COBIT ENTERPRISE GOALS, SOURCE ISACA[30] ...**ERROR! BOOKMARK NOT DEFINED.**

FIGURE 3 1 RESEARCH METHODOLOGY.....53
FIGURE 3 2 FLOW MODEL PRODUCE INFORMATION SECURITY POLICY 57
FIGURE 3 3 RESEARCH FLOW 58

FIGURE 4 1 MAPPING ENTERPRISE GOALS AND IT GOALS, SOURCE(ISACA,2012)[30] .60
FIGURE 4 2FIGURE IT RELATED GOAL MAPPING TO ENTERPRISE GOAL; SOURCE ISACA[30] 64

LIST OF TABLES

TABLE 1.1 IT SERVICES PRODUCT PT. XYZ SOURCE FROM: (PT. XYZ, 2016).....11

TABLE 2 1 CLOUD SERVICE LEVEL.....18
TABLE 2 2 9 STEPS TOWARD COMPLIANCE WITH FISMA[21] 25
TABLE 2 3 ISO27001 REQUIREMENT [21].....26
TABLE 2 4 PCIDSS HIGH LEVEL OVERVIEW SOURCE PCI COUNCIL [28].....28
TABLE 2 5 MAPPING CLOUD AREA WITH COMPLIANCE RELATE.....34
TABLE 2 6 THREAT AND RECOMMENDATION SECURITY COMPLIANCE MODEL [33].....35
TABLE 2 7 INDUSTRIAL SECTOR CORRESPONDING REGULATIONS [3] 35
TABLE 2 8 REQUIREMENTS PCI DSS[37] 36
TABLE 2 9 COMPARATION OF COMPLIANCE WHEN PCI DSS STAND WITH ISO 27001 45
TABLE 2 10 RESULT OF COUNT PCI DSS AND ISO 45
TABLE 2 11 MAPPING PCI DSS WITH COBIT 5 .....**ERROR! BOOKMARK NOT DEFINED.**

TABLE 3 1 RESEARCH FRAMEWORK 55

TABLE 4 1 FGD RESULTS 70