**Indonesian Journal of Electrical Engineering and Computer Science**
Vol. 12, No. 2, November 2018, pp. 634~640
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i2.pp634-640


# Information Structure Framework for ISMS Planning and Certification: Malaysian Data

**Palaniappan Shamala[1], Muruga Chinniah[2], Cik Feresa Mohd Foozy[3], Chuah Chai Wen[4], Aida Mustapha[5], Rabiah Ahmad[6]**
[1,3,4,5]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia
[2]Faculty of Business Management, Universiti Teknologi MARA (UiTM), Segamat, Johor. Malaysia
[6]Center for Advanced Computing Technology, Faculty of Information and Communication Technology, UniversitiTeknikal Malaysia Melaka (UTeM), Melaka, Malaysia

**Article Info**

***Article history:***

Received May 13, 2018
Revised Jul 14, 2018
Accepted Jul 28, 2018

***Keywords:***

Information security management system (ISMS)
Information structure
Cerification
Malaysia Practitioners

**ABSTRACT**

Information security are becoming an important aspect of organizations. Organisations also are progressively conscious of its important in their business strategy. The awareness make organisations are currently applying for information security management system (ISMS) to effectively manage their information assets. Therefore, this research aims to provide an Information Structure Framework for ISMS planning and certification. Then Likert structured questionnaire was distributed and the findings have been analyzed using Rasch Measurement Model (RMM). The results from this study, managed to develop Information Structure Framework for ISMS. The proposed framework consists of information structure focuses on providing the information outline which is structured in a way, in which the components are put together to form a meaningful structure which can be navigated at any time. The framework contributes to the field of ISMS and certification area. The framework provides an awareness on knowing beforehand what to do and to what extent they are already conquering the information needed for getting clear direction and to develop ISMS.



***Corresponding Author:***

Palaniappan Shamala,
Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia (UTHM),
Johor, Malaysia.
Email: shamala@uthm.edu.my

## 1. INTRODUCTION

In the current information age, the issue of information security has become a vital entity. This acceptance has been due to the fact that most of the organisations have extensively replaced the physical forms of data to electronic forms of data as it has the capacity to speed up any information-based activities [1]. Hence organisations are becoming gradually aware that information security is a significant aspect of their business strategy.

Undoubtedly, these concerns created an awareness for organisations to achieve an ideal level of information security by applying Information Security Management System (ISMS) for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives [2]–[4]. ISMS can be defined as a management system used for establishing and maintaining a secure information environment [5].

Basically, ISMS will make sure that the correct people, technologies and processes are in place, and facilitates a proactive approach to manage security and risk [6]–[8]. However, the field of information security has to change from just technical issues or a technology point of view, into a completely different

point of view, where wider concern is given on management issues in which emphasis is given on procedures and processes involved for the development of secure information management system.

The existing of lacking in the research has been carry out to hightlight the need of accurately defined steps of procedures and processes in which a structured way of handling ISMS for organization is provided. It is found that all the ISMS methods only differ from each other in terms of details of the analytic process, as well as the information they prescribe [9]. Hence, it will be helpful if organisations have a comprehensive picture of ISMS which giving a holistic view on beforehand on whatever information they looked-for earlier starting of the ISMS planning.

In the current information security world, majority of organisations adopt the well-known "Plan-Do-Check-Act" (PDCA) lifecycle model to implement ISMS in their workplace. The PDCA approach emphasizes on the controls required in information security and only limited information is given regarding with the security objectives and potential strategies to be implemented on these objectives [10], [11]. Therefore, the model is unable to give information on any suggestion on how organisations must develop security strategies and objectives [10], [11]. In addition, since the main reason for developing the PDCA model was to cater to the needs of a methodical methodology when optimizing automated manufacturing processes in the 1950s. PDCA is not very suitable to describe well the most important activities in the ISMS procedures and process [12].

Even though currently there are various of ISMS methods and approaches are available, many organizations are facing the difficulty to determine the most suitable methodology according to their exact requirements [13]. On the contrary, the lacking of having one ideal ISMS method that would be appropriate for all organizations has made the condition even more awkward for end-users [14]. Furthermore, the currently available ISMS methodologies do not outline comprehensive steps of risk assessment and management.

