



INFORMATION QUALITY STRUCTURE FRAMEWORK IN DEVELOPING AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

P SIVA SHAMALA PALANIAPPAN

DOCTOR OF PHILOSOPHY

2017



Faculty of Information and Communication Technology

**INFORMATION QUALITY STRUCTURE FRAMEWORK IN
DEVELOPING AN INFORMATION SECURITY MANAGEMENT
SYSTEM (ISMS)**

P SIVA SHAMALA PALANIAPPAN

Doctor of Philosophy

2017

**INFORMATION QUALITY STRUCTURE FRAMEWORK IN DEVELOPING AN
INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)**

P SIVA SHAMALA PALANIAPPAN

**A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy**

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I declare that this thesis entitled “Information Quality Structure Framework In Developing An Information Security Management System (ISMS)” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature :

Name : P SIVA SHAMALA PALANIAPPAN

Date :

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Doctor of Philosophy.

Signature :
Supervisor Name : PROF. DR. RABIAH AHMAD
Date :

DEDICATION

To my beloved mother, father, husband, son, daughters and family.

ABSTRACT

Organisations are progressively aware that information security is an important aspect of their business strategy. The awareness make organisations to achieve an ideal level of management system to establish and maintain a secure information environment. Hence, organisations are currently applying for information security management system (ISMS) to effectively manage their information assets. ISMS will ensure that the right people, processes and technologies are in place, and facilitates a proactive approach to manage security and risk. Unfortunately, limited scholarly investigation has been undertaken to present a need of properly defined steps of process approach in which a structured way of managing ISMS within an organisation is provided. This is due to the well-known process approach, “Plan-Do-Check-Act” lifecycle model which is unable to give information on how organisations should develop security objectives and ISMS strategies. Also, there are no recognized and standard ISMS frameworks for action. The lack of standardized and trustable ISMS methods, and complexity of ISMS standards has caused practitioners to face difficulties in understanding the ISMS requirements. However, after the daunting task on choosing one preferred methods, practitioners are also required to gather information to complete all the ISMS requirement planning. Practically, practitioners gather information in a surveillance mode rather than in decision mode. Hence, practitioners are required to evaluate the collected information resource in order to eliminate all the “garbage” information. Therefore, this research aims to provide an Information Quality Structure Framework for ISMS. This study adopts a mixed method and explanatory sequential approaches to achieve the research objectives. After an extensive literature review, the quantitative study begins with descriptive study in order to determine components of information structure. Then Likert structured questionnaire was distributed and the findings have been analyzed using Rasch Measurement Model (RMM) and SEM-PLS. Qualitative analysis was done by validating the framework on ensuring the proposed framework conforms to real working ISMS specification and its usefulness for organisations. Semi-structured interview among six expert panel in ISMS industry were conducted. The results from this study, managed to develop Information Quality Structure Framework for ISMS. The proposed framework consists of (1) information structure focuses on providing layout of information which is organized in a way, in which the components are put together to form a meaningful structure which can be navigated at any time and (2) quality dimensions: accuracy, objective, completeness, reliability and verifiability ensure the quality of information and (3) provide a synthesis of information quality dimensions parameters to ensure the quality of information is emphasized throughout the ISMS process. The proposed framework contributes to the field of ISMS, certification area and also contributes information quality theory in ISMS field. The proposed framework provides an awareness on knowing beforehand what to do and to what extent they are already conquering the quality information needed for getting clear direction and to develop ISMS.

