International Journal on Advanced Science Engineering Information Technology

Vol.6 (2016) No. 6
ISSN: 2088-5334

An Empirical Study of Information Security Management Success Factors

Mazlina Zammani[#1], Rozilawati Razali[#2]

[#]*Research Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600, Bangi, Selangor, Malaysia*
E-mail: [1]mazlina2002@yahoo.com, [2]rozilawati@ukm.edu.my

Abstract **— Information security management (ISM) is a continuous, structured and systematic security approach to managing and protect the organisation's information from being compromised by irresponsible parties. To ensure the information remains secure, many organisations have implemented ISM by establishing and reviewing information security (IS) policy, processes, procedures, and organisational structures. Regardless of the efforts, security threats, incidents, vulnerabilities, and risks are still plaguing many organisations. Lack of awareness of ISM effectiveness due to low understanding of the success factors is one of the major factors that cause this phenomenon. This study aimed to address this subject by firstly identifying the ISM key factors from existing literature and then by confirming the factors and discovering other related factors from practitioners' perspective. This study used a qualitative method where it adopted semi-structured interviews involving nine practitioners. The data were analysed using content analysis technique. Through the analysis, the study validated several ISM factors and their elements that contribute to the success of ISM. The findings provide practitioners with the high understanding of ISM key factors and could guide practitioners in implementing proper ISM.**

Keywords— **information security management; information security; success factors**

I. INTRODUCTION

In the era of globalisation, protection of information is critical in order to ensure business continuity [1]. Addressing security breaches become a challenge to organisations [2]. Information Security (IS) is a concept that is related to protecting information in order to preserve the value it has for organisations and individuals [3], [4]. Information's confidentiality, integrity, availability, authenticity, accountability, and reliability are ensured through IS [5], [6], [7], [8], [9], [10]. Organisations which are lacking in IS will usually prone to a large number of security breaches and incidents [11]. Recognising this, many organisations have put in place substantial efforts in managing and handling the security of their information. They have implemented Information Security Management (ISM) initiatives by reviewing IS processes, policies, procedures, controls and organisational structures. ISM is a comprehensive approach that involves the implementation of activities and controls to protect organisation's information assets from any intrusion [7], [12], [13], [14]. In spite of the efforts, organisations are still exposed to information security threats, incidents, vulnerabilities and risks [6], [8], [15]. One of the contributing reasons is the ineffective ISM current practices [16]. Organisations often emphasise on the technical aspects without appropriate considerations on the non-technical aspects when implementing ISM [17], [18]. They normally perpetrate into the initiatives without knowing the key factors that affecting its success [19]. Based on the above facts, there is a need to identify the key factors that contribute to the success of ISM. This paper aims to address this issue by identifying and collating the key factors from theoretical and empirical perspectives. The identified factors can be used as a guidance to organisations in improving their ISM practices.

This paper is organised as follows. The next section presents ISM factors and elements that were gathered from the literature and the methodology used to collect and analyse the theoretical and empirical data. Section III presents the findings of the analysis. Finally, section IV concludes the paper by summarising the finding and outlining the future work.

II. MATERIALS AND METHODS

ISM is an ongoing process that involves planning, implementing, monitoring and improving IS activities [8], [9], [20]. In order to ensure the information is well maintained and the organisation's mission, vision and goals can be achieved, the organisation should have an effective ISM.

In the initial stage of ISM, top management shall establish IS policy that is appropriate to the purpose of the

organisation. IS policy is the foremost requirement in ISM [21]. Top management is responsible for formulating the policy which should be clear [8], [9], [10], [22], [23] in defining IS objectives, comprehensive [7], [8], [9], [10], [22], regularly reviewed [8], [9], [10], and communicated [9], [10], [23] to entire organisation and the relevant external parties. Top management shall portray leadership [9], [10], [23], and commitment [7], [8], [9], [10], [19], [22], [23], by ensuring the integration of IS requirements into the organisation's processes; ensuring the IS policy, procedures, controls, and processes are implemented and complied by the employees and third parties; and allocating sufficient financial and human resources for performing ISM processes [5], [8], [9], [10], [22].

