READINESS OF LOCAL AUTHORITIES IN IMPLEMENTING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

FARAH SAFFARIZAN BINTI MOHD ESA

JANUARY 2014

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : FARAH SAFFARIZAN BINTI MOHD ESA
Date of birth : 04 FEB 1980
Title : Readiness Of Local Authorities In Implementing Information Security Management System (ISMS)
Academic Session : 2013/2014 - Sem I

I declare that this thesis is classified as :

☐	**CONFIDENTIAL**	(Contains confidential information under the Official Secret Act 1972)*
☐	**RESTRICTED**	(Contains restricted information as specified by the organization where research was done)*
☑	**OPEN ACCESS**	I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the Purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by :

SIGNATURE	**SIGNATURE OF SUPERVISOR**
800204146008	**DR. NURAZEAN BT MAAROP**
(NEW IC NO. /PASSPORT NO.)	**NAME OF SUPERVISOR**
Date : January 2014	Date : January 2014

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Computer Science (*Information Security*)"

Signature	:	…….
Name of Supervisor	:	Dr. Nurazean binti Maarop
Date	:	…….

READINESS OF LOCAL AUTHORITIES IN IMPLEMENTING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

FARAH SAFFARIZAN BINTI MOHD ESA

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

Advanced Informatics School
Universiti Teknologi Malaysia

JANUARY 2014

I declare that this project report entitled *"Readiness Of Local Authorities In Implementing Information Security Management System (ISMS)"* is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	
Name	:	Farah Saffarizan Binti Mohd Esa
Date	:	January 2014

For my beloved mother, husband and other members of my family, especially to my sister Nurul Nabila which passed away last year.

ACKNOWLEDGEMENT

In the name of ALLAH, the most Merciful and the most Gracious
Assalamualaikum warahmatullah

Alhamdulillah, with the gratitude to Allah for His grace and permission, My first project, which entitled "Readiness Of Local Authorities In Implementing Information Security Management System" are already completed as planned. The deepest appreciation is given to my supervisor, Dr. Norazean binti Maarop for all of her guide and guidance that have been given and also for her dedication and commitment that she gave in order to supervise my research.

In addition, a million of thanks are given to my husband Mohd Hanafiah b. Ahad because his understanding of the demands of the time required to complete this project. A lot of thanks are also given to all parties that involved directly or indirectly in helping provide the information and ideas to me. Also a million sought of forgiveness if there are shortcomings and mistakes that happen during doing this research.

Finally, I hope that this research can meet all the requirement and beneficial to all. Hopefully that all of this effort will get a lot of blessed from Allah.

ABSTRACT

Information Security Management System (ISMS) is an ICT Compliance Standards to provide specifications and controls for protecting information security assets and to increase the integrity and confidence of clients against the agencies, especially those involving the government delivery service. This certification is certified by a certification body of the Standards Industrial Research Institute of Malaysia (SIRIM) and a survey covering the problems faced by Local Authorities in ensuring the confidentiality, integrity and availability of information from any threat and risks that can cripple the agency services. The research process include factors such as threats and vulnerabilities, particularly in security management practices of the agency, which can cause loss of agencies' information and negative impact on the services provided by the Local Authority. Then with studying these factors it can measure the readiness of local authorities in implementing Information Security Management System (ISMS). The process of research studies using quantitative methods in gathering information to analyze the problems faced by the agency to ensure information security is protected such as assessment taxes is the largest contributor earning council. The final result of this research concluded that local authorities are still not ready in implementing Information Security Management System (ISMS).