The information structure framework for ISMS was developed by deploying a questionnaire using Likert scale questions administrated to a group of information security practitioners in Malaysia ($N$=150). The analysis was conducted using Rasch Measurement Model (RMM) analysis technique.The results from this study, managed to develop Information Structure Framework for ISMS planning and certification which consists of information structure focuses on providing layout of information which is organized in a way, in which the components are put together to form a meaningful structure which can be navigated at any time.

This paper seeks to contribute by giving holistic view for practitioners to collect all the needed information and fulfil the requirements for ISMS based on information structure before starting with their actual ISMS implementation. This study contributes to the field of information security management system, particularly in the ISMS certification by providing a process approach framework which lists all the necessary components for guiding practitioners to choose preferred ISMS methodologies or to achieve ISMS certification procedure. The proposed framework provides proper guidelines which can be used by the practitioners to perform ISMS planning development and certification.

This paper is organized into several sections. Section 2 explaining related work for this study. Section 3 explains the research method used followed by the results and discussion. Last but not least, Section 5 concludes the paper.

## 2. RESEARCH METHOD

The research objective is achieved for this study is achieved by structuring the instrument of the study, namely, likert scale questionnaire. This survey was developed and completed by following the four steps as suggested by Czaja and Blair (2005). The steps are a) questionnaire development, b) pilot test, c) survey distribution, d) data analysis and results.

### 2.1. Instrument Creation

The questionnaire consists of two sections. The survey is written in English and contains the following parts- Section 1: Information Structure for ISMS and Section 2: Demographic Profile. Questions in Section 1 are divided into three (3) subsections which are known as (a) management requirements, (b) establishment and assessment and (c) risk management improvement. The Likert scales which have been used for Section 1 is frequency scale, which are: Unimportant (0), Slightly Important (1), Moderately Important (2), Important (3).

### 2.2. Data Collection

This study used cluster sampling. The respondents for this study were collected from authorized websites of (a) SIRIM QAS, (b) CyberSecurity Malaysia. A total of one hundred and fifty (150) samples were finalized as participants in this study. The total population size in the year 2016 was 233 based on the

report of ISO survey 2016. Based on the recommended sample size, population size is 148 [15]. However, 201 questionnaires were distributed, but only 160 sets were returned, of which 150 responses were useful for analysis. This response received represents 75 percent of the proposed sample size.

### 2.3. Data Analysis Using Rasch Measurement Model (RMM)

In this phase, data analysis was conducted using Rasch Measurement Model (RMM) to determine the components of information structure which are supported and accepted through data analysis. RMM is extensively applied in education to calibrate and evaluate items in tests, questionnaires, and other instruments and to score subjects on their abilities, attitudes, or other latent traits [16].RMM states measures should be unidimensional, in order to determine if items relate to one underlying concept [17], [18]. This lets the researcher to select items for a measurement tool that reflect different levels of ability [18]. RMM will be a suitable analysis technique because it measures undimensionality and will create item hierarchies.

Therefore, by using RMM analysis, the researcher can provide indicators of how well each component fits within the underlying construct in the information structure. The RMM analysis uses Winsteps software in order to do the following test- a) model fit (dimensionality), b) item fit and c) illustrates the construct hierarchy by way of item maps.

## 3. RESULTS AND DISCUSSION

Determining the components of ISMS information structure is important to serve as a basic directive guidance to the information security practitioners to identify and gather information and define the steps needed in every phase of the ISMS. Hence, RMM is used to determine whether items which match with the theoretical concept, can be included in developing framework.The final analysis results inspire in generating an information structure for ISMS (Appendix A).

### 3.1. Reliability of Real Survey

In order to confirm the questionnaire survey is reliable to be used for big size sample, the reliability value were determined as in Table 1. Item reliability value for this survey (.99) shows that item reliability for the instrument is excellent to be used as instrument for this research. Moreover, the value of person reliability is also excellent (.95).

Table 1. Reliability of Real Study

| Questionnaire Survey | | Reliability | |
|---|---|---|---|
| | | Real | Model |
| Section 1: Information Structure | Person | 0.95 | 0.95 |
| | Item | 0.99 | 0.99 |

### 3.2. Construct Validity (Personal Component Analysis (PCA)

Personal component analysis will determine the construct validity for real survey and large sample. In order to make sure that all the items fit the unidimensional construct, PCA of residuals were run. In total 44.7% of the Rasch dimension was explained and the unexplained variance was 5.2%. The evidence for the presence of unidimensional construct is shown in Table 2.