ABSTRAK

Organisasi menyadari bahawa keselamatan maklumat merupakan aspek penting dalam strategi perniagaan. Kesedaran ini mendorong organisasi untuk mencapai tahap sistem pengurusan yang ideal bagi mewujudkan dan mengekalkan persekitaran maklumat yang terjamin. Oleh itu, organisasi kini melaksanakan sistem pengurusan keselamatan maklumat (information security management system, ISMS) bagi mengurus aset maklumat dengan berkesan. ISMS akan memastikan bahawa individu, proses, dan teknologi yang tepat tersedia dan memudahkan pendekatan proaktif bagi menguruskan keselamatan dan risiko. Namun begitu, masih sedikit bilangan penyelidikan ilmiah yang mengkaji pendekatan proses yang jelas, yang mencadangkan kaedah berstruktur menguruskan ISMS dalam sesebuah organisasi. Ini kerana pendekatan proses yang diketahui umum, iaitu model kitaran hayat “Rancang-Buat-Semak-Bertindak”, yang tidak mampu menerangkan cara yang sepatutnya dilakukan oleh sesebuah organisasi untuk membangunkan objektif keselamatan dan strategi ISMS. Tambahan pula, tiada spesifikasi rangka kerja ISMS yang diiktiraf untuk tindakan. Kekurangan kaedah ISMS yang dipercayai, serta kerumitan piawaian ISMS menyukarkan pengamal ISMS untuk memahami keperluan ISMS. Walau bagaimanapun, selepas pemilihan kaedah ISMS yang diperlukan, pengamal juga perlu mengumpul maklumat untuk melengkapkan kesemua perancangan keperluan ISMS. Pengamal mengumpul maklumat dalam mod pengawasan dan bukannya dalam mod membuat keputusan. Maka, pengamal perlu menilai sumber maklumat terkumpul untuk menyingkirkan maklumat “tak terpakai”. Oleh itu, kajian ini bertujuan untuk menyediakan Rangka Kerja Struktur Kualiti Maklumat untuk ISMS. Kajian ini menggunakan kaedah gabungan dan pendekatan penerangan berurutan. Selepas proses sorotan kajian yang menyeluruh, kajian kuantitatif bermula dengan kajian deskriptif untuk menentukan komponen-komponen struktur maklumat. Kemudiannya, borang soal selidik berstruktur Likert diedarkan dan dapatan soal selidik ini dianalisis menggunakan Model Pengukuran Rasch dan SEM-PLS. Analisis kualitatif dijalankan dengan mengesahkan rangka kerja yang dicadangkan mematuhi spesifikasi ISMS yang betul serta kegunaannya kepada organisasi. Temu bual separa berstruktur diadakan dalam kalangan enam orang panel pakar dalam industri ISMS. Hasil temu bual digunakan untuk membangunkan Rangka Kerja Struktur Kualiti Maklumat untuk ISMS. Rangka kerja yang dicadangkan terdiri daripada; (1) struktur maklumat yang khususnya menyediakan susun atur maklumat yang terancang supaya komponen diletakkan bersama untuk membentuk struktur yang bermakna, yang boleh dilayari pada bila-bila masa; (2) dimensi berkualiti: ketepatan, bersifat objektif, lengkap, kebolehpercayaan, dan kebolehan ditentusahkan memastikan kualiti maklumat; dan (3) menyediakan gabungan parameter dimensi kualiti maklumat untuk memastikan kualiti maklumat diberi penekanan sepanjang proses ISMS. Rangka kerja ini menyumbang kepada bidang ISMS, skop pensijilan dan juga menyumbang teori kualiti maklumat kepada bidang ISMS. Rangka kerja ini memberi kesedaran bahawa pengamal perlu mengetahui terlebih dahulu perkara yang perlu dilakukan dan sejauh mana perkara tersebut menguasai maklumat berkualiti yang diperlukan untuk memperoleh hala tuju yang jelas dan untuk membangunkan ISMS yang berkesan.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to the Almighty God, for giving me the strength, patience, knowledge, and good health, without which, would have been impossible to complete this thesis successfully.

I am very thankful to my dearest panel of supervisors which consists of:

- a) Professor Dr. Rabiah Ahmad for her in-depth comments, moral support, consistent support in terms of content, direction of the research, and overwhelming stream of ideas.
- b) The late Dr. Mariana Yusoff, for her commitment, encouragement and comments to improve my research and for her professional views. Dr, you are always in my heart and I miss you very much!
- c) Professor Datuk Dr. Shahrin Sahib for his assistance over the course of this research.

