Journal of Systems and Information Technology

Collective information structure model for Information Security Risk Assessment (ISRA)

Palaniappan Shamala Rabiah Ahmad Ali Hussein Zolait Shahrin bin Sahib

Collective information structure model for Information Security Risk Assessment (ISRA)

Palaniappan Shamala
Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia

Rabiah Ahmad
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, UniversitiTeknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Ali Hussein Zolait
College of Information Technology, University of Bahrain, Sakhir, Kingdom of Bahrain, and

Shahrin bin Sahib
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, UniversitiTeknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Received 11 February 2015
Revised 3 April 2015
Accepted 4 April 2015

Abstract

Purpose – Information security has become an essential entity for organizations across the globe to eliminate the possible risks in their organizations by conducting information security risk assessment (ISRA). However, the existence of numerous different types of risk assessment methods, standards, guidelines and specifications readily available causes the organizations to face the daunting tasks in determining the most suitable method that would augur well in meeting their needs. Therefore, to overcome this tedious process, this paper suggests collective information structure model for ISRA.

Design/methodology/approach – The proposed ISRA model was developed by deploying a questionnaire using close-ended questions administrated to a group of information security practitioners in Malaysia ($N = 80$). The purpose of the survey was to strengthen and add more relevant additional features to the existing framework, as it was developed based on secondary data.

Findings – Previous comparative and analyzed studies reveals that all the six types of ISRA methodologies have features of the same kind of information with a slight difference in form. Therefore, questionnaires were designed to insert additional features to the research framework. All the additional features chosen were based on high frequency of more than half percentage agreed responses from respondents. The analyses results inspire in generating a collective information structure model which more practical in the real environment of the workplace.

The authors would like to thank University Tun Hussien Onn Malaysia (UTHM) for supporting this research. The authors would also like to thank SIRIM QAS, CyberSecurity and all the Information Security Practitioners for their support.

Journal of Systems and Information Technology
Vol. 17 No. 2, 2015
pp. 193-219

1328-7265
DOI 10.1108/JSIT-02-2015-0013

Practical implications – Generally, organizations need to make comparisons between methodologies and decide on the best due to the inexistence of agreed reference benchmark in ISRA methodologies. This tedious process leads to unwarranted time, money and energy consumption.

Originality/value – The collective information structure model for ISRA aims to assist organizations in getting a general view of ISRA flow and gathering information on the requirements to be met before risk assessment can be conducted successfully. This model can be conveniently used by organizations to complete all the required planning as well as to select the suitable methods to complete the ISRA.

Keywords Risk assessment, Collective information structure, Info-structure, Information security, Information security risk assessment (ISRA)

Paper type Research paper

1. Introduction

Information security has drawn attention from researchers, professionals, journalists, legislators, governments and citizens to raise awareness among organizations to invest in information security for decision-making and for the continuance of high-standard business operations (Jourdan *et al.*, 2010). Hence, regardless of being government, private or public organizations, most of them are currently applying a range of security counter measures, policies, procedures and guidelines to protect their organizations. This awareness was due to the fact that security incidents can lead to severely adverse consequences for organizations, such as substantial losses to the industry through the direct loss of information assets and financial impact, a loss in organizational reputation and customer confidence and a loss of employee productivity or the risk of legal issues (Alberts and Dorofee, 2002; Dzazali *et al.*, 2009; Shedden *et al.*, 2010, 2011).

To maintain confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, the organizations apply information security risk assessments (ISRA) to determine the extent of the potential threats and the risks associated with the information technology (IT) system (Söderström *et al.*, 2009; Syalim *et al.*, 2009). An ISRA method identifies the security risks in the organizations and provides a measured, analyzed security risk profile of the critical assets in order to build plans to treat the risks (Lichtenstein, 1996; Shedden *et al.*, 2009, 2010, 2011).

Although there are numerous ISRA methods currently available, many organizations are facing the daunting tasks of determining the most appropriate methodology based on their specific needs (Vorster and Labuschagne, 2005). On the contrary, the inexistence of one ideal risk assessment method that would be suitable for all organizations has made the situation even more cumbersome for end-users (Lichtenstein, 1996). Furthermore, the currently available ISRA methodologies do not define detailed steps of risk assessment.

However, this lacking was overcome by using an ISRA info-structure which anchors on identifying the similarities in info-structure among the existing ISRA methodologies. Two types of comparative studies have been conducted to identify the similarities in info-structure among the existing ISRA methodologies (Shamala *et al.*, 2013). Info-structure is the layout of information which is organized in a useful fashion and can be navigated at any time. The ISRA info-structure was developed based on secondary data.

Therefore, a survey was conducted to strengthen and add more relevant features based on the actual risk assessment environment. In addition, through this study, valuable information regarding the general information and complete picture of ISRA

approach in Malaysia will be discovered. This study deployed a questionnaire using closed-ended questions administered to information security practitioners at Malaysia. The results of this study were analyzed and the most agreed features among practitioners were chosen to be added in the framework.

As a final outcome, a collective information structure model was developed. The proposed model can assist organizations in getting a general view of ISRA flow, types of information to be gathered and the requirements to be met before risk assessment can be conducted successfully. Organizations will then be able to establish accurate planning decisions and these enable them to successfully draft correct and consistent planning for the ISRA process.

The paper is organized into several sections. The immediate section describes the overview of information security risk management methodologies and briefly describes information security risk assessment in Malaysia. Section 3 explains the research framework and Section 4 explains the research methodology used in this study. Section 5 presents the survey results, followed by the proposed collective information structure model in Section 6. Last but not least, Section 7 concludes the paper.

2. Literature review

2.1 Overview of information security risk management methodologies

The literature defines information security as a set of processes, procedures, personnel and technology charged in protecting an organization's information assets (Jourdan *et al.*, 2010). Meanwhile, it can also be referred as the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure or use of information and information resources, whether accidental or intentional (Alnatheer and Nelson, 2009). The needs of information security become vital due to the current trends in information transfer through the borderless and vulnerable world. Most of the organizations have substantially replaced the physical form of data with electronic forms of data as permitted by the current broadband networks and high capacity electronic data storage technologies. Information security has attracted the attentions of small or multi-national organizations because the enormous changes in the structure and types of the information technologies applied to information can create risks.

Organizations conduct ISRA by identifying their security risks in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. ISRA is able to determine the extent of the potential threat and the risk associated with an IT system and provide a measured, analyzed profile of critical assets to develop effective plans to treat the risk (Baskerville, 1991; Braber *et al.*, 2007; Lichtenstein, 1996; Shedden *et al.*, 2009, 2010, 2011; Syalim *et al.*, 2009). To make the ISRA process more systematic and effective, practitioners need to properly define detailed steps in risk assessment planning. Risk assessment process involves a series of tasks broken down by phases where each phase requires information for its success. Many research articles have clearly argued and provided evidence that many organizations are facing problems in selecting suitable methods that would augur well in meeting their needs (Bornman and Labuschagne, 2004; Eloff and Eloff, 2005; Lichtenstein, 1996; Saleh and Alfantookh, 2011; Spears, 2006; Syalim *et al.*, 2009; Vorster and Labuschagne, 2005).

Thus, ISRA info-structure could provide the positive impact to ISRA practitioners in knowing before-hand what information they needed before the commencement of the

plan. In fact, the existing ISRA info-structure is sufficient to be used to complete all the required planning followed by selecting the suitable methodologies to complete the risk assessment. However, some extra features added to the previous ISRA info-structure will enable organizations to establish accurate security planning decisions and assist them to successfully draft correct and consistent planning for ISRA process.

2.2 Information security risk assessment in Malaysia

Information Security Management Systems (ISMS) is a systematic and structured approach in managing information which includes policies, processes, procedures, organizational structures and software and hardware functions. Initially, ISMS was initiated from the UK Department of Trade and Industry in 1995 and its main objective was to provide a code of practice for the information security practitioners.