Table 2. Personal Components Analysis (Information Structure)

Personal Components Analysis (Information Structure)

| | | -- Empirical -- | | | Modeled |
|---|---|---|---|---|---|
| Total raw variance in observations | = | 135.7 | 100.0% | | 100.0% |
| Raw variance explained by measures | = | 60.7 | 44.7% | | 44.3% |
| Raw variance explained by persons | = | 27.3 | 20.1% | | 20.0% |
| Raw variance explained by items | = | 33.4 | 24.6% | | 24.4% |
| Raw unexplained variance (total) | = | 75.0 | 55.3% | 100.0% | 55.7% |
| Unexplned variance in 1st contrast | = | 7.0 | 5.2% | 9.4% | |
| Unexplned variance in 2nd contrast | = | 5.8 | 4.3% | 7.8% | |
| Unexplned variance in 3rd contrast | = | 4.6 | 3.4% | 6.2% | |
| Unexplned variance in 4th contrast | = | 4.4 | 3.3% | 5.9% | |
| Unexplned variance in 5th contrast | = | 3.8 | 2.8% | 5.1% | |

### 3.3. Item Hierarchy on Information Structure For ISMS

The components of information structure as required by practitioners to conduct ISMS, as the components in the framework will guide the process of conducting ISMS in a more methodical manner if the practitioners identified beforehand the required information they looked-for earlier the beginning of the ISMS strategy. Results from the item map were conveyed into a logit result table as in Table 3. Table 3 presents the level of respondents' expectation and requirement measured in logit by Rasch model. The Likert scale was converted into a four point scale.

Table 3. Score Category of Logit for Components of Information Structure for ISMS

| Logit | Interpretation |
|---|---|
| -1.90 – 1.15 | Important |
| 1.16 – 4.21 | Moderately Important |
| 4.22 – 7.27 | Slightly Important |
| 7.28 – 10.33 | Unimportant |

Results from Table 4 determined the components that were significant to be included in the information structure which are agreed by information security practitioners. ISMS can be divided into three phases, as management requirement, establishment and assessment, threats and vulnerability, and risk management improvement. There are 75 items (components) altogether for the three phases. Out of 75 items, only 73 items were agreed upon and accepted by information security practitioners.

In this research, items ranked from logit 4.22 and below were accepted as components for information security management system. Based on the results, 73 items are considered as easiest endorsed items and regarded as important in the hierarchy by information security practitioners. As all the accepted items fell below logit 4.22, they are accepted to be components in ISMS's information structure. Unfortunately, only two items fell in the hierarchy as unimportant, and hence, rejected.

### 3.4. Item Measure Quality for Information Structure

Table 4 shows the item measure quality value for components of ISMS information structure. The results indicate that all items values were in the range between 0.5 between 1.5 for MnSq and value for Zstd value ±2.0 was also fulfilled, except two items (highlighted in yellow) had over misfit the framework expectation and were considered to be removed from the framework. Therefore, only the fulfilled items were considered to be added as components in the ISMS information structure.

Table 4. Analysis Results of RMM for Components of Information Structure for ISMS

| COMPONENTS OF INFORMATION STRUCTURE FOR ISMS | | | | | | |
|---|---|---|---|---|---|---|
| MANAGEMENT REQUIREMENTS | | | | | | |
| Criteria for Hiring/Promoting Information Security Practitioners | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Experience when hiring or promoting information security staff | 0.84 | -1.8 | 0.84 | -0.7 | -0.40 | Important |
| Skill and abilities when hiring or promoting information security staff | 0.98 | -0.2 | 1.01 | 0.1 | -0.12 | Important |
| Knowledge when hiring or promoting information security staff | 0.92 | -0.9 | 1.22 | 1.0 | -0.20 | Important |
| Education when hiring or promoting information security staff | 0.90 | -1.1 | 0.74 | -1.3 | -0.04 | Important |
| Professional certification when hiring information security staff | 0.91 | -1.0 | 0.93 | -0.3 | -0.04 | Important |
| Professional designations when hiring information security staff | 0.94 | -0.7 | 0.88 | -0.5 | -0.01 | Important |
| Types of Risks Assessment Documents | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Documentation of business function | 0.84 | -1.9 | 0.75 | -1.2 | -0.08 | Important |
| Documentation of operational | 0.85 | -1.8 | 0.75 | -1.2 | -0.04 | Important |
| Documentation of IT/IS | 0.87 | -1.5 | 0.79 | -0.9 | -0.01 | Important |
| Information Security Management Committee: Top Management | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Chief Executive Officer (CEO): responsible for all day-to-day management decisions and for implementing the organization's long and short term plans. | 1.00 | 0.0 | 0.87 | -0.5 | -0.04 | Important |
| Chief Operating Officer (COO): responsible for the daily operation of the organization. | 1.16 | 1.8 | 1.09 | 0.5 | -0.16 | Important |
| Chief Technology Officer (CTO): focused on scientific and technological issues within an organization. | 0.99 | -0.1 | 0.85 | -0.7 | -0.04 | Important |
| Chief Information Officer (CIO): responsible for the information technology and computer systems that support organizational goals. | 0.94 | -0.7 | 0.83 | -0.8 | -0.04 | Important |