Life as a PhD student, a wife to a PhD student, and a mother of three children, with limited sources of income have never been easy. Thus, the completion of this thesis has been made possible only through the encouragement and support of many family members.

First, special thanks go to my beloved husband, Mr. Muruga Chinniah. Despite being a PhD student himself and facing similar problems and challenges, he has always been there whenever I needed support. I could certainly not have completed this journey without him.

A very special note of thanks to my parents- Mr. Palaniappan & Palaniamah for their care and unquestionable love, encouragement and prayers. For my children- Rheshvan, Maythienie, Nikshanaa, and nephews Pranav and Kailash, who always made my life worth living and their love is a gift I open every day. My siblings- Mrs Sivamalar and Mr Sivanesan who always cheered me up when I was down. I will always love you all.

This acknowledgement is also dedicated to the Ministry of Higher Education Malaysia and Universiti Tun Hussein Onn Malaysia (UTHM) for providing financial support during the course of my PhD.

TABLE OF CONTENTS

	PAGE
DECLARATION	
APPROVAL	
DEDICATION	
ABSTRACT	i
ABSTRAK	ii
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	viii
LIST OF FIGURES	xii
LIST OF APPENDICES	xiv
LIST OF ABBREVIATIONS	xv
LIST OF PUBLICATIONS	xvii
CHAPTER	
1. INTRODUCTION	1
1.1 General Overview	1
1.2 Problem Background	3
1.3 Statement of the Problem	5
1.4 Research Questions	9
1.5 Objectives of the Study	11
1.6 Scope of the Study	16
1.7 Significance of the Study	18
1.8 Structure of Thesis	21
2. LITERATURE REVIEW	24
2.1 Introduction	24
2.2 Operational Definition	26
2.2.1 Information Security	26
2.2.2 Risk Management	26
2.2.3 Risk Assessment	27
2.2.4 Risk Analysis	27
2.2.5 Risk Evaluation	28
2.2.6 Risk Treatment	28
2.2.7 Risk Acceptance	29
2.2.8 Information Security Management System	29
2.3 Overview of Information Security	30
2.4 Overview of Information Security in Malaysia	32
2.4.1 ISO/IEC 27001	36
2.5 Information Security Management System Methodologies	39
2.6 Research Motivation: Lacking in Information Security Management System	41
2.6.1 Comparison among Supporting Literature on Existing ISMS Methodologies	44
2.6.2 Review on Selected Methodologies	48
2.6.3 Comparison Processes to Identify the Similarities in ISMS	54
2.6.4 List of Activities that Require Information in ISMS	58

2.7	Research Motivation: Lacking in Information Security Risk Assessment (ISRA's) Asset Identification	62
2.7.1	ISRA towards Non-Technical Perspective Assets	64
2.7.1.1	Issues in Knowledge	66
2.7.1.2	Issues in Data and Information Assets	70
2.7.2	Technical and Non-Technical Perspective Assets in ISRA's Asset Identification	74
2.8	Components of Information Structure for ISMS	75
2.9	Research Motivation: Integrating Information Quality (IQ) into ISMS	78
2.9.1	Overview of Information Quality	81
2.9.1.1	Classification of Information Quality Dimensions	83
2.9.1.2	Measuring Information Quality	87
2.9.2	Identifying Information Quality Dimensions for ISMS	88
2.9.3	Similarity Situation between Information Quality Dimensions in Web and ISMS	89
2.9.4	Information Quality Dimensions for ISMS	90
2.10	Developing the Research Conceptual Framework	92
2.11	Summary	95
3.	METHODOLOGY	97
3.1	Introduction	97
3.2	Research Paradigm: Pragmatic	98
3.2.1	Research Approach: Mixed Method	100
3.3	Research Design	102
3.4	Developing the Research Conceptual Framework	104
3.5	Research Plan: Techniques and Procedures	109
3.6	Phase One: Literature Review	115
3.6.1	Literature Review to Identify the Mutual Components in Information Structure	115
3.6.2	Literature Review to Identify the Non-Technical Perspective Assets	118
3.6.3	Literature Review to Identify the Information Quality Dimensions for ISMS	120
3.7	Phase Two: Descriptive Study	121
3.7.1	Questionnaire Survey	122
3.7.1.1	Questionnaire Development	123
3.7.1.2	Questionnaire Revision	126
3.7.1.3	Survey Distribution	126
3.7.1.4	Data Analysis	128
3.8	Phase Three: Framework Development	128
3.8.1	Quantitative Approach: Questionnaire Survey	128
3.8.1.1	Questionnaire Development	130
3.8.1.2	Pilot Test	131
3.8.1.3	Survey Distribution	131
3.8.1.4	Data Analysis Using Two Techniques	133
3.8.1.4.1	Data Analysis Using Rasch Measurement Model (RMM)	135
3.8.1.4.2	Data Analysis Using PLS-SEM	138
3.8.2	Qualitative Approach: Semi-Structured Interview	140