It is widely acknowledged in the security research and practice that the rising number of security breached over the years has led to the increased security concerns among organizations throughout the world. Hence, Malaysian organizations are also not lagging behind from protecting data and having information security standards to ensure data security. Thereby, the National ICT Security & Emergency Response Center (NISER) and SIRIM QAS International Sdn. Bhd. have jointly conducted the Information Security Technical Expertise for ISMS pilot program (Jalil and Hamid, 2003). SIRIM Berhad, a company wholly owned by the Malaysian Government, was established on September 1,1996 as a successor company to the Standards and Industrial Research Institute of Malaysia (SIRIM) upon the enactment of the Standards of Malaysia Act in 1996 (StandardsMalaysia, 2009). While based on the CyberSecurity's official Web site, NISER was created in 2001 and, on August 20, 2007, the Prime Minister of Malaysia officiated the rebranding of NISER into CyberSecurity Malaysia. To date, only SIRIM Berhad and CyberSecurity have received the accreditation certificate from Standards Malaysia for complying with ISO/IEC 27001:2007 international standards for certification bodies.

Under the Malaysian Standards System, SIRIM Berhad has been assigned to manage the sector-based industrial standards committees (ISC) and their technical committees (TC) and working groups (WGs) (StandardsMalaysia, 2009). In 2001, Industrial Standards Committees for Information Technology, Communication & Multimedia (ISC G) established a Technical Committee on Information Security (TC/G/5), and their mission is to develop, prepare and review information security and its related standards for Malaysia (Mustafa, 2012). TC/G/5 has established five WGs to undertake the information security standards development projects (Zakaria, 2008).

Based on the Malaysian Cabinet Ministers meeting on 24th February 2010, it was agreed that all the Critical National Information Infrastructure (CNII) sectors such as National Defense & Security, Banking & Finance, Information & Communications, Energy, Transportation, Water, Health Services, Government, Emergency Services, Food & Agriculture are to be certified to ISO/IEC 27001 standards, which is the internationally recognized standards for ISMS by March 2013. Besides CNII sectors, other private and government sectors also apply ISMS certification.

3. Research framework

Figure 1 depicts the research framework for the study.

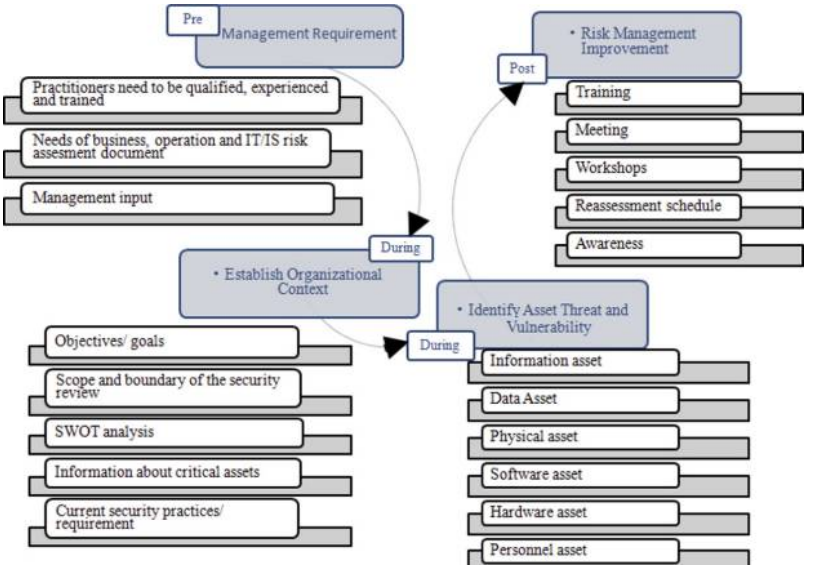

Figure 1.
Research framework

The research framework was generated based on all mutual features that exist in the six types of ISRA methodologies. Among them are:

(1) Professional organization:
- CRAMM (Bornman and Labuschagne, 2004; Sarkheyli and Ithnin, 2010; Siemens, 2005; Yazar, 2002);
- CORAS (Aagedal *et al.*, 2002; Bornman and Labuschagne, 2004; Braber *et al.*, 2007; Dahl, 2008; Fredriksen *et al.*, 2002; Lund *et al.*, 2011; Raymond, 1993; Refsdal, 2011a, 2011b; Vorster and Labuschagne, 2005); and
- OCTAVE (Albert and Dorofee, 2001; Alberts *et al.*, 2003, 2001; Bornman and Labuschagne, 2004; Elky, 2006; Sarkheyli and Ithnin, 2010; Visintine, 2003; Vorster and Labuschagne, 2005).

(2) Research project:
- ISRAM (Karabacak and Sogukpinar, 2005; Vorster and Labuschagne, 2005); and
- Is Risk Analysis Based On Business Model (Suh and Han, 2003; Vorster and Labuschagne, 2005).

(3) International organization:
- NIST 800-30 (NIST, 2010, 2011a, 2011b; Stoneburner *et al.*, 2002; Syalim *et al.*, 2009).

The research framework is made up of four parts, as shown in Figure 1:

(1) the management requirement;

(2) establish organizational context;

(3) identify asset, threat and vulnerability; and
(4) risk management improvement.

There are three repositories in the framework, the ISRA info-structure frame, one to plan beforehand, during and post. This model is developed based on literature reviews and each selected feature in the research framework was based on the highest frequency of the "most often agreed" responses. Because the research framework was developed based on the comparative studies and literature reviews, a study was conducted in 2014 as the main objective to strengthen and add other features on the present research framework.

4. Research methodology

To achieve the research objective, the instrument of the study, namely, questionnaire was structured. Survey questions were formed according to the main features namely, management requirement, establish organizational context, identify assets threats and vulnerabilities and risk management improvement as in the research framework.

4.1 Instrument creation

The questions for the survey were created by referring to journal, conference and survey papers with similar research topics. First, a literature search was undertaken to find out all the information security-related journals, conference papers and surveys. The survey instrument was developed by referring to the following articles in Table I. The symbol "✓" notifies that the questions for the session have been referred to that particular article. However, most questions have been formed by own which only refer to the ways of asking questions and the options offered for questions. To check the reliability and validity of the instrument constructed, a questionnaire was sent to an expert review panel.

The questionnaire was divided into five sections. Section 1 highlights the demography of the respondents. Section 2 defines ISRA profile in Malaysia specifically related to information security units. Section 3 captures the ISRA management requirements which emphasis on how top management provides information security staff with necessary skills, experiences and education. Section 4 determines how organizations gather relevant information to identify the important IT resources of information before establishing the ISMS. Section 5 addresses the risk management improvement to identify the overall security awareness such as training, meeting, workshops, reassessment schedule and awareness.

4.2 Data collection

The lists of respondents were gathered from official Web sites of SIRIM QAS, CyberSecurity Malaysia and International Register of ISMS Certificates. A total of 110 organizations practicing risk assessment at workplace were selected and questionnaires were distributed. As it was a paper–pencil-questionnaire, the questionnaire was personally administrated. Eighty (80) questionnaires were returned. This interprets to 72.70 per cent response rate. All returned questionnaires were found to be usable for further analysis.

