SECURED INFORMATION TECHNOLOGY INFRASTRUCTURE MAINTENANCE FRAMEWORK

FIRKHAN ALI BIN HAMID ALI

UNIVERSITI SAINS ISLAM MALAYSIA

SECURED INFORMATION TECHNOLOGY INFRASTRUCTURE MAINTENANCE FRAMEWORK

Firkhan Ali Bin Hamid Ali
4150136

Thesis submitted in fulfillment for the degree of
DOCTOR OF PHILOSPOPHY
IN SCIENCE AND TECHNOLOGY

Faculty of Science and Technology
UNIVERSITI SAINS ISLAM MALAYSIA

June 2022

AUTHOR DECLARATION

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged

Date : 2nd June 2022

Signature:
Name : Firkhan Ali Bin Hamid Ali
Matric No : 4150136
Address : Taman Sri Mutiara, Batu Pahat, Johor

BIODATA OF AUTHOR

Firkhan Ali bin Hamid Ali (4150136) is an academician in the Information and Communication Technology (ICT) at public university. He has published widely in the areas of Computer Networking, Information Security and Information Technology. He has researched, consulted and taught in the area of Information and Communication Technology since in 1999.

He has been head of Judges Panel in Malaysian-ASEAN Myskills Competition for 2010 in field of IT PC Network. He has been member of Malaysia Industry Expert in IT02-00, Information and Communication Technology with registration number J083 by Department of Skills Development, Ministry of Human Resources for 2009 - 2011.

ACKNOWLEDGEMENT

The great of praise is to Allah S.W.T for giving me the opportunity, time and effort to complete in this thesis. Then, I really hope that it will contribute to the continuously knowledge in the future.

Selawat and Salam for Nabi Muhammad S.A.W.

I want to express my deep appreciation to my supervisor, Prof. Madya Dr. Mohd Zalisham bin Jali that had given me a good supervision, valuable of guidance and support to complete this study.

I am deeply indebted to MOHE, FSKTM and UTHM for his outstanding contribution and support that gives me permission to done this study and including all the staffs of faculty and university for their co-operation.

I am really appreciating the role that all participants of the study especially for experts and interviewees for their effort, dedication and support in sharing the knowledge and experiences in the field of IT Security and research field.

I owe a great debt of gratitude to my father, Hamid Ali Bin Akhbar Ali and mum, Rahmah Talib for her prays, advices and support along the way in my life. Thanks a lot to my late father in law, Allahyarham Monhadi and late mother in law, Allahyarhamah Kasini for supporting me along this study before.

Lastly, I want to express my deep appreciation for the support, understanding and encouragement of my beloved wife, Norsalina Monhadi and five of our kindness sons and daughters, Fatihah Insyirah, Muhammad Al-Fatih, Muhammad Al Ameen, Rufayda Ameena and Muhammad Al Fathan. Thanks a lot to all the contributors especially Dr. Kamaruddin Malik Mohamad. Allah Taala bless all of us every time.

