INFORMATION SECURITY COMPLIANCE ASSESSMENT USING INFORMATION SECURITY MATURITY MODEL

HASSAN HOSSEIN ZADEH

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of computing
Universiti Teknologi Malaysia

AUGUST 2014

This study present to the beautiful flowers in my life

My Father

And

My Mother

Who endowed us happiness and serenity with all their attempts

My very kind wife

Who was an angle with a great patience

ACKNOWLEDGEMENT

First and foremost, Infinite praises to God and with His blessing, my deepest appreciation goes to Dr. Siti Hajar Othman whom I really respect for becoming my supervisor for this final year project as well as for being so ready in guiding me through this research. Your insights have helped a lot.

I would also like to express my thanks to all my family who have supported me, helping me directly in the progress of this research and constantly providing me with moral support all along. I am really grateful to have you by my side all these while. Without them, I would not have been able to complete this report on time.

In particular, I would like to thank my beloved wife for her patience, encouragement, support and understanding.

Last but not least, my greatest appreciation to everyone who has been involved in this research even by coincidence.

ABSTRACT

Information security is an essential factor for business today and is achieved by adopting the suitable set of practices, standards, process, policies and organizational structures. In order to recognize the strength and weaknesses of information security, organizations can implement information security model. Information Security Maturity Model (ISMM) as a security oriented model has been developed in order to determine the level of information security in organization. It has provided five (5) compliance levels of security which contain: none compliance, initial compliance, basic compliance, acceptable compliance and full compliance. The goal of this research is to assessing of the information security compliance in departments of UTM based on this model. So five (5) departments consist of three (3) offices (RMC, SPS, and CTL) and two (2) faculties (FKE, FKM) were chosen. Fully in-structured interview were performed with five (5) IT experts in case study. Analyzing data were done and information security compliance levels for these departments were determined. Based on results, basic compliance level was belonged to RMC and CTL, Wile acceptable compliance level to SPS, FKE and FKM. Besides, none of them were in Full compliance level. According to the results, suggestions in order to enhance compliance level of security were provided. Finally, for the improvement of ISMM model, some other future works were offered by this research.

ABSTRAK

Jadi keselamatan maklumat merupakan faktor penting bagi perniagaan hari ini dan ia dicapai dengan menerima pakai set aktiviti, standard, proses, polisi dan struktur organisasi yang sesuai.Dalam usaha untuk mengenalpasti kekuatan dan kelemahan keselamatan maklumat, organisasi boleh melaksanakan model keselamatan maklumat. Keselamatan Maklumat Model Kematangan (ISMM) merupakan model berorientasikan keselamatan yang telah dibangunkan untuk menentukan tahap keselamatan maklumat dalam organisasi. Ia telah menyediakan lima (5) tahap pematuhan keselamatan yang mengandungi : tiada pematuhan, pematuhan awal, pematuhan asas, pematuhan boleh diterima dan pematuhan sepenuhnya. Tahap pematuhan tersebut adalah sebagai alat untuk menilai objektif keselamatan dalam organisasi. Matlamat kajian ini adalah untuk menilai pematuhan keselamatan maklumat dalam organisasi UTM berdasarkan model ini. Jadi, lima jabatan dalam UTM yang terdiri daripada tiga (3) pejabat (RMC, SPS, and CTL) dan dua (2) fakulti (FKE, FKM) telah dipilih. Temubual berstruktur sepenuhnya telah dijalankan dengan lima (5) IT pakar dalam kajian kes. Menganalisis data telah dilakukan dan tahap pematuhan keselamatan maklumat bagi jabatan tersebut talah ditentukan. Berdasarkan kepada keputusan, tahap pematuhan asas dimiliki of RMC and CTL, manakala SPS, FKE and FKM mencapai tahap pematuhan yang boleh diterima. Selain daripada itu, tiada satu jabatan pun yang mencapai tahap pematuhan sepenuhnya. Menurut keputusan itu, cadangan bagi meningkatkan tahap pematuhan keselamatan disediakan. Akhir sekali, untuk meningkatkan model ISMM, beberapa kerja bagi masa depan telah ditawarkan oleh kajian ini.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BSI	-	British Standards Institute
COBIT	-	Control Objectives for Information and related Technology
CRAMM	-	CCTA Risk Analysis and Management Model
CSRC	-	Computer Security Resource Centre
CTL	-	Centre of Teaching and Learning
FKE	-	Faculty of Electrical Engineering
FKM	-	Faculty of Mechanical Engineering
GMITS	-	Guidelines for the Management of IT Security
ICT	-	Information Communication Technology
ISM3	-	Information Security Management Maturity Model
ISMM	-	Information Security Maturity Model
ISO	-	International Standards Organization
ITGI	-	IT Governance Institute
MM	-	Maturity Model
NIST	-	National Institute of Standards and Technology
OCTAVE	-	Operationally Critical Threat, Asset, and Vulnerability Evaluation

