

**ANALYSIS OF INFORMATION TECHNOLOGY AUDIT  
USING COBIT 5 AND COSO FRAMEWORK  
AT PT BANK XYZ INDONESIA, TBK**

By

Yustinus Wahyu Agung Prasetyo  
2-1851-016

MASTER'S DEGREE  
in

CYBER SECURITY & IT GOVERNANCE  
FACULTY OF ENGINEERING & INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY  
SGU<sup>®</sup>

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

Revision After Thesis Defense [15 July 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.

Yustinus Wahyu Agung Prasetyo

Student

Date

Approved by:

SWISS GERMAN UNIVERSITY

Dr. Ir. Mohammad Achmad Amin Soetomo. M.Sc.

Thesis Advisor

Date

Dr. Mulya R. Mashudi, S.T., M.E.M.

Thesis Co-Advisor

Date

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

Dean

Date

Yustinus Wahyu Agung Prasetyo

---

**ABSTRACT**

**ANALYSIS OF INFORMATION TECHNOLOGY AUDIT  
USING COBIT 5 AND COSO FRAMEWORK  
AT PT BANK XYZ INDONESIA, TBK**

By

Yustinus Wahyu Agung Prasetyo  
Dr. Ir. Mohammad Achmad Amin Soetomo. M.Sc., Advisor  
Dr. Mulya R. Mashudi, S.T., M.E.M., Co-Advisor

SWISS GERMAN UNIVERSITY

Bank XYZ provides several digital banking services for various segments, including the D-Bank mobile banking application, XYZ Online Banking, D-Card Mobile for credit card management, D-Financial for SMEs, D-BisMart. for the supply chain, as well as XYZ Trade Connect and Cash Connect for various customer businesses. It is known that 1) IT risk on the D-Bank application is still high. This can be seen from the number of risk events for IT system failure in its application. 2) The handling of IT problems is still not optimal, this can be seen from customer complaints that often reappear in the D-Bank application, such as failed logins, failed transactions and slow performance. 3) Lack of handling of IT Security services. This can be seen from the number of cyber-attacks that have successfully entered the D-Bank application. Data collected through interviews assisted by a questionnaire. The analysis method used is the Cobit analysis method, COSO analysis and the soft system method. The final result shows that there are several domains and principles that need to be considered by management in order to improve the performance of information technology.

*Keywords: COBIT, COSO, D-Bank.*



## **DEDICATION**

I dedicate this works for the future of the country I loved: Indonesia  
and  
my beloved family



## ACKNOWLEDGEMENTS

I wish to thank the members of committee for their support, patience and good humor. Their gentle but firm direction has been most appreciated. Dr. Ir. Mohammad Achmad Amin Soetomo. M.Sc., was particularly helpful in guiding me toward a research methodology. Dr. Mulya R. Mashudi, S.T., M.E.M 's interest in sense of competence was the impetus for my proposal. I would like to thank help from MIT SGU Batch 23 and others for any help. I realize that this thesis is still far from perfect, therefore any mistakes and errors are surely unintentional and they remain mine.

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.



SWISS GERMAN UNIVERSITY

## TABLE OF CONTENTS

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.....	17
1.3 Research Objectives.....	18
1.4 Research Questions.....	18
1.5 Significance of Study.....	19
1.6 Scope and Limitations.....	19
1.7 Hypothesis.....	19
1.8 Thesis Structure.....	20
CHAPTER 2 - LITERATURE REVIEW.....	21
2.1 Information System/Technology.....	21
2.2 Information System Audit.....	22
2.3 Internal Control System.....	23
2.4 COBIT.....	26
2.5 COSO Internal Control Integrated Framework.....	33
2.6 COSO COBIT Mapping.....	37
2.7 Soft System Method.....	39
2.8 Related Works.....	41
CHAPTER 3 – RESEARCH METHODS.....	62
3.1 Research Methodology.....	62
3.2 Research Framework.....	63
3.3 Data collection Methods.....	66
3.4 Data Analysis Methods.....	67
3.5 Matrix Respondents.....	68
3.6 Combined Analysis.....	68