3.9	Pilot Study	141
3.9.1	Content Validity	142
3.9.2	Validity using Rasch Model	143
3.9.2.1	Dimensionality: Principal Component Analysis (PCA)	143
3.9.2.2	Item Polarity	145
3.9.2.3	Reliability	147
3.9.3	Validity using SPSS for Section 2 and Section 3	149
3.10	Quantitative Sampling Technique	150
3.11	Phase Four: Framework Validation	154
3.11.1	Identifying the Experts and Sampling Technique	154
3.11.2	Qualitative Instrument	154
3.12	Summary	156
4.	DESCRIPTIVE STUDY	158
4.1	Introduction	158
4.2	Components of Information Structure	159
4.3	Sample Characteristics	160
4.4	Survey Results	162
4.4.1	Section 2: Profile of ISMS Firms	163
4.4.1.1	Information Security Policy	164
4.4.2	Section 3: ISMS Management Requirement	166
4.4.2.1	Criteria for Hiring/Promoting Information Security Practitioners	168
4.4.2.2	Types of Risk Assessment Documentations	169
4.4.2.3	Pre-requisite Management Input	170
4.4.3	Section 4: Establish Organizational Context & Identify Asset, Threat and Vulnerability	174
4.4.3.1	Establishment of Organizational Context	175
4.4.3.2	Information Gathering Techniques	177
4.4.3.3	Important Assets to be Protected	178
4.4.4	Section 5: Risk Management Improvement	182
4.4.4.1	Information Security Training	183
4.4.4.2	Self-Development Program	184
4.4.4.3	Reassessment Schedule	186
4.4.4.4	Awareness Program Checklist	187
4.5	Descriptive Study Findings for Phase 3	189
4.6	Summary	190
5.	ANALYSIS RESULTS AND VALIDATION	191
5.1	Introduction	191
5.2	Sample Characteristics	192
5.3	Data analysis: An Overview	195
5.4	Part One: Components of Information Structure	196
5.4.1	Reliability of Real Survey	197
5.4.2	Construct Validity (Personal Component Analysis (PCA))	197
5.4.3	Item Hierarchy on Information Structure For ISMS	198
5.4.4	Item Measure Quality for Information Structure	200
5.5	Part Two: PLS-SEM Analysis	206
5.5.1	Data Screening	206