| Information Security Management Committee: Information Security Professionals | INFIT | | OUTFIT | | Logit | |
|---|---|---|---|---|---|---|
| | MnSq | Zstd | MnSq | Zstd | | |
| Chief Information Security Officer (CISO): Define information security strategic direction, develop and maintain policies and establish roles and responsibility for information security within the organization. | 0.99 | -0.1 | 0.84 | -0.7 | -0.01 | Important |
| Information Security Operations: Perform information security operations, controls and security on the respective departments performing daily operations. | 0.92 | -0.9 | 0.74 | -1.2 | -0.01 | Important |
| Information Security Audits: Involves the verification of compliance against security policies, standards, legal and regulatory requirements. | 1.19 | 2.0 | 1.00 | 0.1 | -0.28 | Important |
| Information Security Compliance: Monitor compliance by the staff to the information security policies, standards and procedures. | 1.07 | 0.8 | 0.97 | -0.1 | -0.01 | Important |
| Top Management Involvement and Support | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Top management attends information security meetings. | 1.04 | 0.5 | 1.09 | 0.5 | -0.01 | Important |
| Top management involves in information security decisions. | 1.13 | 1.5 | 1.16 | 0.8 | -0.12 | Important |
| Top management involves in information security activities. | 1.07 | 0.7 | 1.20 | 0.8 | 1.11 | Important |
| Top management supports information security functions. | 1.14 | 1.4 | 1.06 | 0.3 | -0.94 | Important |
| Top management considers information security an important organizational priority. | 1.24 | 1.9 | 1.09 | 0.4 | -1.44 | Important |
| Top management is regularly involved in deciding important information security issues. | 1.09 | 1.0 | 1.18 | 0.9 | -0.24 | Important |
| Top management takes security issues into account when planning corporate strategies. | 1.12 | 1.2 | 1.25 | 1.1 | -0.60 | Important |
| ESTABLISHMENT AND ASSESSMENT | | | | | | |
| Establish Organizational Context | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Organizational objectives/goals | 0.89 | -1.0 | 0.79 | -0.9 | -0.98 | Important |
| Organizational scope and boundaries | 0.90 | -0.9 | 0.74 | -1.1 | -1.25 | Important |
| Scope and boundary of the security review | 0.92 | -0.7 | 0.85 | -0.5 | -1.44 | Important |
| SWOT analysis | 0.89 | -1.1 | 0.90 | -0.4 | 0.85 | Important |
| Information about critical assets | 0.89 | -1.2 | 0.71 | -1.4 | -0.73 | Important |
| Current security practices/requirement | 0.92 | -0.9 | 0.87 | -0.5 | -0.08 | Important |
| Information related to the operational/business function | 0.86 | -1.6 | 0.72 | -1.4 | -0.44 | Important |
| Person who use/support the IT system | 0.87 | -1.5 | 0.72 | -1.3 | 0.23 | Important |
| Threats and current organizational strength and vulnerabilities | 0.86 | -1.3 | 0.97 | -0.1 | -1.07 | Important |
| Schedules and deliverables | 1.03 | 0.3 | 0.96 | -0.1 | 0.43 | Important |
| Information Gathering Techniques | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Meeting | 1.04 | 0.5 | 0.95 | -0.1 | -0.01 | Important |