The main process in ISM is risk management which consists of risk assessment and risk treatment activities [9]. The purpose of risk management is to identify, analyse and evaluate IS risks, as well as implementing actions to modify and control the risks [24], [25], [26]. Besides risk management process, business continuity management (BCM) also contributes to the success of ISM [8], [22]. The goal of BCM is to ensure the continuity of organisation's business operations during or after adverse situations [27], [28], [29], [30]. BCM requires a comprehensive business continuity plan which is derived from business impact analysis and risk assessment [5]. The business continuity plan determines the processes, procedures, resources, roles and responsibilities involved. To ensure the BCM is effective and valid during the adverse situations, the organisation shall exercise and test the business continuity plan [5], [8], [31], [32].

ISM technical operation activities are carried out by the ISM team. The team is accountable for implementing ISM processes and controls by following the steps written in the ISM procedures. Thus, the procedures should be clear, complete and communicated to the ISM team [5], [8], [32]. The knowledge, commitment and technical skills of the ISM team are highly required in implementing IS processes, procedures and controls [5], [9], [10], [19].

To increase business performance and reduce security breaches and incidents in the organisation, the employees and third parties have to comply with IS policy, laws and regulation [6], [9], [10], [22], [23]. The compliance can be guaranteed if the employees and third parties have the awareness [8], [22], [23], [33] and high motivation [7], [22] on the importance of IS. To raise awareness on the importance of IS and its requirements, the awareness programme should be conducted [7], [8], [9], [10], [22], [23]. On the other hand, the training for the ISM team and dedicated employees should be organised to ensure they are competent to perform their respective duties [7], [8], [9], [10], [22], [23].

In order to ensure ISM is well implemented and maintained, the organisation shall conduct IS audits at planned intervals. The weaknesses in any ISM processes, procedures and controls can be identified during the IS audits [8], [22], [24] or effectiveness assessment [34], [35]. The organisation needs to establish and perform audit programmes [8], [9], [10] which include the planning for auditing process, the training for the IS audit team and executing the audit process. At the end of the auditing process, the audit team must issue an audit report that contains the audit findings [9]. Therefore, the team must possess the required knowledge on IS and the subject matters to be audited, audit skills in identifying problems, and be committed throughout the auditing process [8], [9], [10], [22].

Table 1 summarises the success factors that have been categorised into three aspects: People, Organisation and Process. The People aspect consists of the key players of ISM. The Organisation aspect states the important documents that must be established and followed, while the process aspect outlines the ISM key practices and activities that must be performed by the key players. All of these factors have their own elements that contribute to the success of ISM. The detailed explanation about the factors and elements can be found in [36]

TABLE I
LITERATURE REVIEW ON ISM SUCCESS FACTORS

Aspects	Factors	Elements	Sources
People	Top Management	Leadership, Commitment	[5], [7], [8], [9], [10], [19], [22], [23], [37], [38], [33]
	ISM Team	Knowledge, Skills, Commitment	[5], [9], [10], [19]
	IS Audit Team	Knowledge, Skills, Commitment	[8], [9], [10], [22]
	Employees	Awareness, Motivation, Compliance	[5], [6], [7], [8], [9], [10], [22], [23], [33]
	Third Parties	Awareness, Compliance	[5], [6], [8], [9], [10], [22], [23], [33]
Organisation	IS Policy	Comprehensive, Clear, Reviewed Communicated	[5], [7], [8], [9], [10], [22], [23]
	IS Procedures	Clear, Complete, Communicated	[5], [8], [32]
Process	Competency Development & Awareness	Training, Awareness Programmes	[5], [7], [8], [9], [10], [22], [23]
	Resource Planning	Human Resources, Financial Resources	[5], [8], [9], [10], [22]
	Risk Management	Risk Assessment, Risk Treatment	[5], [6], [9], [10], [22], [23], [24], [37]
	Business Continuity Management	BCM Plan, Testing	[5], [8], [31], [32]
	IS Audit	Audit Programme, Audit Finding & Reporting	[5], [8], [9], [10]

The methodology used in this research was a qualitative method. The qualitative method was chosen because it allows researchers to obtain the data in detail and allows a deeper understanding of the subject matter. As mentioned earlier, this study was carried out to identify the success factors of ISM. The identified factors that were gathered from the literature were expanded by conducting an empirical work involving interviewing ISM experienced practitioners. Fig. 1 illustrates the research design.