RMC	-	Research Management Centre
SEI	-	Software Engineering Institute
SPS	-	School of Graduate Studies
SSE-CMM	-	Systems Security Engineering Capability Maturity Model
TCO	-	Total Cost of Ownership

CHAPTER 1

INTRODUCTION

1.1 Introduction

Information is like the assets of organization and guarding them is necessary from vulnerability and attacks due to continuing the tasks of any organizations. Information security is explaining the safeguard of information and the important elements about it, such as systems and hardware devices which keep and transfer information. Education, awareness programs, Policies, and also technology are used to guard information and prevent it free from danger. Information security plans a wide area which involves information security management, computer and network security, and also is an essential rule and main part in the safeguard of data (Risvold, 2010).

Presently, information is not only a crucial organisational property, but also an essential element in obtaining competitive benefit. In plenty of situations, information manages most of the business procedures, and includes employees from many rankings: from major management to entry level workers (Lessing, 2008). Nowadays, information is getting to be a significant success element to the states and organizations. Organizations have been actively utilizing security systems (Herath & Rao, 2009). Hence, securing this kind of a crucial asset is a key business necessity that should be well planned and implemented continuously in a structured approach.

Ensuring security of information is an important factor for achieving success utilization of such systems.

To achieve the aims of security, organization need to evaluate level of the information security continuation and search for their problems and solve them. Information security maturity model (ISMM) is created as a tool to analyse the capability of organizations to achieve the goals of security, including, confidentiality, integrity, and availability.

1.2 Problem background

It is an information age, in which protecting of such assets drives economy and politics, and involves culture. Intricacy and security do not typically get along; the suitable awareness is the best driver for the best practice. Information is turning into an extremely necessary asset to the success of governments and organizations and needs to be treated as such. It should be clear, stored, integrated, transmitted and available at any time require to authorized user.

Information security is obtained by utilizing and executing the suitable set of quality controls that involve policies, procedures, standards, practices, awareness programs or organizational structures and ethics (Alaboodi, 2007). Obtaining three goals of Information Security (Confidentiality, Integrity and Availability) is not to mean gaining security (Saleh, 2011). Security is obtained by protecting against attacks and obtaining the organization's mission in spite of incidents and attacks. One problem with organizations' security is that it is typically observed in isolation and organizations do not connect the security needs to the business aims. The reason for these organizational problems is related to the financial issues that organizations exposure for unneeded costs on security and control (Saleh, Abbad, & Alghazo, 2012). Challenges of evaluating the implementation of security at organizations are

the other problem with organizations' security. Besides execution challenges, doing perfect practices in the execution of security is required (Saleh, 2011).

The concept of information security standards which have models with quantifiable impact on the business turns into more present in exercise and more respected by professionals. Maturity model (MM) can be called organized set of components that explain certain characteristics of development (maturity) in the organization (Stevanović, 2011).

In order to determine and discover the effectiveness and weaknesses of specific organization's security, a broad range model has been improved. A maturity model is presented that offers a start for security execution, a typical and shared view point of security, and a method for prioritizing acts. Furthermore , this Information Security model has five conformity levels and four core indicators to benchmark the execution of security in organizations (Saleh *et al*., 2012).