ABSTRAK

Penyelenggaraan keselamatan infrastruktur teknologi maklumat telah mendapat perhatian luar biasa dalam beberapa tahun kebelakangan ini bermula daripada sebuah syarikat kecil sehingga ke agensi kerajaan. Namun begitu, kelebihan penggunaannya bersifat fleksibiliti dan skalabiliti dengan pelaburan awal rendah dibayangi oleh cabaran keselamatan yang menganggu gugat perlaksanaannya. Khususnya, implementasi infrastruktur teknologi maklumat yang fleksibel tetapi kompleks telah terdedah kepada pelbagai jenis ancaman keselamatan bermula daripada masalah kecil seperti kesilapan konfigurasi sehingga menyebabkan berlakunya insiden keselamatan. Isu ini berlarutan dengan sebahagian besar kerangka kerja penyelenggaraan keselamatan teknologi maklumat (IT) yang digunakan mempunyai kekurangan dari segi pelaksanaan kerana kerumitan, tidak ada piawai tindakan dan bertujuan hanya untuk mengumpulkan maklumat dengan tujuan dokumentasi. Ditambah lagi dengan keterbatasan penyelidikan ilmiah menunjukkan keperluan penyediaan dalam menyatakan dengan terperinci setiap langkah bagi pendekatan proses yang diurus dengan berstruktur dalam pengurusan kerangka penyelenggaraan keselamatan teknologi maklumat bagi sesebuah organisasi. Oleh itu, objektif utama penyelidikan ini adalah untuk membangunkan kerangka kerja penyelenggaraan keselamatan IT untuk infrastruktur teknologi maklumat. Kajian ini telah menggunakan kaedah campuran dan *explanatory sequential research* untuk mencapai objektif kajian. Pertama, tinjauan literatur yang meluas telah dilakukan. Kemudian, kaedah kuantitatif dimulakan dengan kajian deskriptif untuk menentukan komponen kerangka penyelenggaraan keselamatan IT. Sebanyak 271 responden terlibat melalui kaedah persampelan *simple random* untuk mengambil bahagian dalam pengumpulan data kuantitatif. Oleh itu, soal selidik berskala Likert diedarkan dan penemuannya dianalisis dengan menggunakan kaedah analisis statistik seperti Keizer-Meyer dan *Bartlett's Test*. Seterusnya, kaedah kualitatif digunakan untuk mengesahkan kerangka kerja yang dicadangkan sesuai dengan situasi sebenar penyelenggaraan keselamatan IT dan kegunaannya kepada organisasi yang disasarkan. Temu ramah separa struktur yang mendalam telah dijalankan ke atas enam orang pakar dalam bidang keselamatan dan infrastruktur IT. Hasil daripada temu ramah ini dianalisis isi kandungan dan kiraan statistik hasilnya. Hasil daripada penyelidikan ini telah berjaya mengembangkan kerangka penyelenggaraan keselamatan IT untuk infrastruktur IT. Kerangka yang dicadangkan terdiri daripada (1) pengenalpastian aset IT, (2) pengenalpastian pencerobohan keselamatan IT, (3) perlindungan ofensif keselamatan IT, (4) perlindungan pertahanan keselamatan IT dan (5) objektif perlindungan keselamatan IT. Kerangka kerja yang dicadangkan menyumbang kepada bidang penyelenggaraan keselamatan teknologi maklumat dalam organisasi. Rangka kerja yang dicadangkan memberi kesedaran untuk mengetahui terlebih dahulu perkara yang harus dilakukan dan sejauh mana pencapaian dalam tindakan praktikal bagi pengurusan keselamatan teknologi maklumat. Akhirnya, kerangka yang dicadangkan ini dapat memberikan maklumat berkualiti dalam menentukan arah pelaksanaan pengurusan keselamatan teknologi maklumat untuk infrastruktur IT.

ABSTRACT

Security maintenance of information technology (IT) infrastructure has gained tremendous popularity in recent years according to the diversity of the types of organizations involved from a small company to the government. However, the requirements of flexibility, scalability, and inexpensive initial investment in the usage of IT infrastructure are eclipsed by security concerns that stymie adoption. The information technology infrastructure, in particular, is highly adaptable but complicated, and it has been vulnerable to a variety of security threats, ranging from simple issues such as incorrect configuration to an IT security incident. Then, most of the existing IT security maintenance frameworks had lack of implementation because of complexity, no standard of action, and just for gathering information only. Moreover, a limited scholarly investigation has been undertaken to present a need for properly defined steps of the process approach in which a structured way of managing the IT security maintenance framework within any organization is provided. As a result, the primary goal of this study is to create a framework for IT infrastructure security maintenance. To attain the objectives, the study used a mixed-method technique in an explanatory sequential research. Firstly, an extensive literature review had been done. Then, the quantitative method begins with a descriptive study in order to determine components of the IT security maintenance framework. A total of 271 respondents were involved through a simple random sampling method to participate in the quantitative data collection. Likert structured type of closed questionnaire was distributed and the finding had been analyzed by using statistical analysis methods like Keiser-Meyer-and Bartlett's Test. The suggested framework is validated using a qualitative method to ensure that it conforms to the current state of IT security infrastructure and is relevant to the targeted organization. Six experts in the disciplines of IT security and infrastructure participated in an in-depth semi-structured interview. Then, doing content and statistical analysis on the results of the findings. The results from this research managed to develop an IT security maintenance framework for IT infrastructure. (1) IT asset identification, (2) IT security breach identification, (3) IT security offensive protection, (4) IT security defensive protection, and (5) IT security objective protection are all part of the suggested framework. The proposed framework contributes to the field of IT security maintenance in the organization. The proposed framework provides awareness on knowing beforehand what to do and to what extent they are already conquering in the action of practical holistic information security management. Lastly, the proposed framework provides quality information for getting direction in the implementation of security maintenance for IT infrastructure.