	Paper	Year	Referred section (Sc) in article Sc1	Sc2	Sc3	Sc4	Sc5
1	Result of the Attitude Survey on Information Security (CICC, 2009)	2009		✓			✓
2	Report on the Culp, 2011 Global Risk Management Study (Culp, 2011)	2011	✓	✓	✓	✓	✓
3	2011 HIMSS Security Survey (HIMSS, 2011)	2011		✓			✓
4	Fighting to close the gap: Ernst and Young's 2012 Global Information Security Survey (Kessel, 2012)	2012		✓	✓		✓
5	The 2011 (ISC)2 Global Information Security Workforce Study (Ayoub, 2011)	2011	✓				
6	Progress in Financial Services Risk Management: A Survey of major financial institutions (Schlich and Jackson, 2008)	2008					✓
7	El Paso Community College Information Security Risk Assessment Survey (Rubio, 2004)	2004					✓
8	Law Firms and Risk Control: Information Security and Confidentiality Survey Results (Stephen *et al.*, 2011)	2011		✓			✓
9	Employer Experiences & Expectations: Findings, Training, and Keeping Qualified Workers (Perron, 2011)	2011					✓
10	Industry Training Review: Results of the employer interviews & survey (Ministry Education, 2012)	2012			✓		
11	State of Security (Evalueserve, 2012)	2012		✓	✓		
12	The Australian Business Assessment of Computer User Security: a national survey (Richards, 2009)	2009		✓			
13	2010/2011: Computer Crime & Security Survey (Richardson, 2011)	2011		✓			
14	Irish Information Security and Cybercrime Survey: A closer look (McDonnel *et al.*, 2012)	2012					✓

Note: ✓: Items referred to develop survey questions

Table I. List of articles referred during questionnaire development

4.3 Sample characteristics

Table II portrays the demographic profile of the respondents by gender, types of industry, job position, educational level, IT security experience, certified information security staff, information security involvement and grade in auditing.

As depicted in the table, the participants work in various industries in both the public and private sectors. The professionals also have variety of roles in the organizations. It was found that 32.50 per cent of professionals are management executives. Professionals who have titles of security officer and security staffs resulted in 13.75 and 15.00 per cent, respectively. It indicates that more than half of the professionals (61.25 per cent) have crucial information security management responsibilities.

Two different questions have been intended to ensure the samples selected for this survey are significant. The samples were notable for two reasons:

(1) For a question about knowing whether practitioners are certified staffs, more than half of participants (65.00 per cent) agreed that they are certified

Profile	Frequency (*N*)	(%)
Gender		
Male	42	52.50
Female	38	47.50
Types of industry		
Financial and insurance service	8	10.00
Electricity, gas, water and waste services	5	6.25
Agriculture, forestry and technical services	–	–
Consultancy	5	6.25
Information technology	33	41.25
Manufacturing	1	1.25
Government-federal, military	16	20.00
Medical/health care – public or private	1	1.25
Consumer products/retail/wholesale	–	–
Professional service – legal, marketing	–	–
Education/research	1	1.25
Travel/hospitality	–	–
Telecommunications	6	7.50
Mining	–	–
Administrative and support services	1	1.25
Culture and recreational services	–	–
Property and business services	1	1.25
Others	2	2.50
Job position		
Executive management	26	32.5
Security officer	11	13.75
security staff	12	15.00
IT staff	24	30.00
Technical management	5	6.25
Consultant/contractor	2	2.50
System administrator	–	–
Education level		
High school graduate or less	1	1.25
Some college/technical school	4	5.00
Associate degree or technical certification	4	5.00
Bachelor	52	65.00
Master	19	23.75
Doctorate	–	–

Table II.
Sample characteristics of respondents

information security staffs. Within this percentage, only 51.25 per cent participants specified the type of certification they get to be declared as certified information security staffs. Professionals who had the Certified Information Security Systems Professional (CISSP) certification and information security related certification resulted in 10.00 and 5.00 per cent, respectively. About another 36.25 per cent professionals held at least auditor certification and became lead auditors. Information security certification is one of the most selective certifications in information security profession and

individuals who certified are held to the highest professional and ethical standards.

(2) The sample of information security professionals provided data from individuals who are highly knowledgeable about the ISRA process at their respective organizations. This is proven by asking their involvement in information security at workplace:

- strategic planning of information security;
- implementation of information security;
- risk analysis and auditing;
- general engineering; and
- providing certification service were given.

The result reported that majority of the participants (97.50 per cent) agreed that they are directly involved in the process of conducting ISRA by choosing options strategic planning of information security, implementation of information security, risk analysis and auditing and providing certification service. While about 2.50 per cent of the participants only involve in ISRA process as general engineers at workplace.

5. Survey result

5.1 Section 2: profile of ISRA firms

The profile of information security section seeks to investigate the history of information security units profile in Malaysia. Table III represents the characteristics of the responding organization profile in terms of their information security department age, size and percentage of IT budget spent on information security.

From the table above, more than half of respondents (56.25 per cent) stated information security firms were established in between 1 and 5 years. Nearly one-third of the firms (33.75 per cent) were old-aged individuals in which firm age more than 10 years and between 6 and 10 years resulted in 7.50 and 26.25 per cent, respectively. On the other hand, around 10.00 per cent of the firms are known as newly established which less than 1 year was. The survey showed that the number of firms forming information security department in their workplace is increasing in the past 10 years due to the awareness in protecting information.

It can be concluded that the information security department in Malaysia is still at an early developing age. This is due to the low number of employees working in this department, nearly half (48.75 per cent) of the respondents indicated 1-5 people, whereas slightly over a third of the respondents (37.50 per cent) stated in the range from 6 to 13 people. It is found that only 13.75 per cent respondents have chosen "others" option which is pointing to the size of their firm that exceeds 13 employees.

Information security department seems to be well aware that the financial and management aspects of dealing with security are as critical to their mission as the technical aspects of security. A question to explore the issue related to budget was aimed at determining the typical size of an organization's information security budget relative to the organization's overall IT budget. As seen in Table III, more than half of the respondents (58.75 per cent) indicated that their organization allocated more than 5 per cent of the total IT budget to security. Only 7.50 per cent of the respondents indicated that security received between 1 and 5 per cent of the budget, 5 per cent of the

Organization Profile	(%)
Information security department age (years)	
Less than 1	10.00
Between 1 and 2	28.75
Between 3 and 5	27.50
Between 6 and 7	13.75
Between 8 and 10	12.50
More than 10	7.50
Information department size	
One people	2.50
2-5 people	46.25
6-9 people	25.00
10-13 people	12.50
Others	13.75
IT budget spent on information security (%)	
More than 10	31.25
8-10	20.00
6-7	7.50
3-5	6.25
1-2	1.25
Less than 1	5.00
None	1.25
Do not know	27.50

Table III.
Characteristics of the responding organization profile

respondents stated security received less than 1 per cent of the budget, while 27.50 per cent of the respondents indicated that the portion was unknown to them.

5.1.1 Information security policy. Security policies are the cornerstone of a successful information security architecture because it provides clear instructions about information security and establishes management support (Filho *et al.*, 2011). Thus, majority of the respondents (98.75 per cent) as stated in the Table IV, were aware of the needs of security policies and they have formal policies/procedures in place related to addressing a security breach, while the remaining respondents (1.25 per cent) are moving forward to develop policies/procedures in the future.

To protect an organization's information assets, the management was using the policy to help the organization ensure that they have the controls in place to work

Does the organization have documented information security policies and procedures in place to respond to threats and/or incidents relating to a security breach?	(%)
We have these types of policies and procedures in place	98.75
We are currently developing those types policies and procedures	–
We do not have this types of plan in place and plans to establish one in the future	1.25
We do not have this type of plan in place and NO plans to establish one in the future	–

Table IV.
Information security policies and procedures in place to respond to threats

toward compliance by mapping policy statements to legislative requirements. Thus, respondents were asked to indicate the types of reference points used for developing their information security policies. Even though there are many types of reference points to refer for developing policies, result reported that the respondents totally agreed to ISO/IEC 27001 (100 per cent) as their reference point. This may be due to the enforcement by the government where, during the Malaysian Cabinet Ministers meeting on February 24, 2010, it was agreed that all the Critical National Information Infrastructure (CNII) sectors are to be certified to ISO/IEC 27001 standards. Apart from ISO/IEC 27001, organizations also refer to other standards as shown in Table V to develop the information security policy.

5.2 Section 3: ISRA management requirement

Management requirement is a process of determining the security capabilities that their ISRA unit should have to prepare them with the desired level of mission support in the face of real-world threats. This section seeks additional features to be added in the post step of risk assessment. Management should take into consideration the basic requirements like using information security staff who haves the detailed knowledge and expertise required to manage the success security aspects, prerequisite management involvement and to review the formal documents that provide an overview of security requirement in place to conduct risk assessment in a more systematic and effective manner.