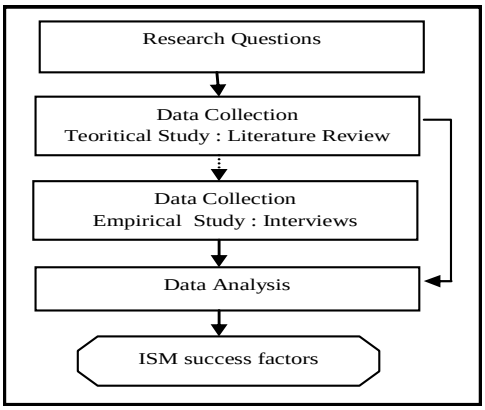

Fig. 1 Research design

A. Research Questions Formulation

The study focused on answering the following questions:

i. What are the factors that contribute to the success of ISM?
ii. What are the specific elements for each of these factors?

The questions acted as the basis for data collection during theoretical and empirical studies.

B. Data Collection

1) Theoretical Study

This study was initiated by analysing the existing literature. This theoretical study reviewed published and unpublished documents in multiple online databases. The findings of the study have been elaborated in [36].

2) Empirical Study

This study aimed to verify the factors that were derived from the theoretical study as well as discovering other relevant factors. This study used semi-structured interviews. A series of individual and focus group interviews with experienced ISM practitioners were conducted.

i. *Sampling*

The sampling was based on the ability of informants to answer the research questions. Thus, purposive sampling method was adopted. For the individual interviews, five ISM practitioners who had actively experienced and involved in ISM from five different agencies were invited to participate in the study. The profiles of the five participants are shown in Table 2.

Meanwhile**,** the participants for the focus group interview comprised of a head of ICT department, ISM coordinator, ISM implementer and ISM auditor. All participants possessed at least five years' experience in ISM. Table 3 outlined the participants' profiles.

ii. *Instruments*

Interview questions were used as the instruments for individual and focus group interviews. The questions were derived based on the findings of the theoretical study. The questions were broken into two parts, A and B. Part A covers the ISM implementation in participants' organisations as well as the participants' experience in implementing ISM. While the questions in part B revolve around twelve ISM success factors which are Top Management, ISM Team, IS Audit Team, Employees, Third Parties, IS Policy, IS Procedures, Competency Development & Awareness, Resource Planning, Risk Management, Business Continuity Management and IS Audit. Table 4 summarised and described the twelve factors that were included in the interview questions.

iii. *Protocol*

For individual interviews, the participants' consents were obtained before conducting the sessions. The appointments were made in advance to set the date and time of interviews. The participants were provided with a brief description of the interview objectives. After obtaining the participants' agreement, formal invitations were sent to the participants. The interviews were conducted between February 2016 and May 2016. The participants were interviewed individually at their workplace which took an average of 90 minutes per person. Each session was recorded using a tape recorder and field notes.

Likewise, participants' agreements were also obtained before conducting the focus group session. Two weeks before the focus group session, an invitation letter containing information about the objectives, date, time and venue was sent to participants. The focus group session was conducted on 14 May 2016 at 10.00 am. The session was recorded using video recorder, audio tape recorder, and field notes. The session took almost three hours.

C. Data Analysis

The data gathered from the theoretical and empirical study were transcribed and analysed using content analysis. Content analysis is a qualitative research technique that has been widely used to analyse written, oral or visual communication messages [39]. The analysis involved identifying the frequent elements in the data. Later, the elements were categorised according to several logical groups of factors by using inductive and deductive reasoning technique. The deductive reasoning involved using the factors and elements identified in the theoretical study and later confirming or disapproving them by comparing with the data from the empirical study. The inductive reasoning recognised new emergent data from the empirical study and then abstracted the data as new factors or grouped it into the existing factors.