ABSTRAK

Sistem Pengurusan Keselamatan Maklumat *(ISMS)* merupakan Standard Pematuhan ICT yang menyediakan spesifikasi dan kawalan–kawalan bagi melindungi keselamatan aset maklumat dan seterusnya meningkatkan integriti dan keyakinan pelanggan terhadap agensi kerajaan khususnya yang melibatkan penyampaian perkhidmatan kerajaan. Pensijilan ini diperakui oleh satu badan pensijilan iaitu *Standards & Industrial Research Institute of Malaysia (SIRIM)* serta kajian yang dijalankan meliputi permasalahan yang dihadapi oleh Pihak Berkuasa Tempatan dalam menjamin kerahsiaan, integriti dan ketersediaan maklumat dari sebarang ancaman dan risiko yang boleh melumpuhkan perkhidmatan agensi. Proses penyelidikan meliputi faktor –faktor ancaman dan kelemahan khususnya di dalam amalan pengurusan keselamatan agensi, yang boleh menyebabkan kehilangan maklumat agensi serta memberi kesan negatif kepada perkhidmatan yang disediakan oleh Pihak Berkuasa Tempatan. Dengan mengkaji faktor tersebut ia dapat mengukur tahap kesediaan Pihak Berkuasa Tempatan dalam melaksanakan Sistem Pengurusan Keselamatan Maklumat *(ISMS).* Proses penyelidikan kajian menggunakan kaedah kuantitatif dalam pengumpulan maklumat dengan menganalisa permasalahan yang dihadapi oleh agensi bagi menjamin keselamatan maklumat dilindungi seperti maklumat cukai taksiran yang merupakan penyumbang terbesar pendapatan majlis. Keputusan akhir penyelidikan ini merumuskan bahawa Pihak Berkuasa Tempatan masih belum bersediakan dalam melaksanakan Sistem Pengurusan Keselamatan Maklumat *(ISMS).*

TABLE OF CONTENTS

CHAPTER	TITLE		PAGE
	DECLARATION		ii
	DEDICATION		iii
	ACKNOWLEDGEMENT		iv
	ABSTRACT		v
	ABSTRAK		vi
	TABLE OF CONTENTS		vii
	LIST OF TABLES		xi
	LIST OF FIGURES		xii
	LIST OF ABBREVIATIONS		xiv
	LIST OF APPENDICES		xv
1	**INTRODUCTION**		1
	1.1	Overview	1
	1.2	Background Of The Problem	3
	1.3	Problem Statement	5
	1.4	Project Aim	5
	1.5	Research Questions	6
	1.6	Research Objectives	7
	1.7	Research Scope	7
	1.8	Summary	8
2	**LITERATURE REVIEW**		9
	2.1	Introduction	9

2.2	The Literature Study		10
	2.2.1	Definitions And A Brief Description Of The Information Security Management System (ISMS)	10
	2.2.2	Briefly of Phase The Information Security Management System (ISMS)	13
	2.2.3	Measurement Factors of Readiness	13
		2.2.3.1 Threat	14
		2.2.3.2 Vulnerabilities	22
2.3	Measurement Readiness Factors for Implementing Information Security Management System Based On Literatures		24
2.4	Proposed The Conceptual Framework For Readiness Of ISMS		31
	2.4.1	ICT Policy and Standard	32
	2.4.2	Vulnerabilities In Term of People	32
	2.4.3	Vulnerabilities In Term of Processes	33
	2.4.4	Threat and Risk	33
2.5	Summary		34
3	**RESEARCH METHODOLOGY**		35
3.1	Introduction		35
3.2	Data Collection And Analysis		35
	3.2.1	Secondary Data Collection	36
	3.2.2.	Primary Data Collection	37
3.3	Operational Framework		38
3.4	Detail of Operational Framework		40
3.5	The Mapping Between The Measurements Factor of Readiness and the Questionnaires		42
3.6	Data Analysis		44
3.7	Data Analysis Methods		44
	3.7.1	Google Docs	44
	3.7.2	SPSS Software	45
3.8	Summary		45