There is no doubt that the information security methodology emphasizes that organizations should only hire information security staff with necessary skills, experiences and qualifications to successfully complete the task. This was due to fact that risk assessments are influenced by the personal experiences and accumulated knowledge of the individuals conducting the risk assessments.

Thus, to know the actual scenario result, questions were asked to understand the actual procedures of hiring staffs whether organizations have any guideline of reference and job descriptions to refer.

Table V. Types of reference points used for developing information security policies

What are the types of reference points used for developing information security policies?	(%)
ISO/IEC 27001 (ISMS requirements specification)	100.00
ISO/IEC 27002 (Code of Practice (Pragmatic ISMS advice)	41.25
National standard or national guideline	6.25
ACSI 33	1.25
HB 231	1.25
HB 171	1.25
RFC 2196	1.25
ISO/IEC 13335	2.50
ISO/IEC 14516	2.50
NIST	5.00
Measures that are requested by business partners	8.75
Company's own rule	13.75
Vendor-specific standards or guides	7.50
Industry-specific IT security standard	21.25
Best practice	22.50

Majority of the respondents as shown in Table VI agreed that they have established the guidelines/terms of reference for education (81.25 per cent), experience (85.00 per cent) and skills (82.50 per cent) to hire information security staff and only very few declined of having guidelines for education (5.00 per cent), experience (2.50 per cent) and skills (3.75 per cent) in place. Even though fewer per cent of respondents (13.75 per cent – education; 12.50 – experience; and 13.75 per cent – skills) do not have it but they do understand the importance of having the guidelines/terms of reference to hire information security staff in future.

5.2.1 Criteria for hiring/promoting information security practitioners. Table VII reveals that organizations have ranked the criteria based on the number of vote when hiring or promoting information security staff.

Majority of the survey respondents (97.50 per cent) voted on experience, skill and abilities and knowledge as their utmost important criteria when hiring/promoting information security staff. Organizations do not need to invest a lot on fresh graduate for training and workshop to gain knowledge in their area. Interestingly, the second highest (92.50 per cent) essential criteria will be education in which two-thirds of the respondents (76.25 per cent) expected their staff to have professional designations in the field of information security. Based on the comparison study done on the six types of risk methodologies, it was agreed among all of them that practitioners who are involved in ISRA must have the skill, qualification, experience and training. However, the survey results reveal that practitioners should take into consideration the experience, skill and abilities and knowledge followed by education and professional designation. Table VII shows that most of the practitioners voted for all the five criteria and gave nod to choose them as a hierarchy of criteria when hiring or promoting information security staff.

5.2.2 Types of risk assessment documentations. As shown in Table VIII, the survey results also agreed with the comparative results of six types of ISRA methodologies which emphasize that security practitioners need to provide the three documents before

Table VI.
Established guideline of reference in place to hire information security staff with necessary skills, experience and education

Does your organization have any established guideline/term of reference to hire potential information security staff with necessary skills, experience and education to successfully complete the task your organization needs to perform?			
	Have (%)	Don't have (%)	Don't have but understand it is important (%)
Education	81.25	5.00	13.75
Experience	85.00	2.50	12.50
Skills	82.50	3.75	13.75

Table VII.
Organization's considered criteria when hiring/promoting information security staff

Which criteria do your organization consider when hiring or promoting information security staff?			
	Considered as important (%)	Not taken into consideration (%)	Do not know (%)
Experience	97.50	1.25	1.25
Skill and abilities	97.50	1.25	1.25
Knowledge	97.50	1.25	1.25
Education	92.50	5.00	2.50
Professional designations	76.25	21.25	2.50

carrying out the risk analysis process. It is important to review and revised these documents in order to draw and plan the ISRA process perfectly.

5.2.3 Pre-requisite management input: Infosec. personnel support & participation and top management involvement and support in information security. Before proceeding with the ISRA, it is important to get the management input to understand and to ensure that the initial step of ISRA is correct. Questions were asked regarding to these features to get clearer pictures of the top management involvement during ISRA process.

In response, Table IX indicates that the ISRA process was not simply delegated to the IT department, but the organization also used professionals with a diverse knowledge of all the functional area, with a believe that a more successful ISRA process could be achieved. More than half of the respondents stated that IS/IT/ technical management (82.5 per cent), department manager/supervisor/ director (70.00 per cent) and system or network administrators (60.00 per cent) are mostly involved in the ISRA process. In knowing who had the final approval of the ISRA process, more than three-quarter of respondents (86.25 per cent) voted on senior manager/executive (CEO, CIO) as shown Table X. As a result, in can concluded that at least the following personnel should be involved during ISRA participation and approval:

- Senior Manager/Executive (e.g. CEO, CIO);
- IS/IT/Technical Management;
- Department Manager/Supervisor/Director; and
- System or Network Administrators.

Because the management input is very important for the success of ISRA, ISRA practitioners were asked to indicate the top management involvement in their

Do your information security team review the organizational business, operational or IT/IS risk assessment documentation as an initial preparations prior to the actual startup of the risk analysis?

	Yes (%)	No (%)
Documentation of IT/IS	93.75	6.25
Documentation of operational	98.75	1.25
Documentation of business function	91.25	8.75

Table VIII. Types of documentation will be used during risk assessment

Which of the following individuals at your organization or your client's organization participated in information security risk analysis? (You may select more than ONE (1) of the following)

	(%)
IS/IT/technical management	82.50
Department manager/supervisor/director	70.00
System or network administrators	60.00
Senior manager/executive (e.g. CEO,CIO)	46.25
Other managerial Officers	33.75
Owner/partner	28.75
General staff	25.00
Consultant/contractor	18.75
Others	1.25

Table IX. Individuals who participated in information security risk analysis

organization. The data presented in Table XI appear to indicate that respondents had agreed that they need top management involvement for the effective risk analysis. A well-informed top management task, when followed effectively can help the management to identify the appropriate controls for providing the mission essential security capabilities. By enabling top management to give positive inputs throughout the risk assessment, it will provide the desired level of mission support in the face of real-world threats.

Seven tasks proposed to be the responsibility of the top management to bear for the sake of effectiveness and success of the ISRA have been supported by the ISRA practitioners. Majority of the respondents had rated "Agree" and "Strongly Agree" on the issue that top management should involve and support in information security task. It was reported when the "Agree" and "Strongly Agree" are totaled up; respondents rated T1 (92.75 per cent), T2 (91.25 per cent), T3 (95), T4 (92.5 per cent), T5 (86.25 per cent), T6 (91.25 per cent) and T7 (82.5 per cent) accordingly. Thus, it can be concluded that ISRA practitioners expect top management involvement and support as shown in the list below:

- Consider IS as important organizational priority.
- Consider IS issues into account when planning corporate strategies.
- Involve in deciding IS issues.
- Involve in IS decisions.

Table X.
Individuals who have the final approval of the information security risk analysis

Which of the following individuals at your organization or your client's organization have the final approval of the information security risk analysis? (You may select more than ONE (1) of the following)	(%)
Senior manager/executive (e.g. CEO,CIO)	86.25
Department manager/supervisor/director	41.25
Owner/partner	11.25
IS/IT/technical management	10.00
Consultant/contractor	1.25
Other managerial officers	–
Others	–

Table XI.
Top management involvement and support in information security task

How does top management involve and support in information security task during risk analysis process in their organization?	Strongly agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly disagree (%)
Consider IS as important organizational priority (T1)	66.25	27.50	2.50	–	3.75
Involved in deciding IS issues (T2)	55.00	36.25	3.75	2.50	2.50
Involve in IS decisions (T3)	55.00	40.00	3.75	–	1.25
Support for IS functions (T4)	51.25	41.25	5.00	1.25	1.25
Attend IS meeting (T5)	47.50	38.75	8.75	3.75	1.25
Consider IS issues into account when planning corporate strategies (T6)	40.00	51.25	6.25	–	2.50
Involve in IS activities (T7)	35.00	47.50	13.75	2.50	1.25

- Involve in IS activities.
- Attend IS meeting.
- Support for IS functions.

