A conceptual framework of info-structure for information security risk assessment (ISRA)

Palaniappan Shamala a,b,*, Rabiah Ahmad a, Mariana Yusoff c

a Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
b Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia
c Centre for Languages and Human Development, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Abstract

Information security has become a vital entity to most organizations today due to current trends in information transfer through a borderless and vulnerable world. The concern and interest in information security is mainly due to the fact that information security risk assessment (ISRA) is a vital method to not only to identify and prioritize information assets but also to identify and monitor the specific threats that an organization induces; especially the chances of these threats occurring and their impact on the respective businesses. However, organizations wanting to conduct risk assessment may face problems in selecting suitable methods that would augur well in meeting their needs. This is due to the existence of numerous methodologies that are readily available. However, there is a lack in agreed reference benchmarking as well as in the comparative framework for evaluating these ISRA methods to access the information security risk. Generally, organizations will choose the most appropriate ISRA method by carrying out a comparative study between the available methodologies in detail before a suitable method is selected to conduct the risk assessment. This paper suggests a conceptual framework of info-structure for ISRA that was developed by comparing and analysing six methodologies which are currently available. The info-structure for ISRA aims to assist organizations in getting a general view of ISRA flow, gathering information on the requirements to be met before risk assessment can be conducted successfully. This info-structure can be conveniently used by organizations to complete all the required planning as well as the selection of suitable methods to complete the ISRA.

1. Introduction

In the current information age, the issue of information security has become a vital entity because organizations across the globe conduct business in an interconnected and information rich environment. Information security risk assessment (ISRA) enables the government, private and public organizations to identify their security risks and provide a measured, analysed security profile of critical information assets in order to develop effective and economically-viable control strategies (Shedden et al., 2011, 2010; Baskerville, 1991; Braber et al., 2007). Risk assessment, both the process

* Corresponding author. Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia.
E-mail addresses: sivashalamapalaniappan@gmail.com, shamala@uthm.edu.my (P. Shamala), rabiah@utem.edu.my (R. Ahmad), mariana@utem.edu.my (M. Yusoff).
2214-2126/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jisa.2013.07.002
and associated techniques, offers an analytical and structured walk-through of the organization’s security state. In addition, it outlines risk scenarios, identifies the consequences, should these occur, the frequency or likelihood of them occurring, the possible treatment options, and the associated costs (Khanmohammadi and Hounb, 2010). However, the main problem in risk assessment is how to assess all risks so that by using the output of the risk assessment, these organizations could define appropriate controls for reducing or eliminating those risks (Syalim et al., 2009).

Nowadays, there are a number of different types of risk assessment methods, standards, guidelines and specifications that are available; some of which are qualitative while others are more quantitative in nature (Saleh and Alfantookh, 2011; Eloff, 2003). Each of these methods has been developed to meet a particular need and hence has different objectives, steps, structure and level of application. However, in general information risk assessment there are three distinct phases namely: context establishment, risk identification and risk analysis (Shedden et al., 2010; Shedden et al., 2009). The common goals to achieve from these three phases are to create risk treatment plans and justify the costs of control selection, development, installation and maintenance to management.

Due to the availability of numerous ISRA methods currently, many organizations are faced with the daunting task 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, there are no constructs available to assist organizations in determining the most appropriate ISRA method to use (Bornman and Labuschagne, 2004). In addition, there is no standardized and trustable ISRA methods currently in existence (Syalim et al., 2009; Spears, 2006; Eloff and Eloff, 2005). There is also no agreed reference benchmark or comparative framework for evaluating these ISRA methods to assess the information security risk (Syalim et al., 2009; Saleh and Alfantookh, 2011; Vorster and Labuschagne, 2005).

In addition, current studies highlight that in order to protect information assets, organizations need to make comparisons between methodologies and decide on the best (Saleh and Alfantookh, 2011; Vorster and Labuschagne, 2005). This tedious process leads to unwarranted time, money and energy consumption. Another ensuing issue here would be the complexities of using formal methodologies that require a high level of expertise. In addition, formal methods do not guarantee the obtaining of the list of all the security risk threatening and control measures.