4	**ANALYSIS AND RESULT**		46
	4.1	Introduction	46
	4.2	Descriptive Analysis of Demographic On Study	47
		4.2.1. Result Analysis of Demographic Based On Position and Experience in the field of ICT	49
	4.3	Analysis To Access The Criterions Of Readiness Based On ICT Policies And Standards In Organizational	51
		4.3.1 Analysis A Readiness Of Compliance Agencies With Organizational Security Policies And Standard Based On Level Of Position	51
	4.4	Analysis Based On Organization Security And Personnel Security	60
		4.4.1 Analysis of Organization Security	61
		4.4.2 Analysis of Personnel Security	65
	4.5	Threat and Risk	72
	4.6	Summary	83
5	**DISCUSSION**		85
	5.1	Introduction	85
	5.2	Summary of the findings	85
		5.2.1 The Criterions Of Compliance With The Government Ict Security Policy At The Local Authorities	86
		5.2.2 Readiness Framework That Can Be Used As A Guideline By The Local Authorities To Assist In Implementing ISMS	87
		5.2.3 Threat And Risks Faced By The Agency So That The Information Is Protected, Not Exposed To The Risks And Threats Based On Readiness Framework	88
	5.3	Summary	89
6	**CONCLUSION**		90
	6.1	Introduction	90
	6.2	Contributions of this study	90
	6.3	Limitation	91

6.4 Future Research 92
6.5 Concluding Remarks 93

REFERENCES 94
Appendices A - B 98 – 108

LIST OF TABLES

TABLE NO	TITLE	PAGE
2.1	Statistics threats by category for the year 2009	18
2.2	Statistics threats by category for the year 2008	19
2.3	Measurement of readiness factors for implementing information security management system	25
2.4	The measurement factors of readiness to in implement Information Security Management Security (ISMS) by research papers	26
3.1	Detail of operational framework	40
4.1	Demographic by respondents	48
4.2	Feedback respondents by level of position category based on working experience and ICT skills	50
4.3	Staff aware about of ICT policy organization	52
4.4	IT policy documents in the organization	53
4.5	Statistics do not fully implement the IT policy or do not have IT policies in the organization	54

LIST OF FIGURES

FIGURE NO	TITLE	PAGE
2.1	MyCERT incident statistics for the year 2009	17
2.2	MyCERT incident statistics for the year 2008	18
2.3	Conceptual framework of readiness to implementing ISMS	31
3.1	Explanation of the framework	39
3.2	Mapping between measurement factor of readiness with the questionnaires	43
4.1	Categories level of position based on work experience	50
4.2	Aware about the existence of an IT policy in organization based on position	52
4.3	Standard used in the organization to ensure information security	55
4.4	Staff awareness about the security policies, standards and/or procedures that use the organization information	56
4.5	Frequency informed about of secure use on information system	57
4.6	Guidelines of information classification scheme for sensitive Information	58
4.7	The roles and responsibilities of security description maintained and documented	59
4.8	The clearly defined responsibilities for the protection of organization assets	60
4.9	Contacts with law enforcement to reported the incidents of security breach	61
4.10	Formal reporting procedures for security breaches	62
4.11	Installation of security tools for restricted area such as CCTV	63

4.12	The operating procedures for maintenance	64
4.13	Audit of information systems security for agency	65
4.14	Appropriate security controls implemented to third party for information access	66
4.15	Maintenance contract signed by a third party for maintenance work	67
4.16	Employees signing confidentiality non-disclosure	68
4.17	Background examination for permanent staff at time offer the job	69
4.18	Frequency of security training and awareness	70
4.19	The staff awareness about of organization's policy	71
4.20	The assess of technical staffs awareness about emerging technologies and related control issues	72
4.21	Formal procedure for multiple users to access to the information and systems	73
4.22	Signed to keep the account password for confidential information	74
4.23	Review of access rights at regular intervals	75
4.24	Types of security breaches experienced	76
4.25	Existing procedures to prevent security breaches	77
4.26	Control of malicious code on their system	78
4.27	Possible attackers can access the organization's information resources	79
4.28	Special controls to protect the confidentiality and Integrity of data	80
4.29	Mechanisms used to control the access of information	81
4.30	Type of vulnerabilities that causes security breach incidents	82
4.31	Type of impact of threats to protected information	83

LIST OF ABBREVIATIONS

ISMS	-	Information Security Management System
MyRAM	-	The Malaysian Public Sector Information Security Risk Assessment Methodology
SIRIM	-	Standards and Industrial Research Institute of Malaysia
NISER	-	National ICT Security and Emergency Response Centre
CCTV	-	Closed Circuit Television
IPS	-	Intrusion Prevention System
ICT	-	Information Communication Technology
MS ISO	-	Malaysian International Organization for Standardization
CSMS	-	Corporate Security Management System
LAN	-	Local Area Network
WAN	-	Wide Area Network
MAMPU	-	The Malaysia Administrative Modernization and Management Planning Unit
MyCERT	-	Malaysian Computer Emergency Response Team