5.3 Section 4: establish organizational context and identify asset, threat and vulnerability

By establishing the organizational context, the organization articulates its objectives, scopes and defines the external and internal parameters to be taken into account when managing risk. In addition, identifying of the key risk to the organization is also a critical step in effective risk management and needs to be comprehensive. This section seeks additional features to be added in the steps which need to be completed during risk assessment.

5.3.1 Establishment of organizational context. In assessing risks, the first step is to define the organizational context. Organizational context establishment allows the organization to determine the basic criteria, purposes, scopes and the boundaries of the business environment to ensure that the risk assessment process achieves the maximum effectiveness and to assure that any risk in the organization's industry is identified. Therefore, respondents were asked to identify the organizational context lists which are essential for defining the risks. Table XII presents a result of organizational context preferences at the respondents' organizations.

Table XIII below shows two columns where the first column shows the list of organizational context which mostly agreed by ISRA methodologies and the second column shows lists which were selected by more than half of the respondents as the organizational context lists.

The combined results of the two columns produced a complete list and should become the priorities by ISRA practitioners to ensure ISRA process added true value:

- organizational objectives/goals;
- organizational scope and boundaries;
- scope and boundary of the security review;
- SWOT analysis;

Which of the following individuals at your organization or your client's organization have the final approval of the information security risk analysis? (You may select more than ONE (1) of the following)

	(%)
Organizational objectives/goals	87.50
Scope and boundary of the security review	86.25
Information about critical assets	78.75
Organizational scope and boundaries	76.25
Threats and current organizational strength and vulnerabilities	75.00
Current security practices/requirement	73.75
Information related to the operational/business function	65.00
Person who use/support the IT system	56.25
Schedule and deliverable	45.00
SWOT analysis	26.25

Table XII. Establishment of organizational context

- information about critical assets;
- current security practices/requirement;
- Information related to the operational/business function;
- Person who use/support the IT system; and
- Threats and current organizational strength and vulnerabilities.

5.3.2 Information gathering techniques. In the risk management planning process, to define the organizational context, it is required to have a keen understanding of the system processing environment. Therefore, gathering relevant information is necessary. Information gathering technique can be used to gather information relevant to the risk assessment within its operational boundary. The assessment personnel should utilize some techniques to collect useful information. Table XIV presents techniques that ISRA practitioners use to gather informative information.

The techniques chosen by more than half of the respondents were selected. Among them are meetings (88.75 per cent), document review (71.25 per cent), security requirement checklist (58.75 per cent), brainstorming (57.50 per cent) and presentation and discussion (56.25 per cent) respectively. Based on the survey result, it can be

Table XIII. List of the organizational context which mostly agreed by ISRA methodologies and survey respondents

Organizational context list (agreed by ISRA methodologies)	Organizational context list (agreed by survey respondents)
Objectives/goals	Organizational objectives/goals
Scope and boundary of the security review	Scope and boundary of the security review
SWOT analysis	Organizational scope and boundaries
Information about critical assets	Threats and current organizational strength and vulnerabilities
Current security practices/requirement	Information about critical assets
	Current security practices/requirement
	Information related to the operational/business function
	Persons who use/support the IT system

Table XIV. Information gathering techniques

What techniques (anyone or a combination) do your organization use in gathering information relevant to identify IT resources of infrastructure or information that are valuable to the organization?	(%)
Meetings	88.75
Document review	71.25
Brainstorming	58.75
Security requirements checklist	57.50
Presentation and discussion	56.25
Interviews	46.25
Use of automated scanning tool	37.50
On-site interview	35.00
Structured questionnaire	25.00
Threat scenario approach	18.75
Delphi techniques	2.50

concluded that, ISRA practitioners mostly agreed that they are using the following information gathering techniques to identify IT resources of infrastructure or information that are valuable to the organization:

- meetings;
- document review;
- security requirement checklist;
- brainstorming; and
- presentation and discussion.

5.3.3 Important assets to be protected. Each organization has to identify the risks to their most important assets and build a strategy for protecting its critical assets. Based on the existing risk management methodologies, the following assets considered as very important for the organization are listed as information assets, data assets, physical assets, software assets, hardware assets and personnel assets. Generally, practitioners will also target these assets as the important assets for their organization when conducting risk assessments. This list of assets, however, is subject to change, whereby it may increase or decrease based on the scope of the security requirements of an organization. To know the similarity in the choices between the practitioners and risk management methodologies, a question was asked about the most important assets that should be protected when doing risk assessment.

With no surprise, ISRA practitioners also agreed with risk management methodologies assets list shown in Table XV. All the assets obtained more than half of the respondents' vote. The respondents voted information assets (95.00 per cent), data assets (91.25 per cent), physical assets (78.75 per cent), hardware assets (77.50 per cent), software assets (72.50 per cent) and personnel assets (65.00 per cent) accordingly. Thus, the list in the research model will remain the same.

5.4 Section 5: risk management improvement

It is a challenging task for the organization to mitigate and protect the organization's most important assets. Organizations achieve an ideal level of information security by minimizing the risks to an acceptable level. Because training the employees and promoting security awareness is a critical aspect (Metalidou *et al.*, 2014) to achieve a successful risk management program, ISRA practitioners should rely on the ongoing continuous processes of the evaluation, improvement, assessment and awareness of the ISRA process to safeguard the mission of their organization. However, based on the

Table XV. Important assets to be protected

Which assets do your organization consider as important and should be protected when doing risk assessment?	(%)
Information assets	95.00
Data assets	91.25
Physical assets	78.75
Hardware assets	77.50
Software assets	72.50
Personnel assets	65.00

comparative studies on six ISRA methodologies, it can be concluded that, the majority of the risk management methodologies are showing the lack of ongoing risk management projects facilitated by training, meeting, workshops, updating of risk, risk monitoring and also reassessment schedule. Therefore, for continuous improvement in risk management, ISRA practitioners should have more courtesy in risk management improvement as shown in Figure 2.

5.4.1 Information security training. When questioned on knowing the types of training provided to information security staffs and general staffs, the results of the study revealed in Table XVI show that staffs with different position should attend different training. Three types of training were listed for the respondents to vote to see whether the staffs needed training in information security. The respondents voted on information security staff should attend external training (83.75 per cent), internal training (68.75 per cent) and seminar (56.25 per cent) accordingly. Because the percentage of respondents' vote reached more than half, it shows that all three types of training are very important for the information security staff to ensure they understand and follow the requirements (Kaplan-Mor *et al.*, 2011) and become important components of the organization to maintain confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. Whereas for general staffs, majority of the respondents (81.25 per cent) agreed that general staffs should participate in internal training. Even though respondents have voted for external training (8.75 per cent) and seminar (25.00 per cent), the level of consent given still do not reach half of the respondents. It shows that general staffs at least need to be provided with internal training, so that they will be aware of the information security policy in place and general "rules of thumb" to make sure these policies are followed.

Based on the answers given by the respondents, the below list has been generated:

(1) information security staffs:
- external training;
- internal training; and
- seminar.

(2) general staffs:
- internal training.

5.4.2 Self-development program. Self-development program may refers as to the number of times individuals have attended formal and in-formal professional development

Figure 2.
Activity lists for risk management improvement

Table XVI.
Types of information security training provided for staffs

What are the ways staff undergo training on information security?	Information security staffs (%)	Genera staffs (%)
Internal training	68.75	81.25
External training	83.75	8.75
Seminar	56.25	25.00
None	–	1.25

programs like seminars, conferences, training sessions, workshops and certification courses or the evidence that these individuals did receive adequate knowledge to support them in their role as the key players in information security management (Dzazali and Zolait, 2012). Employees' professional development should be an ongoing process to ensure information security staffs learn about responsibilities and develop required skills and competencies to accomplish the goals and objectives of their organization. In addition, self-development program also can help staffs to grow personally and professionally in the information security field. To prove that information security staffs are actively engaged in a self-development program, questions about how frequent they have attended self-development program relating to information security within a year were asked. Table XVII reveals most of them were aware of the importance of attending the courses as a way for them to access their skills and qualities, consider their aims in information security and set goals to realize and maximize their potential.