Although there is a wide range of literature on existing ISRA methodologies, there is a need for further research in this area to explore and develop a common info-structure framework in ISRA to meet the demands in this area. Info-structure is the layout of information which is organized in a useful fashion and can be navigated at any time. Therefore, this study employs a newly developed ISRA info-structure conceptual framework which anchors on identifying the similarities in info-structure among the existing ISRA methodologies.

The proposed ISRA info-structure can aid organizations to establish accurate security planning decisions and enable them to successfully draft correct and consistent planning for the ISRA process. The info-structure for ISRA explains the general view of flow, types of information to be gathered and the requirements to be meet before any risk assessment is conducted. ISRA practitioners can collect all the needed information and fulfil the requirements based on the ISRA info-structure before starting with their actual ISRA implementation.

This paper is organized as follows. The next section describes the background of the risk assessment and explains six different ISRA methodologies selected for the comparison. Section 3 explains research approaches used in this research. Section 4 presents the new conceptual framework of ISRA info structure, followed by the conclusion in Section 5.

2. Literature review

2.1. Background of risk assessment

Information security is of paramount importance to organizations. Literature defines information security as a set of processes, procedures, personnel, and technology charged with protecting an organization’s information assets (Jourdan et al., 2010). It also can be defined 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 necessity of information security in organizations has increased because of the enormous changes in structure and type of information technologies applied to information creates risks. Risks to assets are identified in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. The criticality of each risk is rated according to potential impact and likelihood of occurrence.

Organizations wanting to eliminate the possible risks in their organizations by conducting information security risk assessment (ISRA). ISRA able to determine the extent of the potential threat and the risk associated with an IT system (Syalim et al., 2009).

An ISRA method identifies an organization’s security risks and provides a measured, analysed security risk profile of critical assets in order to build plans to treat the risks (Shedden et al., 2011; Shedden et al., 2010; Shedden et al., 2009; Lichtenstein, 1996).

Nowadays, there are a number of different types of risk assessment process, frameworks and methodologies in information security literature (Saleh and Alfantookh, 2011). Table 1 illustrates the list of ISRA methodologies issued by organizations. All the ISRA methodologies have been developed along with supporting tools and documentation that tailor security control implementations to organizations (Braber et al., 2007; Alberts et al., 2003; Stolen et al., 2002; Yazar, 2002).

Although these ISRA methodologies differ in their make-up, order and depth of activities, they generally follow a three phases: context establishment, risk identification, and risk analysis (Shedden et al., 2011; Shedden et al., 2010; Shedden et al., 2009).
The context establishment phase 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 (Shedden et al., 2011; Shedden et al., 2009). 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.

Risk identification is basically a systematic procedure undertaken to discover and select an organization’s most critical information assets as well as the identification of the threats and vulnerabilities of each of these assets.

While risk analysis is the determination of probability: chance of the threat event occurring and its impact: the cost of compromising the asset (Shedden et al., 2011). Once the identification and analysis is done, the organization will then assign value to each threat that they have identified and subsequently determine the probability of that threat occurring and also the impact that threat it would have on that information asset. The integration of probability and impact will represent the level of risk. This analysis of impact and probability can be done through qualitative, quantitative or via a combination of both methods.

Therefore, the ISRA is able to list out a set of threats, of vulnerabilities, a list of the level of risk and a list of control measures. However, there are no fixed standards as to how to develop these lists.

### 2.2 Information security risk management methodologies

Although there is a wide range of literature on currently available ISRA methodologies, the area needs further research due to the lack of trustable and standardized ISRA methods to enable organizations to select a suitable method. Currently available methods do not define detailed steps of risk assessment. As such, organizations have to meticulously define their own security assessment steps. A general practice for any organization is to study the methodologies in detail before a suitable methodology is chosen to conduct the risk assessment. The process of conducting ISRA will be more systematic and convincing if organizations have established a systematic ISRA plan to follow. Basically, properly defined detailed steps of risk assessment planning can assist the risk assessment team to conduct risk assessment in a more systematic and effective manner.