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Questionnaires	98
B	Gantt Chart	108

CHAPTER I

INTRODUCTION

1.1 Overview

The administrative structure of a country is divided into three groups , the federal government, the state government and the local government or local authority in which each administrative unit has different roles and tasks[1]. The local government or local authority is the lowest level of public administration and is the closer to the public in any country [1]. According to research by Abdullah and Wafiah[1],the local government or authority is a unit of local lower-level authorities or government institutions in a small area with power and specific tasks. In Malaysia, the local authority is divided into three categories: the council / city hall, municipal and district council. The function and role played by local authorities is as provided in Part XI Section 73 of the Local Government Act 1976 (Act 171) where local authorities are responsible for maintaining places, providing public services (e.g., garbage removal and solid waste disposal), and protecting public health (e.g., prevention of infectious diseases)[1].To provide the best services to local residents, local authorities must have adequate resources and finances to provide the services parallel to the needs of the people within its jurisdiction[1]. According to Part A , Section 39 of Act 171,the local authority may seek financial aide from several sources as revenue[1]. The source of income generated consists of license bills,

rental markets stalls, annual grants, fines and assessment[1].Therefore, it is important that certification is introduced and adopted by local authorities, where the use of ICT has become a key component for supporting the services.[2].

In addition to the public sector, the protection of government information is most important, to avoid any security violation or threats of ICT, including cyber attacks[3]. Thus, ICT assets of local authorities should have guidelines / standards by the certification body Standards Industrial Research Institute of Malaysia (SIRIM)[3][4]. MS ISO / IEC 27001:2007 Information Security Management System (ISMS) is the complement to the quality management system standard which provides specifications and controls for protecting information asset security and increase confidence and integrity customer to government sector especially Local Authorities[5][6].

> Some researchers believe the reason behind the lack of effectiveness is that security is primarily a "people issue", as well as a technical issue; and based on that it is believed that information systems security management is a knowledge intensive activity that currently depends heavily on the experience of security experts
>
> AlHogail and Berri [7]

To solve this problem , MS ISO / IEC 27001:2007 Information Security Management System (ISMS) is the complement to the quality management system standard which provides specifications and controls for protecting information asset security and increase confidence and integrity customer to government sector especially Local Authorities[8][4]. Through an auditing of ICT assets, corrective actions and improvements can be taken on any weakness, or noncompliance to ICT security management system to enhance the protection available to the principles of confidentiality, integrity and availability. Information Security Management System (ISMS) program based on the standard MS ISO / IEC 27001:2007 is a certification program that has been recognized internationally[3].

Applying a standard into a management system will help the Local Authorities to improve their delivery service for publics or local citizens. Through this standard, the Local Authorities will be able to plan better as to comply with the standard set and also comply with the best practices in the industry[8]. With regard to this matter, this study will be focusing on the Local Authorities readiness in order to apply a standard named as Information Security Management System (ISMS) that compliant to MS ISO/IEC 27001:2007. MS ISO / IEC 27001:2007 can be used as a benchmark of the level of information security management system for the government sector[3][9]. Indirectly, this certification can motivate government sector towards excellence in ICT security management [2].

Other than that, the main purpose of ICT security also is to minimize the impact of security incidents[10]. ICT security is closely related to the protection of information and ICT assets. The Local Authorities must take seriously with protecting the all forms of electronic information [4][2]. This is because the government agency, store information are contributed to the continuity of the government service especially the services that are provided via online[3][2][10].