Since the six ISRA methodologies and actual environment support the fact that staffs should attend self-development programs as an ongoing improvement in risk management, enforcement should exist in every organization for the staffs to participate in the following programs as shown in the list below:

- seminars;
- conferences;
- training sessions;
- workshops; and
- certification courses.

5.4.3 Reassessment schedule. Information security practitioners conduct ISRA to get a baseline picture that can be used to develop a prioritized list of cost-effective measures that should be applied to each of data assets with the intention of reduce risk to an acceptable level. However, according to Bernard (2007), to maintain the efficiency and effectiveness of risk assessment, an ongoing update of risk management program to identify the changes in the security requirements and in the risk solutions are required. In addition, the comparative studies which were done on six ISRA methodologies also emphasized on the importance of having reassessment schedule for an ongoing update of information security requirements. Therefore, question was asked to identify the types of assessment that practitioners should conduct to assess the efficiency and effectiveness of information security. The question was adopted fully from fighting to close the gap: Ernst and Young's (2012) Global Information Security Survey (Kessel, 2012).

Table XVII. Self-development program

How many seminars, conferences, training sessions, and workshop and certification courses relating to information security systems have you attended in the last year?	
Seminar	88
Conferences	43
Training sessions	98
Workshops	85
Certification courses	34

As Table XVIII indicates, a majority of organizations perform internal audit (80.0 per cent) to assess the efficiency or effectiveness of information security. Slightly fewer (73.75 per cent) use the monitoring and evaluation of security incidents and events to assess the efficiency of information security. These were followed by the organizations that used the IT function or information security itself to conduct internal self-assessments (66.25 per cent) and assessment by external party (63.75 per cent). Because the proliferation of threats and the widening gap between vulnerability and security requires multiple sources of assessments, ideally organizations should use the all four of the top ways identified shown in Table XVIII: assessment performed by internal audit; monitoring and evaluation of security incidents and events; internal self-assessments and third-party assessments. Information security practitioners should prepare reassessment schedule for all the four top agreed ways.

5.4.4 Awareness program checklist. Organizations deploy technology to protect their information and technology resources. However, organizations also depend on their employees who use the information and technology resources to safeguard those resources. Hence, organizations introduce information security policy for employees as a statement of the roles and responsibilities to be observed. According to Cavusoglu *et al.* (2004), employees' information security awareness is an important part of an effective information security management program. Information security awareness is defined as an employee's general knowledge about information security and his cognizance of the information security policy of his organization (Bulgurcu *et al.*, 2010; Cavusoglu *et al.*, 2004). Because information security awareness is viewed as knowing something about information security and each organization has its own way to carry out the awareness program, questions were asked to determine whether the organizations have taken steps to disseminate the knowledge of information security to employees. The survey results shows in Table XIX.

In response, it was indicated that more than half of the respondents agreed with the security awareness program checklist. Fewer (1.25 per cent) disagreed with the checklists. It shows that the respondents also conduct information security awareness to educate their employees with security knowledge. This checklist shown below can becomes the guidelines for security practitioners to develop more awareness programs according to their needs:

Table XVIII. Methods used by organization to assess the efficiency and effectiveness of information security

How does your organization assess the efficiency and effectiveness of information security?	(%)
Assessment performed by internal audit function	80.00
Monitoring and evaluation on security incident and events	73.75
Internal self-assessment by IT or information security function	66.25
Assessment by external party	63.75
Evaluation of information security operational performance	47.50
Evaluation of information security costs	15.00
Benchmarking against peers/competition	10.00
No assessment performed	–

In your organization, how is the awareness program carried out?	Strongly agree (%)	Agree (%)	Neutral (%)	Disagree (%)	Strongly disagree (%)
Continuous, ongoing security awareness program exists	30.00	53.75	16.25	–	–
The IT staffs have been sufficiently trained and informed about information security policies	30.00	53.75	15.00	1.25	1.00
Information security awareness is communicated well	28.75	62.50	7.50	1.25	2.00
A variety of business communications (notices, posters, newsletters, ext.) are used to promote security awareness	22.50	51.25	26.25	1.25	3.00
Users receive adequate security refresher training appropriate for their job function	21.25	57.20	20.00	1.25	4.00

Table XIX. Organization awareness program checklist

- a continuous, ongoing security awareness program exists;
- the IT staff have been sufficiently trained and informed about information security policies;
- information security awareness is communicated well;
- a variety of business communications (notices, posters, newsletters, etc.) are used to promote security awareness; and
- users receive adequate security refresher training appropriate for their job function.

6. Collective structural information model

At present, numerous ISRA methodologies currently available and organizations also are still skeptical in choosing the appropriate ISRA methods for them. As such, organizations have to meticulously define their own security assessment steps. As mentioned in the previous part, literature and comparative studies were carried out on six types of ISRA methodologies. These studies reveal that all the six types of ISRA methodologies have features of the same kind of information with a slight difference in form. It was also found that all the methodologies contained mutual features in the structure.

However, to get the ISRA model more practical in the real environment of the workplace, questionnaires were designed to insert additional features to the research framework. All the additional features chosen were based on high frequency of "more than half percentage agreed" responses from respondents. The following model shown in Figure 3 is a final analysis results inspire in generating a collective information structure model. The model was divided into three features, namely:

(1) management requirement;

(2) establishment of organizational context and identification of assets, threats and vulnerabilities; and

(3) risk management improvements.

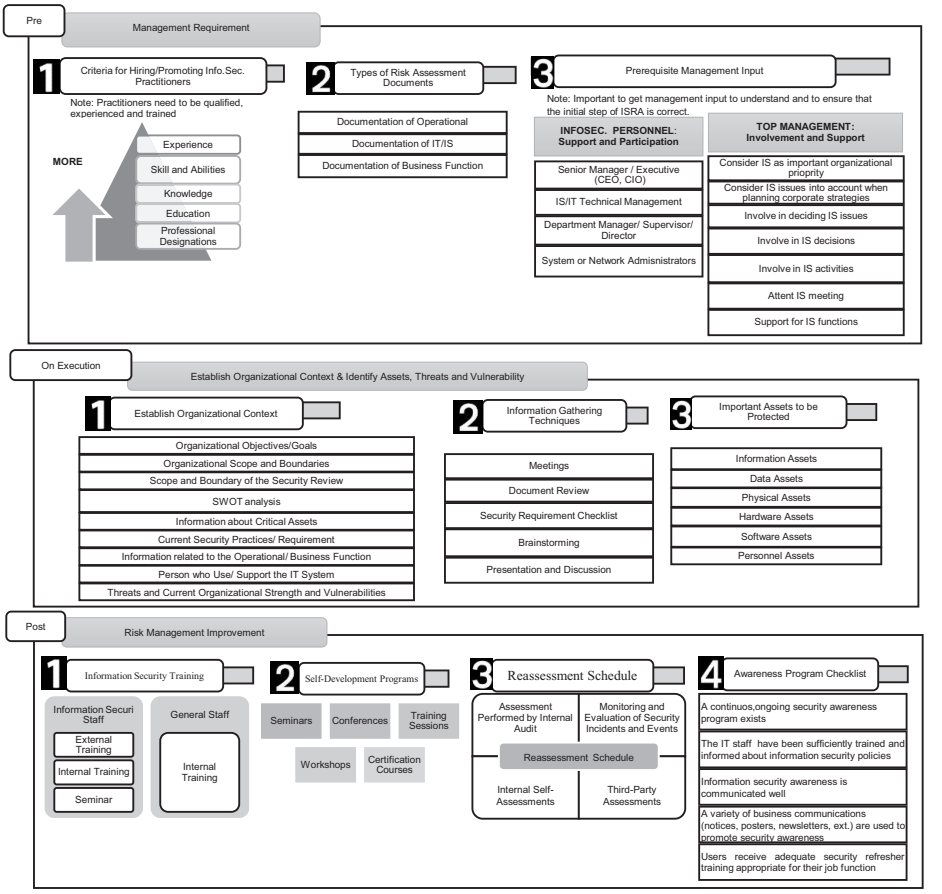

Figure 3.
Collective information structure model for information security risk assessment

The management requirement feature states that practitioners who are involved in ISRA must have the skill, qualification, experience and training. This is because only practitioners who have these characteristics would be able to collect and analyze information accurately and make plausible decisions during the evaluation. Before proceeding with the ISRA, however, it is important to get management input to understand and to ensure that the initial step of ISRA is correct. Moreover, the risk assessment document from business and IS/IT departments also need to be reviewed and revised in order to draw and plan the ISRA process perfectly.