امللخص

اكتسبت الصيانة الأمنية للبنية التحتية لتكنولوجيا المعلومات (IT) شعبية هائلة في السنوات الأخيرة وفقًا لتنوع أنواع المنظمات المشاركة من شركة صغيرة إلى الحكومة .ومع ذلك ، فإن متطلبات المرونة وقابلية التوسع والاستثمار الأولي غير المكلف في استخدام البنية التحتية لتكنولوجيا المعلومات قد طغت عليها المخاوف الأمنية التي تعيق تبنيها .البنية التحتية لتكنولوجيا المعلومات ، على وجه الخصوص ، قابلة للتكيف بدرجة كبيرة ولكنها معقدة ، وكانت عرضة لمجموعة متنوعة من التهديدات الأمنية ، بدءًا من المشكلات البسيطة مثل التكوين غير الصحيح إلى حادث أمان تكنولوجيا المعلومات .بعد ذلك ، كانت معظم أطر صيانة أمن تكنولوجيا المعلومات الحالية تفتقر إلى التنفيذ بسبب التعقيد ، وعدم وجود معيار للعمل ، ولجمع المعلومات فقط .علاوة على ذلك ، تم إجراء تحقيق علمي محدود لتقديم الحاجة إلى خطوات محددة بشكل صحيح لنهج العملية التي يتم فيها توفير طريقة منظمة لإدارة إطار عمل صيانة أمن تكنولوجيا المعلومات داخل أي مؤسسة .نتيجة لذلك ، فإن الهدف الأساسي لهذه الدراسة هو إنشاء إطار عمل لصيانة أمن البنية التحتية لتكنولوجيا المعلومات .لتحقيق الأهداف ، استخدمت الدراسة أسلوب الطريقة المختلطة في بحث توضيحي متسلسل .أولاً ، تم إجراء مراجعة شاملة للأدبيات .بعد ذلك ، تبدأ الطريقة الكمية بدراسة وصفية لتحديد مكونات إطار عمل صيانة أمن تكنولوجيا المعلومات .شارك ما مجموعه 271 مستجيبًا من خلال طريقة أخذ عينات عشوائية بسيطة للمشاركة في جمع البيانات الكمية .تم توزيع نوع ليكرت المهيكل من الاستبيان المغلق وتم تحليل النتيجة باستخدام طرق التحليل الإحصائي مثل اختبار-Keizer Meyerو .Bartlett يتم التحقق من صحة الإطار المقترح باستخدام طريقة نوعية للتأكد من أنه يتوافق مع الوضع الحالي للبنية التحتية لأمن تكنولوجيا المعلومات وأنه وثيق الصلة بالمنظمة المستهدفة .شارك ستة خبراء في تخصصات أمن تكنولوجيا المعلومات والبنية التحتية في مقابلة متعمقة شبه منظمة .ثم عمل المحتوى والتحليل الإحصائي لنتائج النتائج .تمكنت نتائج هذا البحث من تطوير إطار عمل صيانة أمن تكنولوجيا المعلومات للبنية التحتية لتكنولوجيا المعلومات (1) .تحديد أصول تكنولوجيا المعلومات ، (2) تحديد خرق أمن تكنولوجيا المعلومات ، (3) الحماية الهجومية لأمن تكنولوجيا المعلومات ، (4) الحماية الدفاعية لأمن تكنولوجيا المعلومات ، و (5) حماية أهداف أمن تكنولوجيا المعلومات كلها جزء من إطار العمل المقترح .يساهم الإطار المقترح في مجال صيانة أمن تقنية المعلومات في المنظمة .يوفر الإطار المقترح وعيًا بشأن معرفة ما يجب القيام به مسبقًا وإلى أي مدى يتغلبون بالفعل في عمل الإدارة العملية الشاملة لأمن المعلومات .أخيرًا ، يوفر الإطار المقترح معلومات جيدة للحصول على التوجيه في تنفيذ صيانة الأمان للبنية التحتية لتكنولوجيا المعلومات.