5.5.1.1	Detection of Missing Data	206
5.5.1.2	Detection of Outliers	207
5.5.1.3	Normality Test	207
5.5.2	Analysis and Results of Measurement Models	208
5.5.3	Analysis and Results of Structural Model	215
5.6	Part Three: Characteristics of Information Quality Dimensions	220
5.6.1	Reliability of Real Survey	220
5.6.2	Construct Validity (Personal Component Analysis (PCA))	221
5.6.3	Item Hierarchy on Information Quality Dimensions	222
5.6.4	Item Measure Quality for Information Quality Dimensions	223
5.7	Quantitative Analysis Results	226
5.8	Summary	226
6.	VALIDATION AND SYNTHESIS	228
6.1	Introduction	228
6.2	Validation and Synthesis through Expert Reviews	228
6.2.1	Experts for Semi-Structured Interview	229
6.3	Findings on Expert Review Validation	231
6.3.1	Validation Findings on Components Suitability in the Framework	231
6.4	Development of Information Quality Structure Framework	242
6.5	Findings on Synthesized Information Quality Dimensions	249
6.6	Experts Review on Framework Usefulness	253
6.7	Comparison Proposed Framework with PDCA	257
6.8	Summary	262
7.	DISCUSSION AND CONCLUSION	263
7.1	Introduction	263
7.2	Summary of the Research	264
7.3	Conclusion on the Research Objectives	267
7.3.1	Research Objective 1	268
7.3.2	Research Objective 2	272
7.3.3	Research Objective 3	277
7.4	Contribution	278
7.5	Limitations of the Study	282
7.6	Future Research	283
7.7	Summary	284
	REFERENCES	286
	APPENDICES	319

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Elaboration on the Methods Used to Answer the RQ	14
2.1	List of ISMS Methodologies Issued By Organization	39
2.2	Supporting Literature of ISMS methodology	38
2.3	Details of ISMS Methodologies used for Comparison	49
2.4	The Six Types of Methodologies Flowchart Diagram Conducting Risk Assessment	52
2.6	Comparative Study to Specify the Sub-Components for Each Main Component which are the Most often Agreed Components by Methodologies	56
2.7	Analysis on Non-Technical Perspective Assets	65
2.8	Types of Media Commonly Contain Information	73
2.9	Classifications of Information Quality Dimensions	84
2.10	Summary and Frequency of the Information Quality Dimensions Frameworks	91
3.1	Response Pattern	123
3.2	Response Pattern	132
3.3	Interpretation on Mean Square Value	136
3.4	Interpretation on Zstd Value	137
3.5	PLS Measurement Model Validity Test	139
3.6	Rating Scale Instrument Quality Criteria for PCA	143
3.7	Item Polarity for Section 1: Information Structure	146
3.8	Item Polarity for Section 2: Information Structure	147
3.9	Rating Scale Instrument Quality Criteria	148
3.10	Person and Item Reliability for Questionnaire Survey in this Research	148
3.11	Person and Item Reliability for Questionnaire Survey in this Research	149
3.12	Sampling Size and Logit for Item Calibration	151
3.13	Sampling Frame (Quantitative Phase 2 and Phase 3)	153
4.1	Sample Characteristics of Respondents	160
4.2	Characteristics of the Responding Organization Profile	163
4.3	Information Security Policies and Procedures In Place to Respond to Threats	165
4.4	Types of Reference Points Used for Developing Information Security Policies	166
4.5	Established Guideline of Reference in Place to Hire Information Security Staff with necessary Skills, Experience and Education	167
4.6	Organization's Considered Criteria when Hiring/ Promoting Information Security Staff	168
4.7	Types Of Documentation will be Used During Risk Assessment	170
4.8	Individuals Who Participate in Information Security Risk Analysis	171
4.9	Individuals who have the Final Approval of the Information Security Risk Analysis	172
4.10	Top Management Involvement and Support in Information Security Task	173