3.7	Method Analysis.....	69
3.8	Validation .....	72
CHAPTER 4 – RESULTS AND DISCUSSIONS.....		74
4.1	Identification of the D-Bank Infrastructure and System Environment.....	74
4.2.	COBIT analysis.....	77
4.2.1	DSS01 - Manage Operations.....	79
4.2.2	DSS02 - Manage Service Request and Incidents .....	80
4.2.3	DSS03 - Manage Problems .....	82
4.2.4	DSS04 - Manage Continuity .....	84
4.2.5	DSS05 - Manage Security Services.....	85
4.2.6	DSS06 - Manage Business Process Control.....	86
4.2.7	COBIT Domain Maturity Level .....	87
4.3.	COSO Analysis.....	90
4.3.1.	Environmental Control .....	90
4.3.2.	Risk Assessment.....	93
4.3.3.	Control Activities .....	95
4.3.4.	Information and Communication .....	97
4.3.5.	Monitoring .....	98
4.4.	COBIT COSO Mapping .....	100
4.4.	Validation.....	107
4.4.1	Expert validation with Lecture IT & Business .....	107
4.4.2	Expert Validation with Head of Technology Risk Management at Global Bank.....	108
4.5.	Implications and System Design Analysis.....	109
CHAPTER 5 – CONCLUSION.....		116
5.1	Conclusions .....	116
5.2	Recommendations .....	117
5.3	Future Works .....	117
GLOSSARY .....		119
Appendix 1 Quisionare Answers – COBIT .....		120
Appendix 2 Quisionare Answers - COSO .....		132
Appendix 3 Documents Reviewed.....		138
Appendix 4 Recommendation to IT Organization Model .....		139
Appendix 5 Omnichannel (D-Bank Project).....		140
Appendix 6 Focus Group Discussion .....		141
Appendix 7 Interview with Expert - Validation I .....		142
Appendix 8 Interview with Expert - Validation II.....		143
REFERENCES .....		145
CURRICULUM VITAE.....		151



## LIST OF FIGURES

	Page
Figure 1. 1 IT Incidents in the last 3 years.....	15
Figure 1. 2 IT Incident Based on Criticality Level .....	16
Figure 1. 3 Sample Incident in ORMS.....	17
Figure 1. 4 Fishbone diagram .....	18
Figure 2. 1 COSO Internal Control Framework Cube .....	34
Figure 2. 2 COSO COBIT Mapping Cube.....	38
Figure 3. 1 Research Methodology .....	63
Figure 3. 2 COBIT 5 PAM - ISACA .....	63
Figure 3. 3 Proposed Research Framework .....	64
Figure 3. 4 Generic Process Reference Model.....	69
Figure 4. 1 Architectural Diagram (Current) .....	74
Figure 4. 2 Architectural Diagram (Proposed) .....	75
Figure 4. 3 Current Data Flow Internet Banking .....	75
Figure 4. 4 Current Data Flow Mobile Banking .....	76
Figure 4. 5 Proposed Data Flow Mobile Banking .....	76
Figure 4. 6 Maturity Level Index .....	89
Figure 4. 7 Environment Control Maturity Index.....	92
Figure 4. 8 Risk Assessment Maturity Index.....	94
Figure 4. 9 Control Activities Maturity Index .....	96
Figure 4. 10 Information and Communication Maturity Index .....	98
Figure 4. 11 Monitoring Maturity Index.....	99
Figure 4. 12 COBIT X COSO Venn Diagram.....	106
Figure 4. 13 D-Bank Governance & Control Model Improvement.....	115

## LIST OF TABLES

Table	Page
Table 2. 1 Comparisons of Internal Control Framework .....	25
Table 2. 2 Mapping of COBIT 5 and COSO (ISACA, 2014).....	39
Table 2. 3 Previous work and research position .....	41
Table 3. 1 Correspondent's Profiles.....	68
Table 3. 2 COSO Principles .....	71
Table 4. 1 Level of attainment of governance maturity (ISACA 2012) .....	77
Table 4. 2 ISO / IEC 15504 rating scale (ISACA 2013) .....	78
Table 4. 3 Level of Achievement in Performance Management and Conformity Monitoring. DSS01 - Manage Operations .....	79
Table 4. 4 Level of Achievement in Performance Management and Conformity Monitoring. DSS02 - Manage Service Request and Incidents .....	81
Table 4. 5 Achievement Levels of Performance Management and Conformity Monitoring. DSS03 - Manage Problems.....	83
Table 4. 6 Achievement Levels of Performance Management and Conformity Monitoring. DSS04 - Manage Continuity.....	84
Table 4. 7 Level of Achievement in Performance Management and Conformity Monitoring. DSS05 - Manage Security Services .....	85
Table 4. 8 Level of Achievement in Performance Management and Conformity Monitoring. DSS06 - Manage Business Process Control .....	86
Table 4. 9 Level of Achievement in Performance Management and Conformity Monitoring. Environmental Control .....	91
Table 4. 10 Level of Achievement in Risk Assessment Performance Management and Compliance Monitoring .....	93
Table 4. 11 Achievement Levels of Performance Management and Monitoring of Conformity Control Activities .....	95
Table 4. 12 Level of Achievement in Performance Management and Monitoring of Control Activities Conformity .....	97
Table 4. 13 Level of Achievement in Performance Management and Monitoring Compliance Monitoring .....	99
Table 4. 14 COBIT COSO Mapping .....	101
Table 4. 15 CATWOE of the D-Bank .....	113
Table 4. 16 D-Bank Management Performance Measurement.....	113