TABLE OF CONTENTS

CONTENT	PAGE
AUTHOR DECLARATION	i
BIODATA OF AUTHOR	ii
ACKNOWLEDGEMENT	iii
ABSTRAK	iv
ABSTRACT	v
AL-MULAKHKHAS	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	x
LIST OF FIGURES	xiii
LIST OF APPENDICES	xiiii
ABBREVIATION	xiv
LIST OF PUBLICATIONS	xv
CHAPTER I : INTRODUCTION	
1.1 Introduction	1
1.2 Background Study	2
1.3 Problem Statement	6
1.4 Research Questions	9
1.5 Objective	10
1.6 Research Scopes	10
1.7 Research Significant	12
1.7.1 Significance to Academic	12
1.7.2 Significance to Practice	13
1.8 Research Methodology	14
1.9 Organization of the Thesis	15
CHAPTER II : LITERATURE REVIEW	
2.1 Introduction	18
2.2 Initial Work on Information Infrastructure	18
2.3 Literature Review Knowledge Framework Overview	20
2.4 Information Technology	21
2.5 Information Technology Infrastructure	24
2.5.1 Physical Information Technology Infrastructure Requirements	24
2.5.2 Logical Information Technology Infrastructure Requirements	31
2.5.3 Information Technology Infrastructure Planning	34
2.5.4 Information Technology Infrastructure Governance	35
2.5.5 Information Technology Infrastructure Limitation	37
2.6 IT Security	39
2.6.1 IT Security Breach	39
2.6.2 IT Security Offensive Protection	45
2.6.2.1 Vulnerability Assessment	45
2.6.2.2 Penetration Testing	48
2.6.2.3 Security Audit	50

2.6.3 IT Security Defensive Protection 52
2.6.4 IT Security Management 61
2.6.5 IT Security Management Model Review 66
2.6.5.1 ISO 27001 69
2.6.5.2 ISO/IEC 27001:2005 (ISMS - Requirements) 69
2.6.5.3 ISO/IEC 27002:2005 (Code of Practice for Info. Sec. Manage.) 70
2.6.5.4 ISO/IEC 13335 (IT Security Management) 72
2.6.6 IT Security Maintenance 73
2.7 Theoretical Conceptual Framework 74
2.8 Chapter Summary 78

CHAPTER III : RESEARCH METHODOLOGY
3.1 Introduction 80
3.2 Research Paradigm 80
3.3 The Rationale of Mix-Methods Approach 82
3.4 Research Design 83
3.5 Population 87
3.6 Sampling Technique 87
3.7 Sample Size 89
3.8 Data Collection 90
3.9 Development of Research Instruments 91
3.10 Participating Respondents 93
3.11 Validity of Instruments 93
3.12 Data Analysis (Reliability and Validity) 94
3.13 Qualitative Method: In-depth Semi-Structured Interview 95
3.13.1 Participating Respondents 96
3.13.2 Framework Validation 97
3.14 Pilot Study 97
3.15 Conceptual Framework 99
3.16 Ethical Assurance 102
3.17 Chapter Summary 102