4.11	Organizational Context	175
4.12	List of the Organizational Context Which Mostly Agreed By Methodologies and Survey Respondents	176
4.13	Information Gathering Techniques	177
4.14	Important Technical Assets to be Protected	179
4.15	Important Non-Technical Assets-Knowledge to be Protected	180
4.16	Important Non-Technical Assets-Unofficial form of Information to be Protected	181
4.17	Types of Information Security Training Provided for Staffs	184
4.18	Self-Development Program	185
4.19	Methods used by Organization to Assess the Efficiency and Effectiveness of Information Security	186
4.20	Organization Awareness Program Checklist	188
5.1	Sample Characteristics of Respondents	193
5.2	Reliability of Real Study	197
5.3	Personal Components Analysis (Information Structure)	198
5.4	Score Category of Logit for Components of Information Structure for ISMS	198
5.5	Analysis Results of RMM for Components of Information Structure for ISMS	201
5.6	Skewness and Kurtois Analysis	208
5.7	Convergent Validity Of Measurement Model	210
5.8	Discriminant Validity of Measurement Model	214
5.9	Results of the Structural Model Analysis	216
5.10	Summarized Findings of Structural Model	219
5.11	Reliability of Real Study	221
5.12	Personal Components Analysis (Information Quality Dimensions)	221
5.13	Score Category of Logit for Information Quality Dimensions	222
5.14	Analysis Results of RMM for Information Quality Dimensions	224
6.1	Experts' Background	230
6.2	Summary of Experts' Comments	239
6.3	The Reorganizing and Updating Actions	240
6.4	Characteristics for Information Quality Dimensions	248
6.5	Synthesized findings in relation to parameter task to achieve information quality dimensions	250
6.6	Summary of framework Usefulness	256
6.7	Comparison between PDCA Model and Proposed Framework	259
7.1	Summary Results of 13 Hypothesis	275

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Relationship between Objectives and Research Questions	13
2.1	Literature Review for Chapter 2	24
2.2	ISMS Methodologies	46
2.3	List of Activities that Require Information to Plan ISMS	55
2.4	List of Activities Diagram for ISMS	61
2.5	List of Important Assets Based on Technical Perspective	64
2.6	Technical and Non-Technical Perspective Asset Identification in ISRA	75
2.7	Components of Information Structure for ISMS	77
2.8	Conceptual Framework of the Study	94
3.1	Research Design	103
3.2	Relationship between Input-Process-Output with Proposed Framework	105
3.3	The Hypothesized Research Framework	108
3.4	Research Procedure	110
3.5	Research Procedure Phase by Phase	111
3.6	Research Techniques and Procedures for Phase One and Two	112
3.7	Research Techniques and Procedures for Phase Three	113
3.8	Research Techniques and Procedures for Phase Four	114
3.9	Activities Flow for Identifying the Similarities in Information Structure	116
3.10	Activity Flow for Identifying the Non-Technical Perspective Assets	118
3.11	Steps to Identify Relevant Materials for Review	118
3.12	Activity Flow for Identifying Potential Information Quality Dimensions for ISMS	120
3.13	Questionnaire Survey Execution	123
3.14	Questionnaire Survey Execution	129
3.15	Personal Component Analysis (PCA) for Section 1	144
3.16	Personal Component Analysis (PCA) for Section 2	144
4.1	Activity Lists for Risk Management Improvement	182
4.2	Summary of Data Analysis Procedures	196
5.1	Item Map (Hierarchy) on Components of Information Structure for ISMS	199
5.2	Convergent Validity: Outer Loadings of Measurement Model	212
5.3	Structural Model	218
6.1	Information Quality Structure Framework	243
6.2	Information Structure for ISMS	246
6.3	PDCA Model Applied to ISMS Processes	258

LIST OF APPENDIXES

APPENDIX	TITLE	PAGE
A	Table 2.5 Comparative Study of Identifying All the Methodologies had Common Mutual Components	319
B	Survey Questionnaire 2013 Survey On Information Security	320
C	Management System (ISMS) Implementation In It Based Organization	321
D		322
E	Content Validity: Descriptive Study Questionnaire	323
F	Survey Questionnaire Information Structure, Information Quality Dimensions and Effectiveness of Quality Information	324
G	Content Validity: Likert Scale Questionnaire	325
	Semi-Structured Interview Questions Panel Expert Validation and Synthesis	
	Information Quality Structure Framework	