1.2 Background of the Problem

Nowadays, most of government sector use ICT technologies as one of the methods for operate more efficiently and with quality. For local authorities, all of the services provided are related in the use of ICT technology. For example, the collection of taxes assessment is a major income for the local authorities in Malaysia, up to 65% or two-thirds income for authorities[1]. Valuation List is a complete record of all information related to a proportional holding (taxes assessment) local authorities[1]. Each local authority has its own valuation list which enable local governments to estimate the number or amount of grip available and help local authorities to calculate the expected revenue from a tax assessment for the

year[1]. This information is stored in a server database which can be accessed through electronic *Pihak Berkuasa Tempatan* (ePBT) system[4]. In addition, this information can also be accessed through an online services customers that are provided by the agency. The taxes assessment information is can accessed by customers to know detailed information about their property and make payments through online, the information indirectly exposed to cyber threats[1].

This is supported by the results of the study Pecina et.al[11], there are 2 types that can cause on the data destruction the is a threat and vulnerability. The threat of data destruction for the category of cyber threats (virtual assault) is a against the infrastructure, applications of physical and wireless communications[12]. Cyber threats are divided into several categories namely intrusion, fraud, harassment, malicious code or denial of service[13]. Vulnerability can be defined as weakness the in ICT infrastructure[3]. It may exist in the security system procedures, system design, phase in the implementation application, internal controls, employees issues, organization security and so on.

Besides that it, according to a study by Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), only a few government agencies implement Information Security Management System. For local authorities, only the Alor Setar City Council implementing these standards[8]. It shows awareness of local authorities to protect their data with information security management practices more effectively is lower. According to a study conducted by the National Security Council, there is an increased incidence of information security breaches in 2009 with a variety of categories by 3564 compared to 2008.Negative effect when this happens to local authorities, will be disrupted daily operations and give a bad image of the government[12]. Customer property info can be questioned, doubted and the main income of the Council will be indirectly affected[4].

Some of the interest earned if the performance of the ISMS is information to be protected cannot be accessed without authorization, the information is accurate

and do not doubt, to increase public confidence in government services provided by Pecina et al [11]. Other than that, this readiness study will also help the Council to assess the level of readiness of each agency in implementing these standards. And also , minimize the problem of the system failure, and cyber incidents in order to guarantee the continuity aspect of government services[3][10].

1.3 Problem Statement

According to a study by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU) on December 2012, only one local authority (Alor Setar City Council) among 144 local authorities are implementing Information Security Management System for the purpose of protecting their property assessment information which is the largest contributor in generating revenues. Therefore, the implementation of the ISMS should be implemented by the agency to ensure the property assessment information protected by reviewing the readiness of local authorities to establish a guideline for references of the agency. In addition, the weakness of local authorities in managing their property assessment information can contribute to the threat of data loss and can be a crippling council operation to providing the best services to their customers. Revenue generated from the collection of tax assessment is used to provide public facilities such as roads, street lighting, services of garbage collection and so on.

1.4 Project Aim

This study aims to provide a readiness framework of the current security policy use by the agency, that can be used to produce guidelines related to the

implementation of Information Security Management System (ISMS). Research will also be carried out taking into account the factors that contributed to the readiness of Local Authorities in implementing the standards. Factors to assess the readiness must measure in terms of threat and vulnerability on the information assets protected by the Local Authority. In addition, other factors such as the current policy used by the agency, security management practices in organizations and employees can also be measured as a benchmark to assess the readiness of the agency to implement the ISMS certification.

1.5 Research Questions

The study specifically focused on the readiness of agencies to implement a compliance Information Security Management System (ISMS). The research questions are:

i. What are the criterions for assessing the of readiness to implement Information Security Management System (ISMS) for Local Authorities?

ii. How to develop the readiness framework as the guideline to assist Council implementing ISMS?

iii. What are the threats and risk that are often experienced by Local Authorities in protecting information assets?

1.6 Research Objectives

The purpose of this research is to study at the problem about the security information management and select the appropriate approach for the best practice in readiness of agencies for implementing Information Security Management System (ISMS). The research objectives as below:

i. To identify the criterions of compliance with the Government ICT Security Policy at the Local Authorities.

ii. To develop a readiness framework that can be used as a guideline by the local authorities to assist in implementing ISMS.

iii. To evaluate the threats and risks faced by the agency so that the information is protected, not exposed to the risks and threats based on readiness framework.