CHAPTER IV : RESULT AND DISCUSSION
4.1 Introduction 105
4.2 Response Rate and Missing Data 105
4.3 Demographic Profile of Respondents 106
4.4 Reliability 110
4.5 Normality Test 110
4.6 Descriptive Statistics 111
4.6.1 To analyse the Factors Influencing the IT security Maintenance 111
4.6.1.1 IT Asset Identification 112
4.6.1.2 Security Breach Identification 114
4.6.1.3 IT Security Offensive Protection 116
4.6.1.4 IT Security Defensive Protection 118
4.6.1.5 IT Security Objectives 120
4.7 Statistical Test 122
4.7.1 The Relationship Between the factors influencing the IT security Maintenance 122

4.8 Validity of Measurement Model 124
4.9 Confirmatory Factor Analysis (CFA) 127
4.10 Factors Influencing IT Security Maintenance 146
4.10.1 IT Asset Identification 146
4.10.2 Security Breach Identification 148
4.10.3 IT Security Offensive Protection 148
4.10.4 IT Security Defensive Protection 149
4.10.5 IT Security Objectives 150
4.11 Result of Hypothesis Testing 152
4.12 The Result of Framework Validation 153
4.13 Chapter Summary 156

CHAPTER V : CONCLUSIONS AND RECOMMENDATIONS
5.1 Introduction 158
5.2 Conclusion on Verification 158
5.3 Achivement of Objectives 163
5.4 Framework Application 166
5.5 Contributions 167
5.6 Limitation of Study 173
5.7 Direction for Future Research 173
5.8 Recommendations 174

REREFENCES 176

APPENDICES
APPENDIX A: Formal Letter for Doing Research Activity 197
APPENDIX B: Survey Questionnaire 198
APPENDIX C: Expert Report for Questionnaire Items 212
APPENDIX D: Interview Form for Framework Validation 214
APPENDIX E: Respondent's Response on Framework Validation 217

LIST OF TABLES

Tables	Page
Table 1.1: Research Problem, Questions, Activities and Outcome	15
Table 2.1: International standard for ISP	67
Table 3.1: Determining Sample Size	89
Table 3.2: Reliability range of items	95
Table 3.3: Respondent's Profile	96
Table 3.4: The Result of Reliability Test for Pilot Study	99
Table 4.1: Survey Response Rate	105
Table 4.2: Company Profile	107
Table 4.3: Profile of Interviewee	108
Table 4.4: Distribution of Information Security Environment	109
Table 4.5: Test of Reliability	110
Table 4.6: Test of Normality for Each Factor	111
Table 4.7: Frequencies and Percentages for IT Asset Identification	113
Table 4.8: Frequencies and Percentages for Security Breach Identification	115
Table 4.9: Frequencies and Percentages for IT Security Offensive Protection	117
Table 4.10: Frequencies and Percentages for IT Security Defensive Protection	119
Table 4.11: Frequencies and Percentages for IT Security Objectives	121
Table 4.12: Correlation the Variables	123
Table 4.13: Factor Analysis of IT Asset Identification	124
Table 4.14: Factor Analysis of Security Breach Identification	125
Table 4.15: Factor Analysis of IT Security Offensive Protection	125
Table 4.16: Factor Analysis of IT Security Defensive Protection	126

Table 4.17: Factor Analysis of IT Security Objectives 127

Table 4.18: Sampling Adequacy and Sphericity 133

Table 4.19: Collinearity Statistics 134

Table 4.20: CFA Cut Off Values 135

Table 4.21: FL, AVE, CR and Discriminant Validity of Asset Identification Scale 136

Table 4.22: Model Fit Statistics for Asset Identification Scale 137

Table 4.23: FL, AVE, CR and Discriminant Validity of Security Breach Identification Scale 137

Table 4.24: Model Fit Statistics for Security Breach Identification Scale 138

Table 4.25: FL, AVE, CR and Discriminant Validity of Security Offensive Protection Scale 139