| Brainstorming | 0.96 | -0.4 | 0.82 | -0.8 | -0.01 | Important |
| Document Review | 0.96 | -0.4 | 0.99 | 0.1 | -0.01 | Important |
| Security requirement checklist | 1.04 | 0.5 | 1.03 | 0.2 | -0.28 | Important |
| Presentation and discussion | 0.87 | -1.6 | 0.77 | -1.1 | -0.01 | Important |
| Technical Assets | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Information Assets | 0.81 | -1.5 | 0.89 | -0.3 | -1.79 | Important |
| Data Assets | 0.89 | -0.8 | 0.83 | -0.5 | -1.90 | Important |
| Physical Assets | 1.06 | 0.7 | 1.12 | 0.6 | -0.52 | Important |
| Hardware Assets | 0.91 | -0.9 | 0.75 | -1.2 | -0.64 | Important |
| Software Assets | 0.89 | -1.1 | 0.74 | -1.2 | -0.90 | Important |
| Personnel Assets | 1.00 | 0 | 0.80 | -0.9 | -0.01 | Important |
| Non-Technical Assets: Core Knowledge of Organization | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Teams of expertise applied their mutual thought, knowledge and expertise to ensure the continuity in organization's routine process. | 1.01 | 0.2 | 0.90 | -0.4 | -0.01 | Important |
| Staff with experience and expertise are the organization's important process knowledgeable resource and valuably needed to make decision and apply strategies. | 1.10 | 1.2 | 0.95 | -0.2 | -0.24 | Important |
| Experts' knowledge which is codified or articulated in publications, documentations, audio-visual materials, flowcharts, scripts, procedures and so on. | 0.94 | -1.6 | 0.78 | -1.0 | -0.08 | Important |
| Non-Technical Assets: Informal & Unofficial Information Exits on three types of Media: | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Digital media (example: desktop PCs, notebook computer, personal digital assistants (PDAs) | 1.03 | 0.4 | 0.85 | -0.6 | -0.20 | Important |
| Physical media (paper documents which can be written, printed) | 1.10 | 1.1 | 0.94 | -0.2 | -0.04 | Important |
| Cognitive media (Exists in the mind of a personnel) | 1.01 | 0.2 | 0.86 | -0.6 | -0.08 | Important |
| Non-Technical Assets: Informal & Unofficial Information is leaked through the following workaround activities: | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| Storage: Saving or coping data/information to a data storage device | 1.17 | 1.7 | 1.02 | 0.2 | -0.85 | Important |
| Distribution/ Transmission: Exchange documentation within, between and among organizations | 0.99 | -0.1 | 0.98 | 0.0 | -1.48 | Important |
| Access & Use: Activities such as printing, photocopying, capturing, scanning, typing, writing, reading, hearing and speaking/discussing/conversing | 1.12 | 1.2 | 1.08 | 0.4 | -0.94 | Important |
| Destruction: During the process of destroying information which is no longer valuable/ necessitated to be preserved. | 1.17 | 1.8 | 0.96 | -0.1 | -0.48 | Important |
| RISK MANAGEMENT IMPROVEMENT | | | | | | |
| Information Security Training for Information Security Staff | INFIT | | OUTFIT | | Logit | |
| | MnSq | Zstd | MnSq | Zstd | | |
| External training | 1.04 | 0.5 | 0.95 | -0.2 | -0.04 | Important |
| Internal training | 0.92 | -0.9 | 0.74 | -1.2 | -0.01 | Important |
| Seminar | 0.91 | -1.0 | 0.98 | 0.0 | -0.08 | Important |