1.7 Research Scope

The study focuses on the readiness of agencies in implementing the Information Security Management System (ISMS) to ensure of agency information security in terms of confidentiality, integrity and availability. The target group for this study is comprised of IT personnel from computer technician grade until Head of ICT Department. This is needed to assess the level of staff awareness to information security issues regardless of grade specific. The target group also includes specific skills of ICT application development, network and security, hardware solution and so on.

Total target respondents are 50 people which include various ICT positions. The questionnaires developed using Google Docs application. This question is disseminated to Local Authority ICT group on social networking as a medium to spread. The target group consists of officers and employees of ICT from 144 local authorities in Malaysia.

1.8 Summary

A summary of this chapter is to identify the readiness of agencies to implement the ISMS certification standard based on security compliance adopted by the agency in the management security of the information is protected. And from the research, the findings can be summarized either a local authority willing or not in implementing Information Security Management System (ISMS) to protect their information, particularly information of taxes assessment.

REFERENCES

[1] R. Abdullah and R. N. Wafiah, "Penambahbaikan pengurusan penyemakan semula senarai nilaian pihak berkuasa tempatan," Universiti Teknologi Malaysia, Faculty of Geoinformation Science and Engineering, 2009.

[2] P. Upadhyaya, S. Shakya, and M. Pokharel, "E-government security readiness assessment for developing countries: Case study: Nepal Govt. organizations," *Internet AH-ICI 2012 Third Asian Himalayas Int. Conf. On*, pp. 1–5, Nov. 2012.

[3] Jabatan Perdana Menteri, "Panduan Keperluan Dan Persediaan Pelaksanaan Pernsijilan MS ISO/EIC 27001: 2007 DAlam Sektor Awam." 24 November 2010, 24-Nov-2010.

[4] Setiausaha Kerajaan Negeri, "Buku Dasar Keselamatan ICT Negeri Sembilan," 2010. [Online]. Available: http://pdtpd.ns.gov.my/en/images/pdf/dasarkeselamatanict.pdf. [Accessed: 03-Dec-2013].

[5] V. Vasudevan, A. Mangla, F. Ummer, S. Shetty, S. Pakala, and S. Anbalahan, *Application Security in the ISO27001 Environment*. It Governance Ltd, 2008.

[6] M. Al-Awadi and K. Renaud, "Success factors in information security implementation in organizations," in *IADIS International Conference e-Society 2007*, 2007, pp. 169–176.

[7] A. AlHogail and J. Berri, "Enhancing IT security in organizations through knowledge management," *Inf. Technol. E-Serv. ICITeS 2012 Int. Conf. On*, pp. 1–6, Mar. 2012.

[8] Malaysian Administrative Modernisation and Management Planning Unit, MAMPU, "TMalaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS)." [Online]. Available: http://www.mampu.gov.my/documents/10228/18762/chapter1.pdf/fcac2246-d1c3-4d95-b410-97615384a6d0. [Accessed: 03-Dec-2013].

[9] D. Milicevic and M. Goeken, “Application of models in information security management,” *Res. Chall. Inf. Sci. RCIS 2011 Fifth Int. Conf. On*, pp. 1–6, May 2011.

[10] Y. Zhiwei and J. Zhongyuan, “A Survey on the Evolution of Risk Evaluation for Information Systems Security,” *2012 Int. Conf. Future Electr. Power Energy Syst.*, vol. 17, Part B, no. 0, pp. 1288–1294, 2012.

[11] K. Pecina, R. Estremera, A. Bilbao, and E. Bilbao, “Physical and Logical Security management organization model based on ISO 31000 and ISO 27001,” *Secur. Technol. ICCST 2011 IEEE Int. Carnahan Conf. On*, pp. 1–5, Oct. 2011.

[12] Webmaster MKN, “Laman Web Rasmi Majlis Keselamatan Negara,” 2013. [Online]. Available: http://www.mkn.gov.my/mkn/default/article_m.php?mod=4&fokus=17. [Accessed: 03-Dec-2013].