TABLE II
PARTICIPANTS' PROFILES FOR INDIVIDUAL INTERVIEWS

Participant Code	Agency	Position	ISM Experience
INF 1	A	Senior Information Technology Officer	6 years
INF 2	B	Information Technology Officer	3 years
INF 3	C	Information Technology Officer	5 years
INF 4	D	Senior Information Technology Officer	4 years
INF 5	E	Chief Senior Information Technology Officer	6 years

TABLE III
PARTICIPANTS' PROFILES FOR FOCUS GROUP INTERVIEWS

Participant Code	Position	ISM Roles	ISM Experience
FG1	Head of Department	Top Management Representative	6 years
FG2	Senior Information Technology Officer	ISM Coordinator	6 years
FG3	Senior Information Technology Officer	ISM Implementer	5 years
FG4	Senior Information Technology Officer	ISM Auditor	6 years

TABLE IV
INTERVIEW QUESTIONS DESCRIPTION

Factors	Description
Top Management	To verify whether top management should have full commitment and strong leadership in order to achieve ISM outcomes.
ISM Team	To confirm the team must have wide IS knowledge and be updated with the current security issues as well as be skilful and committed to implementing IS process and activities.
IS Audit Team	To substantiate whether the auditors should possess the required knowledge on the people and processes to be audited; technical skills for identifying problems, getting the information and reporting the audit results; and provide fully commitment to ensure the effectiveness and completion of the auditing process.
Employees	To affirm whether the awareness, motivation, and compliance of the employees impact the ISM success.
Third Parties	To confirm whether the awareness and compliance of the third parties affect the ISM success.
IS Policy	To confirm whether the policy must be comprehensive which covers the requirements and controls prescribed by the ISM standards; clear in describing IS objectives and the responsibilities of the parties involved; communicated to the employees and stakeholders and regularly reviewed to ensure it is significant to the recent needs.
IS Procedures	To identify the required characteristics of good quality procedures.
Competency Development & Awareness	To validate whether the competency development and awareness programmes are important to develop the competency of ISM team and employees.
Resource Planning	To confirm whether it is important to include resource planning process to support and carry out ISM activities. Resource planning comprises human and financial resources.
Risk Management	To substantiate whether the risk management, which consists of risk assessment and risk treatment, is a key to the success of ISM.
Business Continuity Management	To verify whether the Business Continuity Management plan and testing contribute to the success of ISM.
IS Audit	To affirm whether it is important to monitor, measure and evaluate the compliance of IS processes, controls, and activities in order to ensure the effectiveness of ISM. The main tasks relating to IS audit are audit programme and audit finding & reporting.

III. Results and Discussion

The results of data analysis are presented in the following paragraphs. To support the results, a number of interview excerpts are provided. The elements pertaining to the respective factors are shown in bold.

A. *People*

People refer to the individuals or teams who are directly involved in the planning, implementing, monitoring and improving the ISM processes. Six factors identified in the people aspect are the Top Management, Coordinator Team, IS Team, IS Audit Team, Employees and Third Parties.

1) Top Management

The success of ISM in the organisation is strongly associated with the knowledge, leadership, and commitment of its top management. Top management should have a clear understanding regarding ISM governance, objectives, and issues. Top management is accountable for ensuring the policy, procedures, processes, and controls are established, implemented and complied by the entire organisation and the external parties. In addition, top management is also responsible for monitoring and reviewing the effectiveness of ISM as well as providing adequate resources to support ISM processes. Below are some of the comments from the participants:

- *"The direction and commitment of top management are very important in establishing, implementing and supporting ISM processes and activities especially if it engages budget and manpower".* - INF1
- *"If top management does not have the strength of leadership and commitment, ISM will not run as expected and the staff may not give full attention to the implementation."* - INF2
- *"Top management must have the knowledge in ISM. They need to be clear about the objectives, scope, and issues of the ISM and how to integrate ISM objectives with organisation objectives. In addition, leadership and commitment of top managements are essential. Leadership can be seen from how top management manages the ISM by ensuring the policy, procedures, processes, and controls are established and well implemented in the organisation, while commitment can be measured by the support during the implementation"* – INF 4.

2) ISM Team

ISM Team consists of a designated staff involved in most IS activities. The knowledge, skills, commitment, willingness and cooperation of ISM team are desirable in carrying out the ISM processes. The team must always be updated with the current security issues and should own broad IS knowledge. Moreover, the team must be skilful, cooperate, and committed to their work tasks. They must be always willing to accept new directed tasks.