Establishing organizational context implies the acquisition of all relevant information about the organization's industry, structure, operation, property, current security status, its overarching strategy, overall goals and long-term strategy. In addition, it also allows the organization to determine the basic criteria, purpose, scope and the boundary of business environment to ensure that the risk assessment process garners optimal results and to assure that any risk in the organization's industry is identified for rectification. While during the assets, threats and vulnerability

identification, practitioners will select an organization's most critical information assets as well as the identification of the threats and vulnerabilities of each of these assets.

Risk management improvements are facilitated by training, meeting, workshops, updating of risk, risk monitoring and also reassessment schedule. ISRA is considered as a continuous process which needs monitoring and continuous awareness the staff. Risk management improvement will guide practitioners for ongoing process to achieve:

- developing staffs' skills by providing training;
- motivating staffs with self-development programs;
- scheduling and monitoring reassessments; and
- conducting awareness program.

7. Discussion and conclusion

At present, numerous methodologies are available and organizations need further research due to the lack of trustable and standardized ISRA methods to enable organizations to select a suitable method to conduct the risk assessment. Generally, all organizations need to study the methodologies in detail before a suitable methodology is chosen. However, with the proposed model, the process of conducting ISRA will be more systematic and convincing if the organizations knew before-hand what information they needed before the commencement of the plan. As the information security department is responsible for doing the risk assessment, it needs to complete all the required planning before starting the actual risk assessment.

The success of the risk assessment fully depends on the information gathered to make concise and accurate security planning decisions. This study highlighted the achievement of developing the collective information structure model in ISRA to guide the ISRA practitioners with the general view of flow, types of information to be gathered and the requirements to be met before risk assessment is conducted. ISRA practitioners do planning by deciding in advance what to do, how to do it, when to do it and who to do it, which lead to achieve clear direction to reach risk management goals and objectives.

In conclusion, this research has provided an invaluable input to information security risk assessment world. Gathering complete information would encourage in making a plan that leads to a clear direction, and ultimately help to make decisions that lead to success. Practitioners need to be clear with overview of information security risk assessment and the flow of information to be collected. Generally, practitioners are required to refer to a different types of ISRA standard or methodology, according to their needs. It will complicate the process of information gathering and planning as their understanding of the standards and the methodology is different. However, with the collective information structure of the ISRA model which was generated based on the mutual features in six ISRA methodologies and agreed by ISRA practitioners in Malaysia, definitely this will be an efficient and effective guide in the process of gathering and planning. In addition, this remarkable model is believed to build sufficient and complete information and guiding ISRA practitioners getting to know exactly what the outcome of their decision will be and provide trustable and applicable guidelines to practitioners.

The model is applicable for all types of organizations which conducting information security risk assessment. Although the choice of the quantitative survey method in this

research was adequate for obtaining data to answer the research objective, future research may adopt a different method to unravel certain phenomena related to information security risk assessment methodology. Future studies may use a qualitative research design involving case study or observation as well as conducting case study by approaching ISRA practices in organization to adopt and implement the model. Other possible methods to be used could be an integrative triangulation approach, combining both quantitative and qualitative design involving in-depth interviews with top-level managers using this model.

7.1 Limitations of the study

This study has limitations. First, this study only questioned security professionals who had registered under SIRIM QAS and CyberSecurity. Jourdan *et al.* (2010) described a research regarding an organization's information security practices as very intrusive. This research study also faced similar obstacles, but these non-response issues were fixed by targeting information security professionals who have opted to receive questionnaires from researchers. In fact, in Malaysia, there are many information security certification bodies apart from SIRIM and CyberSecurity. Only SIRIM and Cybersecurity agreed to give the lists of organizations that have obtained certification of information security. In the meantime, other agencies preferred not to share the list of organizations registered under them due to confidentiality. Fortunately, most of the respondents under SIRIM and Cybersecurity responded to the questionnaire and provide support to complete this study. Using this strategy, this research project managed to achieve a favorable response rate.

References

Aagedal, J.Ø., Braber, F. Den, Dimitrakos, T., Gran, B.A., Raptis, D. and Stølen, K. (2002), "Model-based risk assessment to improve enterprise security", *Proceedings of the Fifth International IEEE Conference on Distributed Object Computing (EDOC 2002)*, *Lausanne*, pp. 51-62.

Albert, C. and Dorofee, A.J. (2001), *OCTAVE Criteria Version 2.0*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Alberts, C.J. and Dorofee, A.J. (2002), *Managing Information Security Risks: The Octave Approach*, Addison Wesley Longman Publishing Co., Boston, MA, pp. 1-512.

Alberts, C.J., Dorofee, A.J. and Allen, J.H. (2001), *OCTAVE Catalog of Practices Version 2.0*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), *Introduction to the OCTAVE® Approach – Networked Systems Survivability Program*, Software Engineering Institute, Carnegie Mellon University, pp. 1-27.

Alnatheer, M. and Nelson, K. (2009), "Proposed Framework for understanding information security culture and practices in the Saudi context", *Australian Information Security Management Conference*, Perth, pp. 6-17.

Ayoub, R.C. (2011), *The 2011 (ISC) Global Information Security Workforce Study*, Frost & Sullivan Market Survey, California, pp. 2-27.

Baskerville, R. (1991), "Risk analysis as a source of professional knowledge", *Computers & Security*, Vol. 10 No. 8, pp. 749-764.

Bernard, R. (2007), "Information lifecycle security risk assessment: a tool for closing security gaps", *Computers & Security*, Vol. 26 No. 1, pp. 26-30.

Bornman, W.G. and Labuschagne, L. (2004), "A comparative framework for evaluating information security risk management methods", *Information Security South Africa Conference*, South Africa.

Braber, F. Den Hogganvik, I., Lund, M.S., Stølen, K. and Vraalsen, F. (2007), "Model-based security analysis in seven steps – a guided tour to the CORAS method", *BT Technology Journal*, Vol. 25 No. 1, pp. 101-117.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *Information Security Policy Compliance*, Vol. 34 No. 3, pp. 523-548.

Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2004), "Economics of IT security management: four improvements to current security practices", *Communications of the Association for Information Systems*, Vol. 14 No. 1, pp. 65-75.

CICC (2009), "Result of the attitude survey on information security", available at: www.cicc.or.jp/japanese/kouenkai/pdf_ppt/afit/11Mr_Ikeda.pdf (accessed 29 March 2015).

Culp, S. (2011), *Report on the Accenture 2011 Global Risk Management Study: Risk Management as a Source of Competitive Advantage and High Performance*, Technical Report, Accenture.

Dahl, H.E.I. (2008), "The CORAS method for security risk analysis", *Tutorial Presentation at 7th Estonian Summer School on Computer and Systems Science in cooperation with the Nordic Network on Dependable Systems (NODES)*, Otepää, Estonia.

Dzazali, S. and Zolait, A.H. (2012), "Assessment of information security maturity", *Journal of Systems and Information Technology*, Vol. 14 No. 1, pp. 23-57.

Dzazali, S., Sulaiman, A. and Zolait, A.H. (2009), "Information security landscape and maturity level: case study of Malaysian Public Service (MPS) organizations", *Government Information Quarterly*, Vol. 26 No. 4, pp. 584-593.