[13] Webmaster MyCERT, “Malaysian Computer Emergency Response Team,” 2013. [Online]. Available: http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html. [Accessed: 03-Dec-2013].

[14] Chi-Hsiang Wang and Dwen-Ren Tsai, “Integrated installing ISO 9000 and ISO 27000 management systems on an organization,” *Secur. Technol. 2009 43rd Annu. 2009 Int. Carnahan Conf. On*, pp. 265–267, Oct. 2009.

[15] M. Mohseni, “Has your organization compliance with ISMS? A case study in an Iranian Bank,” *ArXiv Prepr. ArXiv13030468*, 2013.

[16] Y. Qian, Y. Fang, and J. J. Gonzalez, “Managing information security risks during new technology adoption,” *Comput. Secur.*, vol. 31, no. 8, pp. 859–869, Nov. 2012.

[17] R. Montesino and S. Fenz, “Information Security Automation: How Far Can We Go?,” 2011, pp. 280–285.

[18] Z. Cosic and M. Boban, “Information security management — Defining approaches to Information Security policies in ISMS,” *Intell. Syst. Inform. SISY 2010 8th Int. Symp. On*, pp. 83–85, Sep. 2010.

[19] Craig S Wright, “Implementing an Information Security Management System (ISMS) Training process,” 2011. [Online]. Available: http://www.giac.org/paper/g2700/39/implementing-information-security-management-system-isms-training-process/107335. [Accessed: 03-Dec-2013].

[20] N. Feng, H. J. Wang, and M. Li, “A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis,” *Bus. Intell. Risk Manag.*, vol. 256, no. 0, pp. 57–73, Jan. 2013.

[21] N. Modiri and Y. M. Sobhanzadeh, “Information Security Management,” *Comput. Intell. Commun. Netw. CICN 2011 Int. Conf. On*, pp. 481–484, Oct. 2011.

[22] R. Montesino and S. Fenz, “Automation Possibilities in Information Security Management,” *Intell. Secur. Inform. Conf. EISIC 2011 Eur.*, pp. 259–262, Sep. 2011.

[23] W. Boehmer, “Toward a Target Function of an Information Security Management System,” *Comput. Inf. Technol. CIT 2010 IEEE 10th Int. Conf. On*, pp. 809–816, Jun. 2010.

[24] J. J. C. H. Ryan, T. A. Mazzuchi, D. J. Ryan, J. Lopez de la Cruz, and R. Cooke, “Quantifying information security risks using expert judgment elicitation,” *Spec. Issue Oper. Res. Risk Manag.*, vol. 39, no. 4, pp. 774–784, Apr. 2012.

[25] Unit Malaysian Administrative Modernisation and Management Planning, Ed., *The Malaysian public sector information security risk assessment methodology (MyRAM) handbook*. Putrajaya: Malaysian Administrative Modernisation and Management Planning Unit, 2005.

[26] “SUCCESS FACTORS IN INFORMATION SECURITY IMPLEMENTATION IN ORGANIZATIONS.” [Online]. Available: http://www.dcs.gla.ac.uk/~karen/Papers/sucessFactors2.pdf. [Accessed: 30-May-2013].

[27] Joy Wong, “The 2007 Estonian Cyberattacks : New Frontiers in International Conflict,” Dec-2012. [Online]. Available: http://blogs.law.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/. [Accessed: 03-Dec-2013].

[28] Majlis Keselamatan Negara, “Buku Arahan Keselamatan Malaysia,” 2010. [Online]. Available: http://www.moe.gov.my/bpsm/v1/muatturun/nota%20kissm%202/8.0%20%20ARAHAN%20KESELAMATAN.pdf. [Accessed: 03-Dec-2013].

[29] I. Tashi and S. Ghernaouti-Helie, "A Security Management Assurance Model to Holistically Assess the Information Security Posture," *Availab. Reliab. Secur. 2009 ARES 09 Int. Conf. On*, pp. 756–761, Mar. 2009.

[30] H. Susanto12, M. N. Almunawar, and Y. C. Tuan, "Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level," *Int. J. Eng. Technol.*, vol. 2, no. 1, 2012.