## 4. CONCLUSION

The main contribution of this study is the information structure framework for ISMS. The existing ISMS process approach and certification model which is popularly used by organisations to structure all their ISMS processes is PDCA model. The PDCA model uses Deming's theory to form the basis for total quality management and ISO 9001 quality standards. The PDCA model's limitation is that the model is unable to give information on any suggestions on how organisations should develop security objectives and strategies. However, the information structure framework lists out all the components involved in the ISMS process. Practitioners only need to follow the layout information flow together with the quality elements to achieve the ISMS development.

Each of the iinformation security department in the organization have responsibility to do the strategic planning. The department required to comprehensivly prepare all the compulsory planning before beginning to do their actual security management. Therefore, by having the proposed information structure framework, the process of gathering required information in order to conduct the ISMS will be more methodical and convincing if the organisations able to recognize beforehand all the required information they wanted earlier the commencement of the plan. It is believed to guides the practitioners step by steps with the general view of flow, types of information to be gathered and the requirements to be met before ISMS is conducted. 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 achieving a clear direction to reach ISMS goals and objectives.

The benefit of the framework is offered to information security practitioners, regardless of whether practitioners are newly approaching to apply ISMS or those that have been long in this field. This study contributes to the field of information security management system, particularly in the ISMS certification by providing a process approach framework which lists all the necessary components for guiding practitioners to choose preferred ISMS methodologies or to achieve ISMS certification procedure. The proposed framework provides proper guidelines which can be used by the practitioners to perform ISMS planning development and certification.

## ACKNOWLEDGEMENTS

We would like to say thank you to Universiti Tun Hussein Onn Malaysia (UTHM) for kindly proving us with the internal funding (Vot B29000).

## REFERENCES

[1] R. Bernard, "Information Lifecycle Security Risk Assessment: A Tool for Closing Security Gaps," *Comput. Secur.*, vol. 26, no. 1, pp. 26–30, Feb. 2007.
[2] D. J. Landoll, *The Security Risk Assessment Handbook- A Complete Guide for Performing Security Risk Assessments*. Boca Raton New York: Auerbach Publications, Taylor & Francis Group, 2006.
[3] Z. I. Saleh, "Proposed Framework for Security Risk Assessment," *J. Inf. Secur.*, vol. 02, no. 02, pp. 85–90, 2011.
[4] E. Hulitt and R. B. Vaughn, "Information System Security Compliance to FISMA Standard- a Quantitative Measure," *Telecommun. Syst.*, vol. 45, no. 2, pp. 139–152, 2010.
[5] J. Eloff and M. Eloff, "Information Security Management – A New Paradigm," in *Proceedings of SAICSIT*, 2003, pp. 130–136.
[6] Y. Barlette and V. V. Fomin, "Exploring the suitability of IS security management standards for SMEs," in *Proceedings of the 41st Hawaii International Conference on System Sciences*, 2008, pp. 1–10.
[7] J. Brenner, "ISO 27001: Risk management and compliance," *Risk Manag.*, vol. 54, no. 1, pp. 24–29, 2007.
[8] V. V. Fomin, H. J. de Vries, and Y. Barlette, "ISO/IEC 27001 Information System Management Standard: Exploring The Reasons for Low Adoption," in *Proceedings of The third European Conference on Management of Technology (EUROMOT)*, 2008.
[9] M. Korman, T. Sommestad, J. Hallberg, J. Bengtsson, and M. Ekstedt, "Overview of Enterprise Information Needs in Information Security Risk Assessment," in *Enterprise Distributed Object Computing Conference (EDOC), 2014 IEEE 18th International*, 2014, pp. 42–51.
[10] T. Tsiakis, A. Chatzipoulidis, T. Kargidis, and A. Belidis, "Information Technology Security Governance Approach Comparison in E-banking," in *In International Conference on Security Technology*, 2011, pp. 75–84.
[11] T. C. C. Tan, A. B. Ruighaver, and A. Ahmad, "Information Security Governance : When Compliance Becomes More Important than Security," in *In IFIP International Information Security Conference*, 2014, pp. 55–67.
[12] F. J. Bjorck, "Discovering Information Security Management," Stockholm University & Royal Institute of Technology, 2005.
[13] A. Vorster and L. E. S. Labuschagne, "A Framework for Comparing Different Information Security Risk Analysis Methodologies," in *Proceedings of SAICSIT 2005*, 2005, pp. 95–103.
[14] S. Lichtenstein, "Factors in the selection of a risk assessment method," *Inf. Manag. Comput. Secur.*, vol. 4, no. 4, pp. 20–25, 1996.
[15] U. Sekaran, *Research method of business: A skill-building approach*. New York: John Wiley and Sons, Inc, 2003.

[16] X. An and Y. Yung, "Item Response Theory : What It Is and How You Can Use the IRT Procedure to Apply It," in *Proceedings of the SAS Global Forum 2014 Conference*, 2014, pp. 1–14.
[17] B. D. Wright, "A History of Social Science Measurement," *Educ. Meas. Issues Pract.*, vol. 16, no. 4, pp. 33–45, 1997.
[18] L. M. Searing, "Family Functioning Scale Validation: A Rasch Analysis," 2008.