1.3 Aim of Project

This study can help the organization to analyze and assess the compliance level of information security in order to find strengths and weaknesses of its information security level and enhancing this level of security.

1.4 Problem Statement

In spite of the enhancing investment in information security and critical role played in today's organisations, knowing how to provide information security effectively still stays one of the challenging points in the IT field (Alaboodi, 2007). Particularly, the analysis and delivery of trusted information systems stays

troublesome and has attracted the consideration of many researchers. Security is a core necessity of states and organizations which should be combined into business procedures and culture.

Much more investigate is required to be carried out to perform best practices in the execution of security. All organizations require evaluating its information security continuity to find out the level of their security and try to enhance their information security. Therefore, there is an inherent require in both academia and industry for an organized and complete methodology of information security system. It is needed to be integrated in nature, evaluate development, and give a quantity measure of information security cost.

Five (5) departments in UTM are chosen to investigate and study about the compliance level of their security information by using ISMM and find the weakness of them in order to enhance the grade of InfoSec. According to Alaboodi (2007) it is predicted Information Security Maturity Model (ISMM) can have a greater rate of accomplishment in securing computing place.

1.5 Research Objectives

1. To study the various Information Security Models based on previous studies and to focus on Information Security Maturity Model (ISMM).
2. Data gathering related to information security practices in case study based on compliance levels of ISMM and analyzing them.
3. To measure compliance level to ISMM among selected case studies to determine strengths and weaknesses. Providing suggestions in order to enhance information security level.

1.6 Scope of project:

In order to reach the objectives stated above, the scope of this study is limited to the following:

1. This study focuses on information security models and specially focuses on information security maturity model (ISMM).
2. Project assessment is accomplished by performing the fully in-structured interview with IT experts in order to assess compliance level of information security in five (5) departments of UTM.

1.7 Research Question

The questions in this report which are going to be discussed can be mentioned as follow:

1. What are the characteristics of current information security models?
2. What are the suitable models which can use for implementation information security?
3. How to determine compliance level to the information security maturity model?
4. How to find the strength and weaknesses of information security in organizations?

1.8 Significance of the Study

The common information security goals are confidentiality, integrity, and availability. Attaining these aims does not ensure obtaining security. Security is

accomplished by the avoidance of attacks against information systems as well as from obtaining the organization's mission in spite of attacks and accidents. An organization that regularly assess and checking its security execution will gain the maximum level and it will gain the goals of security. This study can help organizations to analyze their compliance level of information security.

1.9 Structure of Thesis

This thesis is framed into six chapters. The content of each chapter is presented as following: chapter 1explains the problem background, problem statement, project objectives, project scopes, research questions and significant of the project. Chapter 2 presents literature review. Chapter 3 discusses on the project methodology. Followed by, chapter 4 presents the overview of information security models, introducing compliance levels of ISMM, and explains about gathering data. Chapter 5 is comprised of analyzing data and discussion as well as providing suggestions in order to enhance information security level in five (5) departments in UTM. Finally, chapter 6 includes conclusion, achievements, future work and summary.

1.10 Summary

This chapter explained about information security, then problem background was discussed, next problem statement was stated. In the following, research objectives and scope of project were explained. The rest research questions and significant of the study were discussed. Finally, structure of thesis was determined.

REFERENCES

AlAboodi, S. S. 2006 A new approach for assessing the maturity of information security. *Information Systems Control Journal, 3*, 36.

Alaboodi, S. S. 2007 Towards evaluating security implementations using the Information Security Maturity Model (ISMM).

Badr, Y., & Stephan, J. 2007 Security and risk management in supply chains. *Journal of Information Assurance and Security, 2*(4), 288-296.

Beres, Y., Mont, M. C., Griffin, J., & Shiu, S. 2009 *Using security metrics coupled with predictive modeling and simulation to assess security processes.* Paper presented at the Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement.