Elky, S. (2006), "An introduction to information system risk management", SANS Institute, pp.1-13, available at: www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

Eloff, J.H.P. and Eloff, M.M. (2005), "Information security architecture", *Computer Fraud & Security*, Vol. 2005 No. 11, pp. 10-16.

Evalueserve (2012), *State of Security Survey*, Technical Report, Evalueserve, pp. 1-19.

Filho, E.L., Hashimoto, G.T., Pedro, F., Souza, J.H.P. De and Paulo, S. (2011), "The impact of corporate culture in security policies – a methodology", The Seventh International Conference on Networking and Service (ICNS 2011), Venice,, pp. 98-103.

Fredriksen, R., Kristiansen, M., Gran, B.A., Stølen, K., Opperud, T.A. and Dimitrakos, T. (2002), "The CORAS framework for a model-based risk management process", *Computer Safety, Reliability and Security*, Springer Berlin Heidelberg, pp. 94-105.

HIMSS (2011), *HIMSS Security Survey Final Report*, Healthcare Information and Management Systems Society, USA, pp. 1-20.

Jalil, S.A. and Hamid, R.A. (2003), *ISMS Pilot Program Experiences: Benefits, Challenges & Recommendations*, CyberSecurity, Malaysia.

Jourdan, Z., Rainer, R.K., Marshall, T.E. and Ford, F.N. (2010), "An investigation of organizational information security risk analysis", *Journal of Service Science*, Vol. 3 No. 2, pp. 33-42.

Kaplan-Mor, N., Glezer, C. and Zviran, M. (2011), "A comparative analysis of end-user training methods", *Journal of Systems and Information Technology*, Vol. 13 No. 1, pp. 25-42.

Karabacak, B. and Sogukpinar, I. (2005), "ISRAM: information security risk analysis method", *Computers & Security*, Vol. 24 No. 2, pp. 147-159.

Kessel, P.V. (2012), *Fighting to Close the Gap: Ernst & Young's 2012 Global Information Security Survey*, Ernst & Young Global Limited, UK, pp. 1-48.

Lichtenstein, S. (1996), "Factors in the selection of a risk assessment method", *Information Management & Computer Security*, Vol. 4 No. 4, pp. 20-25.

Lund, M.S., Solhaug, B. and Stølen, K. (2011), "Model-driven risk analysis", *Model-Driven Risk Analysis, The CORAS Approach*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 23-43.

McDonnel, C., Carstensen, J. and Ward, J. (2012), *Irish Information Security and Cybercrime Survey A Closer Look*, Deloitte Touche Tohmatsu Limited, Ireland, pp. 1-11.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G. and Skourlas, C. (2014), "Human factor and information security in higher education Efthymia", *Journal of Systems and Information Technology*, Vol. 16 No. 3, pp. 210-221.

Ministry Education (2012), *Industry Training Review: Results of the Employer Interviews & Survey*, Ministry of Education, New Zealand.

Mustafa, T. (2012), *Information Security Standards Development in Malaysia*, Technical Report, Technical Committee on Information Security, USA.

NIST (2010), *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST, USA, pp. 1-93.

NIST (2011a), *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST, USA.

NIST (2011b), *Guide for Conducting Risk Assessments: Information Security*, NIST, USA.

Perron, R. (2011), *Employer Experiences and Expectations: Findings, Training, and Keeping Qualified Workers*, American Association of Retired Persons, Washington, DC, pp. 1-51.

Raymond, K. (1993), "Reference model of open distributed processing (RM-ODP): introduction", *Open Distributed Processing*, Springer, USA, pp. 3-14.

Refsdal, A. (2011a), *The CORAS Approach To Model- Driven Risk Analysis*, SINTEF, Scandinavia.

Refsdal, A. (2011b), "Analysing risk in practice: the CORAS approach to model-driven risk analysis", *18th ACM Conference on Computer and Communications Security (CCS 2011)*, Chicago, IL.

Richards, K. (2009), *The Australian Business Assessment of Computer User Security: A National Survey, Research and Public Policy Series*, No 102, Australian Institute of Criminology, Canberra, pp. 1-102.

Richardson, R. (2011), *2010/2011 CSI Computer Crime and Security Survey*, Computer Security Institute (CSI), New York, NY, pp. 1-42.

Rubio, F. (2004), *El Paso Community College Information Security Risk Assessment Survey*, El Paso Community College, US, pp. 1-23.

Saleh, M.S. and Alfantookh, A. (2011), "A new comprehensive framework for enterprise information security risk management", *Applied Computing and Informatics, King Saud University*, Vol. 9 No. 2, pp. 107-118.

Sarkheyli, A. and Ithnin, N.B. (2010), "Improving the current risk analysis techniques by study of their process and using the human body's immune system", *5th International Symposium IEEE on Telecommunications*, Tehran, pp. 651-656.

Schlich, B. and Jackson, P. (2008), *Progress in Financial Services Risk Management: A Survey of Major Financial Institutions*, Ernst & Young Global Limited, UK, pp. 1-63.

Shamala, P., Ahmad, R. and Yusoff, M. (2013), "A conceptual framework of info structure for information security risk assessment (ISRA)", *Journal of Information Security and Applications, Elsevier Ltd*, Vol. 18 No. 1, pp. 45-52.

Shedden, P., Scheepers, R., Smith, W. and Ahmad, A. (2011), "Incorporating a knowledge perspective into security risk assessments", *Journal of Information and Knowledge Management Systems*, Vol. 41 No. 2, pp. 152-166.

Shedden, P., Smith, W. and Ahmad, A. (2010), "Information security risk assessment: towards a business practice perspective", *Australian Information Security Management Conference*, Perth, pp. 119-130.

Shedden, P., Smith, W., Scheepers, R. and Ahmad, A. (2009), "Towards a knowledge perspective in information security risk assessments – an illustrative case study", *Australasian Conference on Information Systems*, Melbourne, pp. 74-84.

Siemens (2005), *Managing CRAMM Reviews Using PRINCE*, Siemens Enterprise, United Kingdom.

Söderström, E., Åhlfeldt, R. and Eriksson, N. (2009), "Standards for information security and processes in healthcare", in Stockdale, R. (Ed.), *Journal of Systems and Information Technology*, Vol. 11 No. 3, pp. 295-308.

Spears, J.L. (2006), "A holistic risk analysis method for identifying information security risks", *Security Management, Integrity, and Internal Control in Information Systems*, Springer, New York, Vol. 193, pp. 185-202.

StandardsMalaysia (2009), *Guide to the Malaysian Standards Sysyem*, StandardsMalaysia, Malaysia, pp. 1-81.

Stephen, F., Douglas and Charlton, G. (2011), *Information Security and Confidentiality Survey Results*, CNA, San Diego, pp. 1-11.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology Special (NIST).

Suh, B. and Han, I. (2003), "The IS risk analysis based on a business model", *Information & Management*, Vol. 41 No. 2, pp. 149-158.

Syalim, A., Hori, Y. and Sakurai, K. (2009), "Comparison of risk analysis methods: Mehari, Magerit, NIST800-30 and Microsoft's security management guide", *International Conference on Availability, Reliability and Security*, *IEEE Computer Society, Fukuoka*, pp. 726-731.

Visintine, V. (2003), *An Introduction to Information Risk Assessment*, GSEC Practical, SANS Institute.

Vorster, A. and Labuschagne, L.E.S. (2005), "A framework for comparing different information security risk analysis methodologies", *Proceedings of Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT research in Developing Countries (SAICSIT 2005), South African Institute for Computer Scientists and Information Technologists, South Africa*, pp. 95-103.

Yazar, Z. (2002), *A Qualitative Risk Analysis and Management Tool-CRAMM*, GSEC Practical, SANS Institute.

Zakaria, M.Z. (2008), *Information Security Standards Activities in Malaysia*, Technical Report, Technical Committee on Information Security, Malaysia, pp. 1-16.

Corresponding author
Ali Hussein Zolait can be contacted at: alizolait@gmail.com