A number of comments from the participants are presented below:

- *"ISM team should have the wide IS knowledge and technical skills because most of the operations are carried out by them. Commitment is needed to ensure the tasks run smoothly."* - INF1
- *"In my opinion, ISM team must possess a very good knowledge in order to complete their tasks. Skills are also important because if there are no skills, the progress of the running tasks will be a bit slow. Similarly, the commitment and cooperation of all team members are also necessary. "*- FG2
- *"Willingness of ISM team is very important. The team must be ready to commit to any incoming tasks. They need to work together so that the tasks can be finished on time."* – FG3
- *"Knowledge, skills and commitment of ISM team are needed to ensure the success of ISM. In addition, the team must be willing to work outside their scope of work."* – INF4

3) Coordinator Team

The coordinator team plays a major role in coordinating ISM activities. Major ISM documents and activities are managed by the team. The team acts as a liaison between top management, ISM team, IS audit team and employees. The team is responsible for organising the training and awareness programmes, managing the resources, harmonising ISM documents and presenting the progress of ISM to the top management. Thus, the team must own ISM knowledge, give a commitment in coordinating ISM activities and have good communication skills when communicating with other parties.

The statement is supported by the following participant's comment:

- *"The coordinator team is the owner of major ISM documents. They harmonise the documents and present the progress of ISM to the top management. They also coordinate ISM activities. Therefore knowledge is very important as the team must be familiar with the whole processes of ISM. Their commitment is required to conduct ISM activities such as training and awareness programmes. In order to deliver information, the team should be able to communicate effectively with all level of staff in the organisation. "* - INF5

4) IS Audit Team

The IS audit team is accountable to ensure IS controls, processes, procedures, and activities are executed correctly. The team should have appropriate knowledge on the people, processes, and procedures that need to be audited. Moreover, auditing skills, communication skills, commitment and cooperation within team members are required throughout the auditing process.

The comments below express the perception of IS audit team:

- *"IS audit team need to be familiar with ISM objectives, designated ISM personnel, and ISM processes and procedures before implementing the auditing process. Auditing skills, commitment and cooperation among team members are essential to guarantee the effectiveness of the auditing process."* - INF2
- *"The IS audit team contributes to the success of ISM. The compliance with IS policy and procedures can be monitored through auditing."* - INF3

- *"The team's commitment is necessary to complete the auditing task in the prescribed time. Auditing skills and communication skills are important to obtain information. Sometimes, the auditees assume that auditors always want to dig for auditees' errors and weaknesses. It might be because of the way they ask questions. Hence, it is vital for the audit team to have good communication skills"* - INF5
- *"Firstly, IS audit team should understand the whole processes of ISM. Lack of knowledge can cause the wrong questions to be asked. In addition, the team must possess auditing skills as well as giving a full commitment in auditing task. The commitment can be seen in terms of punctuality and implementation of auditing activities"* - INF4

5) Employees

The organisation's employees should have awareness on the IS policy, controls, threats, and risks. The employees have to comply with the IS policy, rules, and laws in order to reduce security incidents. The motivation of the employees enhances the success of ISM implementation.

The statement is supported by the following participants' comments:

- *"In ISM, employees are the second important persons after ISM team. Even though the ISM team have implemented security measures appropriately, but if employees break up the rules or do not comply with the security policy and controls, the implementation of ISM is meaningless. Therefore, employees must be aware and comply with the IS policy, laws, and rules."* – INF2
- *"Employees must realise the importance of IS. The awareness includes the knowledge and understanding on the security aspects. The employees must be well informed on IS policy and regulation, the objective of ISM, and the incoming threats and risks. When the objective of ISM is known, then compliance can be achieved. Employees' motivation is needed in this aspect."* - INF4

6) Third Parties

Third parties are referring to individuals or companies involved in providing services to organisations on a contract basis in a particular period of time. To ensure the organisation's information remain secure, the third parties must be aware and comply with security policy, laws, and contract.

The statement is supported by the following participants' comments:

- *"Awareness is not only important to the employees, but also to the third parties. Third parties' awareness contributes to the success of ISM. Third parties must be aware on IS policy and comply with the policy."* - FG 1
- *"Organisation receives services from third parties. Therefore, third parties have to conform to the contract and the policy. They need to sign a non-disclosure agreement. If they violate the policy or contract, the organisation must take action against them."* - INF 5
- *"Third parties are affecting the success of ISM. They must comply with the organisation's security controls and laws. "* - INF 4

B. *Organisation*

Organisation aspect refers to the strategic and technical documents that must be established and followed during the ISM processes. Two factors identified in organisation aspect are IS policy and IS procedures.