Table 4.26: Model Fit Statistics for Security Offensive Protection Scale 140

Table 4.27: FL, AVE, CR and Discriminant Validity of Security Defensive Protection Scale 141

Table 4.28: Model Fit Statistics for Security Defensive Protection Scale 142

Table 4.29: FL, AVE, CR and Discriminant Validity of Security Objectives Scale 142

Table 4.30: Model Fit Statistics for Security Objectives Scale 143

Table 4.31: Model Fit Statistics for Measurement Model 143

Table 4.32: AVE, CR and Discriminant Validity of the Measurement Model 144

Table 4.33: Result of Hypothesis 153

Table 4.34: Rating Results of the Framework Validation 154

Table 4.35: Summary of Respondent's Response on Validation Framework's question 155

LIST OF FIGURES

Figures	Page
Figure 1.1: Cybersecurity Incident Report 2020	3
Figure 2.1: Topics Cover in Literature Review	21
Figure 2.2: Physical of IT Requirements	26
Figure 2.3: Logical of IT Requirements	31
Figure 2.4: IT Security Breach	40
Figure 2.5: Proposed IT Security Maintenance Framework	77
Figure 3.1: Research Procedure	82
Figure 3.2: Research Design	85
Figure 3.3: Input-Process-Output Model of Proposed Framework	100
Figure 3.4: Main Hypotheses of Research Framework	102
Figure 4.1: CFA Graphic Model	145

LIST OF APPENDICES

Appendices	Page
Appendix A: Formal Letter for Doing Research Activity	197
Appendix B: Survey Questionnaire	198
Appendix C: Expert Report for Questionnaire Items	212
Appendix D: Interview Form for Framework Validation	214
Appendix E: Respondent's Response on Framework Validation	217

ABBREVIATION

IT	Information Technology
SME	Small Medium Enterprise
ISMS	Information Security Management System
ISO	International Standard Organization
SMB	Small Medium Business
IDC	International Data Corporation
CIO	Chief Information Officer
ENISA	European Network and Security Administration
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
SLA	Service Level Agreement
IDS	Intrusion Detection System
ISP	Information Security Policy
BSI	British Standards Institution
PDCA	Plan-Do-Check-Act
CISO	Chief Information Security Officer

LIST OF PUBLICATIONS

Firkhan Ali Bin Hamid Ali, Mohd Zalisham Jali (2019). Intelligent Human-Technology Based In Digital Security Maintenance for IT Infrastructure. Paper presented at 2019 IEEE Symposium on Acoustic, Speech and Signal Processing (Universiti Teknologi Petronas, Center for Advance and Professional Education (Cape), Kuala Lumpur).

Firkhan Ali Bin Hamid Ali, Mohd Zalisham Jali (2018). Human-Technology Centric In Cyber Security Maintenance for Digital Transformation Era, *Journal of Physics: Conference Series* 1018 (1), 012012.

Firkhan Ali Bin Hamid Ali, Mohd Zalisham Jali (2018). Human-Technology Centric in Cyber Security Maintenance for Digital Transformation Era. Paper presented at 8th edition of the International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT 18) by Sfax University and IEEE Tunisia Section. 18-20 December 2018.

Firkhan Ali Hamid Ali, Mohd Zalisham Jali (2017). Cyber Security Maintenance Based on Human-Technology Aspects in Digital Transformation Era, *Journal of Education and Social Sciences* , Zes Rokman Resources (2131022-P) , 10, 279, ISSN:22891552

Firkhan Ali Hamid Ali, Mohd Zalisham Jali (2017). A Study of Security Management Model for IT Infrastructure Maintenance. Paper presented at Seminar on Information Retrieval and Knowledge Management 2017 (SIRKM'17). UPM Serdang. 19 July 2017.

Firkhan Ali Bin Hamid Ali, Mohd Zalisham Jali (2016). An Overview of Conceptual Model for Security Maintenance in IT Infrastructure. National Conference on Education and Social Sciences 2017 (NACESS 2016). OUM Seremban. 16 November 2016.