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 menyedari 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

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDIXES

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 Natioanal 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