Risk assessment is a fundamental decision making process in the development of information security and it is a two-stage process (Lichtenstein, 1996). At the first stage, risk assessment teams have to define the scope of the risk assessment, identify information assets and determine and prioritize risks to the assets. In the second stage i.e. the risk management process stage, the assessment team makes decisions on controlling the identified risks. Apart from these two stage, risk assessments also looks at other roles such as involvement of management in information security decision making and enabling definition and refinement of security policy. Thus, it can be said that the risk assessment process involves a series of tasks broken down by phases where each phase requires information for its success. ISRA info-structure is important to serve as a basic guide to the ISRA practitioners to identify and gather information and define the steps needed in every phase of the risk assessment.

In a nutshell, concerned organizations undertake various types of preferred methodologies, depending on their needs, for comparison when embarking on ISRA in their organizations. Among them are as follows:

- **a. Professional organization:**
  - i. CRAMM (Bornman and Labuschagne, 2004; Yazar, 2002; Sarkheyli and Ithnin, 2010; Enterprise, 2005)
  - ii. CORAS (Braber et al., 2007; Vorster and Labuschagne, 2005; Bornman and Labuschagne, 2004; Aagedal et al., 2002; Fredriksen et al., 2002; Raymond, 1993; Lund et al., 2011; Dahl, 2008; Refsdal, 2011a,b)
  - iii. OCTAVE (Vorster and Labuschagne, 2005; Bornman and Labuschagne, 2004; Alberts et al., 2003; Sarkheyli and Ithnin, 2010; Albert and Dorofee, 2001; Alberts et al., 2001; Elky, 2006; Visintine, 2003)
- **b. Research project:**
  - i. ISRAM (Vorster and Labuschagne, 2005; Karabacak and Sogukpinar, 2005)
  - ii. Is risk analysis based on business model (Vorster and Labuschagne, 2005; Suh and Han, 2003)
- **c. International organization:**
  - i. NIST 800-30 (Syalim et al., 2009; J. T. F. NIST, 2011a; Stoneburner et al., 2002; J. T. F. NIST, 2011b; J. T. F. NIST, 2010)

The reason for the selection of various types of methods for comparison is because they have been well documented. The majority of ISRA methods are proprietary with very little publicly available information apart from marketing literature. Often organizations do not have the available capital to purchase different ISRA methods in order to evaluate them. Therefore, the evaluation process was often based on documentation obtained through printed material, presentation software, demonstration server platforms or internet published material.

This info structures for the ISRA were determined by doing a comparative analysis on the different types of ISRA

### Table 1 – List of risk management methodologies issued by organizations.

<table>
<thead>
<tr>
<th>Issue by</th>
<th>Example</th>
</tr>
</thead>
</table>

...
methodologies. For this reason a brief overview of each method is given in Table 2 below.

3. Research approach

This study developed based on the research approach presented in Fig. 1 in order to identify the similarities in infrastructure among the existing ISRA methodologies that might influence the successful planning and implementation of ISRA in organizations. Altogether six types of methodologies have been used.