7) IS Policy

IS policy is a strategic document that consists of objectives, directions, and rules that must be established and followed by the entire employees and third parties. The policy must be clear in defining IS objectives, and the roles and responsibilities of the employees and third parties. It must be comprehensive which covers the requirements and controls set by the ISM standards and aligns with the organisation's mission and vision. IS policy shall be reviewed regularly to ensure it is relevant to the present needs and must be communicated to the employees, stakeholders and third parties.

A number of comments from the participants are presented below:

- *"The scope of IS policy should be broad which cover all IS requirements and the parties involved in the organisation. In addition, the policy should be reviewed regularly. It is not a static document. The policy must be communicated to the entire organisation through multiple channels such as organisation's website or pamphlets. "*- INF5
- *"IS policy is a strategic document and must be established before performing any IS activities. The policy is important to the success of ISM. The goals and objectives of the policy must be clear and understandable. The policy should be reviewed at least once a year and be communicated to entire employees, third parties and stakeholders."* - FG1
- *"A comprehensive security policy covers all security aspects. The periodic review must be done to make sure the policy is up to date. Most importantly, the policy must be communicated to everyone."* – INF 2
- *"In developing IS policy, each component in the policy must be identified thoroughly. It includes the control and responsibilities of the delegated personnel and employees. Based on international standards, the policy should also be revealed to the entire organisation. "* - FG4

8) IS Procedures

IS procedures are the operating guidelines that contain a series of actions that explain how to perform IS processes. The procedures are directly derived from the IS policy. To ensure the implementation of ISM is executed appropriately and correctly, the procedures must be clear and completely describe the steps to accomplish IS processes or activities. The procedures should be reviewed periodically or when environment changes and must be communicated among IS team members.

Some of the comments from the participants are presented below:

- *"Recently, there are many IS procedures have been developed in the organisation, for example 'password change procedure'. All steps in the procedure need to be correctly followed. Thus, the procedure must be clear and complete to enable users to follow the prescribed steps."* – FG3
- *"The clarity and completeness of the procedure can be seen from the steps written in the procedure. It is more understandable if the procedure is complete and explaining in detail the steps to be taken. The objective, roles, responsibilities should be included in the procedure. "* - FG4
- *"The clarity of procedures is similar to the clarity of IS policy. However, the procedures must be more specific. The procedures need to be frequently reviewed and communicated to the team members as the members turn in and out of the organisation."* - INF4
- *"IS procedures are the guidelines for implementing IS processes and activities based on the needs outlined in the security policy. The procedures must be clear, complete and reviewed regularly."*- INF5

C. *Process*

The findings show a number of main processes involved in ISM namely Resource Planning, Competency Development and Awareness, Risk Management, IS Auditing and Business Continuity Management.

9) Resource Planning

Resource planning is essential to support and perform ISM processes. Resource planning consists of financial resources and human resources. Financial resources comprise the cost of buying new assets and maintaining existing assets, the cost of manpower and the cost to perform IS activities. Meanwhile, human resources refer to the teams or individuals to be engaged in ISM activities.

The statements are supported by the following participants' comments:

- *"The more manpower is allocated, the faster tasks can be completed. At the same time, the financial resource is required to send the individuals or ISM team members to the relevant training so that they improve their skills and enhance their knowledge."* – INF 5
- *"It's more of human resource. Is the number of ISM team members to perform IS tasks sufficient? Are they experienced and qualified?"*- INF4
- *"In risk management process, there will be a decision to purchase new assets or maintain the existing assets. Therefore, the budget needs to be adequate."* - FG4
- *"Financial resources are necessary to perform IS processes and activities. For example, the organisation requests an external IS auditor to perform the audit. Certainly, it needs a budget for the auditing costs. Financial resources are also needed in order to organise the training and awareness programmes to the ISM team, IS audit team and employees. Usually, the high budget allocation is only required in the early stage of ISM implementation. "*- FG1

10) Competency Development and Awareness

The competency and awareness of ISM teams, IS audit team, employees and third parties can be gained through the training and awareness programmes. The purpose of the training programmes is to ensure that the people have knowledge and skills in each task handling. Meanwhile, the purpose of the awareness programmes is to ensure the people are aware of IS policy, threats, risks as well as their roles and responsibilities.