LIST OF ABBREVIATIONS

ABBREVIATION	DEFINITION
ISMS	Information Security Management System
CIA	Confidential, Integrity and Availability
PDCA	Plan-Design-Check-Act
ISRA	Information Security Risk Assessment
ISRM	Information Security Risk Management
NITC	National Information Technology Council
MyCERT	Malaysian Computer Emergency Response Team
NISER	National ICT Security & Emergency Response Centre
SIRIM	Standards and Industrial Research Institute of Malaysia
CNII	Critical National Information Infrastructure
SOA	Statement of Applicability
ISM	Information Security Management
CRAMM	CCTA Risk Analysis and Management Method
CORAS	Construct a platform for Risk Analysis of Security Critical Systems
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
ISRAM	Information Security Risk Analysis Method
SEM	Structural Equation Modelling
RMM	Rasch Measurement Model
PLS	Partial Least Square
PCA	Principal Component Analysis
MnSq	Mean Square Value
Zstd	Standardized Z
AVE	Average Variance Extracted

LIST OF PUBLICATIONS

Journals

Shamala, P., Ahmad, R. & Yusoff, M., 2013. A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1), pp.45–52.

Shamala, P. et al., 2015. Collective information structure model for Information Security Risk Assessment (ISRA). *Journal of Systems and Information Technology*, 17(2), pp.193–219.

Shamala, P., Ahmad, R. and bin Sahib, S., 2015. Generic Taxonomy of Assets Identification for Information Security Risk Assessment (ISRA). *Journal of Information Assurance and Security*, 10(6), pp.260-268.

Shamala, P., Ahmad, R. and bin Sahib, S., 2016. Generic Taxonomy of Assets Identification during Risk Assessment in Information Security Management. *International Business Management*, 10(17), pp. 3982-3991.

Conference Proceedings

Shamala, P. and Ahmad, R., 2014. A proposed taxonomy of assets for information security risk assessment (ISRA). In *Fourth World Congress Information and Communication Technologies (WICT)*, IEEE. pp. 29-33.

Shamala, P. and Ahmad, R., 2015. Generic Taxonomy of Assets Identification during Risk Assessment in Information Security Management. In *4th International Conference on Technology Management, Business and Entrepreneurship, ICTMBE*, (pp. 29-33).

Awards

Bronze Medal: Shamala, P. and Ahmad, R., 2013. New Info Structure Framework for Information Security Risk Assessment (ISRA). Competition and Exhibition 3rd National Invention Innovation & Design-NiiD UiTM Perak.

Gold Medal: Shamala, P. and Ahmad, R., 2016. Integrating Information Quality Dimensions in Information Security Management System (ISMS). Invention, Innovation & Design Competition 2015/2016, Asia e University.

CHAPTER 1

INTRODUCTION

1.1 General Overview

In the current information age, the issue of information security has become a vital entity because organisations across the globe conduct business in an interconnected and information-rich environment. This popularity has been due to the fact that most of the organisations have substantially replaced the physical forms of data to electronic forms of data as it has the capacity to speed up any information-based activities (Bernard, 2007). Hence organisations are becoming progressively aware that information security is an important aspect of their business strategy.

This scenario is supported by the survey conducted by PricewaterhouseCoopers (PwC) in whereby a study was conducted about the global state on Information Security (PWC, 2016). The survey revealed that organisations steadily increased the amount of resources for protecting their corporate assets by boosting their information security budget by 24 percent in 2015. This increment could be considered as a sign that the value of information to organisations is growing dramatically. Therefore, in order to ensure the continued accessibility, confidentiality and integrity of information, the majority (91 percent) of organisations have decided to implement key security safeguards.

Undoubtedly, these concerns created an awareness for organisations to achieve an ideal level of information security by applying Information Security Management System (ISMS) for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives (Saleh, 2011;

Landoll, 2006; Hulitt & Vaughn, 2010). ISMS can be defined as a management system used for establishing and maintaining a secure information environment (Eloff & Eloff, 2003).