<table>
<thead>
<tr>
<th>Features</th>
<th>Developed by</th>
<th>Used by</th>
<th>Risk assessment approach</th>
<th>Risk model/Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management methodologies</td>
<td>Central Computer and Telecommunication Agency (CCTA)</td>
<td>Anyone</td>
<td>Qualitative</td>
<td>1. Identification and valuation of assets 2. Threat and vulnerability assessment 3. Countermeasure selection and recommendation</td>
</tr>
<tr>
<td>OCTAVE</td>
<td>National Research Institute of Electronics and Cryptology 2. Gebze Institute of Technology in Turkey</td>
<td>Anyone</td>
<td>Quantitative</td>
<td>1. Survey-based model: Two separate and independent surveys are conducted for the two attributes of risk namely probability and consequence. 2. Consists of 7 main steps: a. First four steps: survey preparation b. Fifth step: conduction of survey c. Last two steps: Results are obtained and assessed.</td>
</tr>
<tr>
<td>Research project ISRAM</td>
<td>Korea Advances Institute of Science and Technology</td>
<td>Anyone</td>
<td>Quantitative</td>
<td>Stage 1: the organizational investigation Stage 2: asset identification and evaluation Stage 3: threat and vulnerability assessment Stage 4: annual loss expectancy calculation</td>
</tr>
<tr>
<td>International organization NIST 800-30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
organizational context, identification of assets, threats and vulnerabilities, and risk management improvements. Each of the main features is divided further into sub features. Comparison processes were carried out twice. The final phase was to classify these filtered features into the conceptual framework of ISRA info structure.

4. Conceptual framework of info-structure ISRA

At the present time numerous methodologies are available and organizations are faced with the daunting task of choosing the appropriate methodology for use. Each of these methods requires complete and adequate information to start ISRA activities. Small or multi-national organizations require planning before risk assessment is conducted. Thus, it would be helpful if the organization knew beforehand what information they needed before commencement of the plan. Based on the analysis, it can be concluded that all the methods chosen for this comparison required the 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.

As mentioned in the previous part, two types of comparative studies have been conducted to create the info-structure for ISRA. In the first step of doing the comparative study, it was identified that all the methodologies had common mutual features. Hence, all the common mutual features in the six methodologies were listed out. Based on the features, information was extracted and included in the respective methodologies. The filled information can either be similar or different from each other.

Based on the first comparative analyses, it can be concluded that each of these methodologies had been developed to meet a specific need thus had a different risk model/phase, steps and structure, tiers involvement, involvement of people in management, objectives, ways of information gathering techniques and level of application. Saleh & Alfantookh (Saleh and Alfantookh, 2011) concur in opinion. However, the main goal of all the ISRA is to reduce, mitigate, transfer or accept risks to an acceptable level by prioritizing and estimating the risk value (Saleh and Alfantookh, 2011; Straub and Welke, 1998). Hence, it can be concluded that any organization, regardless of their size, they have to ensure that the details for the activity listed below are gathered accurately:

a. Management requirement  
b. Establish organizational context  
c. Identify assets threats and vulnerabilities  
d. Risk management improvement

As the information security department is responsible for doing risk assessments, it needs to plan ahead before starting with the actual risk assessment. Basically, the success of the information security risk management is fully dependent on the information gathered in order to make concise and accurate security planning decisions. The above list is the list of activities in ISRA where prior information needs to be sought before proceeding with the three phases of ISRA known as context establishment, risk identification and risk analysis.

The second step of the comparative study carried out was to specify the sub-features for each main feature. In the second step of the comparative study, every individual element of the sub features duly cross-checked and marked against all the six methodologies in the table. The features chosen were based on the highest frequency of “most often agreed” responses collected from the comparative table found in Appendix A.

All of the six risk management methodologies concur 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.

Below are the sub-activities that should be considered by ISRA practitioners for management requirement.
Practitioners need to be qualified, experienced and trained
Needs of business, operation and IT/IS risk assessment document
Management input

Among the sub-activities that most risk management methodologies adopted for organizational context are listed below.

- Objectives/goals
- Scope and boundary of the security review
- SWOT analysis
- Information about critical assets
- Current security practices/requirement

Each organization has to identify the risks to their most important assets and build a strategy for protecting its critical assets. Normally ISRA practitioner will examine which assets are most important to the organization in the early process of doing risk assessment. Based on the existing risk management methodologies, the assets that will be considered first as important assets for an organization are listed as below. In practical ISRA, practitioner will usually be targeting these assets as 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 security requirements of an organization.