Brotby, W. K. 2007 *Information Security Governance: Guidance for Information Security Managers*: ISACA.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007 The OCTAVE Allegro Guidebook, v1. 0: May.

Consulting, I. 2003 CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0. *Walton-on-Thames. UK: SIEMENS*.

Debreceny, R. S. 2006 *Re-engineering IT internal controls: applying capability maturity models to the evaluation of IT controls.* Paper presented at the System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on.

Fang, H. 2011 Study and Practice of SSE-CMM. *Information Security and Communications Privacy, 8*, 036.

Harris, S. 2009 *CISA Certified Information Systems Auditor all-in-one exam guide*: McGraw-Hill, Inc.

Herath, T., & Rao, H. R. 2009 Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Institute, I. G. 2006 *COBIT Mapping: Mapping SEI's CMM for Software with COBIT 4.0*: ISACA.

Jacobs, P., Arnab, A., & Irwin, B. 2013 *Classification of Security Operation Centers.* Paper presented at the Information Security for South Africa, 2013.

Karabulut, Y., Kerschbaum, F., Massacci, F., Robinson, P., & Yautsiukhin, A. 2007 Security and trust in it business outsourcing: a manifesto. *Electronic Notes in Theoretical Computer Science*, *179*, 47-58.

Larsen, M. H., Pedersen, M. K., & Viborg Andersen, K. 2006 *IT Governance: Reviewing 17 IT governance tools and analysing the case of Novozymes A/S.* Paper presented at the System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on.

Lessing, M. 2008 Best practices show the way to Information Security Maturity.

Maček, D., Magdalenić, I., & Ivković, N. 2011 *Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods.* Paper presented at the 22nd Central European Conference on Information and Intelligent Systems.

Mazumdar, C., Barik, M. S., & Sengupta, A. 2007 *Enterprise Information Security Risk Analysis: A Quantitative Methodology.* Paper presented at the Proceedings of the National Workshop on Software Security (NWSS 2007), N. Delhi, India.

Musman, S., Tanner, M., Temin, A., Elsaesser, E., & Loren, L. 2011 *A systems engineering approach for crown jewels estimation and mission assurance decision making.* Paper presented at the Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on.

Oliver, D., & Lainhart, J. 2012 COBIT 5: Adding Value Through Effective Geit. *EDPACS*, *46*(3), 1-12.

PANDEY, S. K. 2012 A Comparative Study of Risk Assessment Methodologies for Information Systems. *Bulletin of Electrical Engineering and Informatics*, *1*(2), 111-122.

Risvold, M. O. 2010 Organizational issues related to information security behavior.

Rouyet-Ruiz, J. 2008 COBIT as a Tool for IT Governance: between Auditing and IT Governance. *The European Journal for the Informatics Professional, 9*(1), 40-43.

Saint-Germain, R. 2005 Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-66.

Saleh, M. F. 2011 Information Security Maturity Model. *International Journal of Computer Science and Security (IJCSS), 5*(3), 21.

Saleh, M. F., Abbad, M., & Alghazo, J. M. 2012 Compliance to the Information Security Maturity Model in Saudi Arabia.

Samy, G. N., Ahmad, R., & Ismail, Z. 2010 *A framework for integrated risk management process using survival analysis approach in information security*. Paper presented at the Information Assurance and Security (IAS), 2010 Sixth International Conference on.

Schneier, B. 2011 *Secrets and lies: digital security in a networked world*: Wiley. com.

Siponen, M., & Willison, R. 2009 Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270.

Sommestad, T., Ekstedt, M., & Johnson, P. 2010 A probabilistic relational model for security risk analysis. *Computers & Security, 29*(6), 659-679.

Stevanović, B. 2011 Maturity Models in Information Security. *International Journal of Information, 1*(2).

Vidyaraman, S., Chandrasekaran, M., & Upadhyaya, S. 2008 *Position: the user is the enemy*. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

Harris, Shon (Feb, 2013), CISSP All-in-One Exam Guide, 6rd Edition, McGraw-Hill Osborne Media.

NIST, "Security Maturity Levels," 2012.[Online]. Available:

http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html