Basically, ISMS will ensure that the right people, processes and technologies are in place, and facilitates a proactive approach to manage security and risk (Barlette & Fomin, 2008; Brenner, 2007; Fomin et al., 2008). However, the field of information security has to change from just technical issues or a technology point of view, into a completely different point of view, where wider concern is given on management issues in which emphasis is given on procedures and processes involved for the development of secure information management system.

Limited scholarly investigation has been undertaken to present the need of properly defined steps of processes and procedures in which a structured way of managing ISMS within an organization is provided. ISMS is the process of involving a series of tasks broken down by phases where each phase requires information and properly defined detailed steps to make the planning process more systematic. This is because the success of the information security management system fully depends on the information gathered in order to make concise and accurate security planning decisions.

Thus, it would be helpful if the organization knew beforehand what information they need before commencement of the plan while maintaining the quality of information in order to make effective decisions. It is vital to have a holistic picture of ISMS flow and what types of quality input information need to be gathered on the requirements to be met before security management can be conducted successfully.

Therefore, this research attempts to introduce an information quality structure framework. The proposed framework consists of two parts, namely information structure and information quality. Therefore, this chapter provides an introduction to this context for this research.

1.2 Problem Background

As to maintain confidentiality, integrity, and availability (CIA) of information, organisations require to establish comprehensive and systematic ISMS. The management needs to implement some form of ISMS in order to address any information security related issues as part of their information security management in their organization (Eloff & Eloff, 2003). ISMS is part of overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (ISO/IEC 27001, 2005). The policies, procedures, guidelines, code-of-practises, technologies, human issues, legal and ethical issues and associated resources and activities have become the de facto “common-language” for organisations to enable information security management requirement (Humphreys, 2008).

ISMS is collectively managed by an organization, in the pursuit of protecting its information assets (Rebollo et al., 2011; Eloff & Eloff, 2003; Eloff & Eloff, 2005; Nowak, 2015). Generally, organisations that want to achieve the ISMS will consider to put in place a cost-effective execution plan that includes appropriate security controls for mitigating identified risks and protecting the confidentiality, integrity and availability of an organization’s information assets. In addition, it also involves ongoing monitoring to ensure that these controls remain effective. It helps practitioners to make strategic decisions to ensure that the right people, processes and technologies are in place in order to handle security and risk (Brenner, 2007).

It is undeniable that, three important aspects, namely processes and procedures, people and technology to guide information security practitioners are required in order to assure the

consistent implementation of controls across an organization's information systems and business processes. Most of the research in information security has only captured the interest of many practitioners and scholars in the issues related to technology and also personnel. It is proven in which, even organisations employing technology based security, the organization's computers, network and information are still facing high security risks (Kolokotronis et al., 2002; Jourdan et al., 2010; Richardson, 2008). Meanwhile, another group of researchers argue that, although security policies, standards and awareness strategies are currently in place and with well-designed security strategies, still security incidents occur due to human factors (Colwill, 2009; Filho et al., 2011).

However, researchers also have dealt with the topic covering information security processes and procedures. It is supported by critical literature review conducted by author Silic & Back to offer implications for future research directions on information security (Silic & Back, 2014). They analyzed and categorized all the 1,588 articles into thirteen themes. Among all the themes covered, the themes of which may be associated with processes and procedures are risk assessment and information security governance. The key findings for risk assessment focus on analyzing vulnerabilities and threats to the information resources and planning, measuring and implementing what countermeasures to take for developing security requirements and specifications (Feng et al., 2014). Meanwhile, information security governance theme refers to frameworks, standards and security policies where researchers focus on defining and implementing strategy and security policy in order to protect against the possible risks.

As the deployment of information security evolved, information security management needs to consider on management level process and procedure approach framework. This is because, even though there are technological, personnel and strategic solutions are implemented, security issues are still occurring. It is proven by EY's Global Information Security Survey 2013 (Ernst & Young, 2013), which statistically reported that although there is increase in investment