- Information asset
- Data assets
- Physical assets
- Software assets
- Hardware assets
- Personnel assets

ISRA practitioners have to consider the relationships between critical assets, the threats to those assets, and vulnerabilities that can expose assets to threats. Fundamentally, ISRA practitioners will describe security requirements for the critical assets and identify threats to the critical assets based on the identified critical assets. Based on the Suh and Han (Suh and Han, 2003) standpoint, the boundary of risk analysis should be established during the asset identification to find out the protection priority of each asset. Perhaps all organizations will have a similar list of critical assets, but the threat to the asset will vary according to the scope of information security of the organization.

ISRA methodologies emphasise that a majority of the risk management methodologies do not provide for risk management projects that 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. Based on the two comparisons, it can be concluded that, ISRA management should consider the following sub activities as a list for risk management improvement.

- Training
- Meeting
- Workshops
- Reassessment schedule
- Awareness

Fig. 2 – Conceptual framework of Info-Structure for ISRA.
The following model shown in Fig. 2 is a result of careful merging of salient items from both the main and sub activities listed above.

5. Discussion and conclusion

In today’s security environment it has almost become unfeasible to offer complete protection to information systems in organizations. In addition, since there a big numbers of methodologies are currently available for use; organizations are still scepticism in choosing the appropriate ISRA methods for them. Thus, the goal of the present study is focused on the development of an info-structure for ISRA which explains the general view of flow, types of information to be gathered and requirements to be met before any risk assessment is conducted. The conceptual framework of info-structure for ISRA was developed by comparing and analyzing six methodologies in detail and identifying mutual features in the structure. The mutual features were then used to form the info-structure for ISRA.

The proposed info-structure for ISRA can be used to complete all the required planning followed by selection of suitable methodologies to complete the risk assessment successfully. To date the info-structure for ISRA has been created based on comparison studies on available methodologies and literature review. The researcher assures that further research will be conducted based on quantitative and qualitative methods to make the info-structure more complete and detailed for information security assessment in all types of organizations.

Acknowledgement

Authors would like to thank University Tun Hussien Onn Malaysia (UTHM) for supporting this research.

Appendix A. Comparison among the ISRA methodologies at Phase 5

<table>
<thead>
<tr>
<th>Elements/Features</th>
<th>ISRA methodologies</th>
<th>Professional organization</th>
<th>Research project</th>
<th>International organization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CRAMM</td>
<td>CORAS</td>
<td>OCTAVE</td>
</tr>
<tr>
<td>Management requirements</td>
<td>Practitioners need to be qualified, experienced and trained</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Needs of IT/IS risk assessment document</td>
<td>Management input</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish organizational context</td>
<td>Objectives/goals</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Scope and boundary of the security review</td>
<td>SWOT analysis</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Information about critical assets</td>
<td>Current security practices/requirement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Information related to the operational/business function</td>
<td>Schedule and deliverables</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Person who use/support the IT system</td>
<td>Identify assets threats and vulnerabilities</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ASSETS</td>
<td>Data asset</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Software asset</td>
<td>Information asset</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Physical asset</td>
<td>Personnel/people</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hardware asset</td>
<td>Various facilities assets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Risk management improvement</td>
<td>Training</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Meeting</td>
<td>Workshops</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reassessment Schedule/Updating risk</td>
<td>Risk monitoring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Awareness</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

 ✓-fulfils criteria.
 ×-Does not fulfil criteria.
 ?-Could not find in the documents whether fulfils or does not fulfil.
References


Dahl HEI. The CORAS method for security risk analysis; 2008.


J. T. F. NIST. Guide for applying the risk management framework to federal information systems. no. February, 2010.


J. T. F. NIST. Managing information security risk. no. March, 2011.


Refsdal A. The CORAS approach to model-driven risk analysis; 2011.


Straub DW, Welke RJ. Coping with systems risk security planning models for management decision making. no. 404; 1998. p. 441–69.


Visintine V. An introduction to information risk assessment. SANS Institute; 2003.