A number of comments from the participants are presented below:

- *"Through the training, employees learn a lot of new things. Their skills and understanding on IS are increased. While awareness programmes are important for the employees, stakeholders and third parties to be aware of IS policy and be alert to what are happening around them."* - INF 3
- *"It is vital to have relevant training. Training roadmap or training schedule is necessary* so *that the entire personnel involved in ISM get the adequate training to perform their tasks perfectly. "* - INF4
- *"ISM is not only focused at the headquarters but to all the branches. Therefore, awareness programmes must be done at all levels. There are many ways to distribute the awareness such as email and leaflet distribution. Questionnaires are distributed to analyse the level of employees' awareness before and after undergoing the awareness programmes. "* - FG3

11) *Risk Management*

Risk management is the key process in ISM. Risk management is a process of measuring and analysing the risk levels and taking appropriate actions to control the risks. Two major components in risk management are risk assessment and risk treatment. Risk assessment involves sub-activities such as establishing the risk acceptance criteria, identifying assets and threats, determining the impacts and probability of risk occurrence and determining the risk levels. The risk treatment involves the activity of implementing the protection strategies based on the risk assessment results.

The statements are supported by the following participants' comments:

- *"Risk management is an important process in ISM. The purpose of risk management is to monitor the risk level of ICT assets. ICT assets consist of information, data, hardware, software, and people. The level of risks and security incidents might be reduced if we execute the risk management activities correctly."* - INF 1
- *"The objective of risk management is to mitigate risks as well as reducing adverse impacts on assets to an acceptable level. The methodology used in risk management helps the organisation in managing the risks appropriately. ISM team must be committed to executing the risk management activities. We need the support from top management to achieve the risk management objective."*- INF 2

- *"We need to be clear with the scope of ISM before carry out risk management process. First of all, we need to know the boundaries. From there we can identify the assets and assess their levels of risk by applying risk assessment activity. Next, the assets with the high level of risk will be treated after reporting and getting approval from top management. "* - FG 2
- *"Risk management involves activities such as identifying assets and threats, establishing the risk acceptance criteria, assessing the probability of risks occurrence, determining the levels of risk, and performing protection strategies."* - INF 5

12) IS Audit

IS audit is one of the requirements in ISM standards. Through the IS audit process, the compliance of IS policy, procedures, processes, controls and activities can be monitored, measured and evaluated. The components in audit process are audit programme which consists of audit planning, audit execution, and auditor training; audit findings and reporting; and follow-up audit to check the corrective and preventive actions that have been done. Below are some of the comments from the participants:

- *"IS audit is one of the requirements in ISM standards. The purpose of the audit is to review and evaluate the compliance on IS processes, policy, and procedures. Audit programme should be developed, established and implemented. The programme is led by the Chief Auditor. After performing the audit, the audit reporting which includes the audit findings shall be presented to the top management and ISM team for further actions. "* - FG4
- *"After completing the audit programme, within a certain period of time, the IS audit team should carry out a follow-up audit to check the status of corrective and preventive actions made by IS teams or employees. "* - INF 2
- *"Audit plan is needed before performing the actual audit. Then, during the audit, the audit team should be skilful to locate the findings. It is also important to write in detail in the audit report. The report should be accompanied by findings evidence. "* FG 1

13) Business Continuity Management

Business continuity management ensures the organisation's businesses operate smoothly during and after the unintended events. When the unintended events occur, business continuity plan that outlines the resources, processes, procedures, and responsibilities should be activated. Organisation shall carry out periodic tests on the business continuity plan to ensure its validity and effectiveness. Below are some comments from the participants:

- "*The important thing in Business Continuity Management is the business continuity plan. The organisation should determines IS requirements and must be embedded in the business continuity plan. The plan outlines the processes, procedures, resources and responsibilities for controlling incidents or disasters."* - INF4
- *"Business continuity plan and simulations are closely related to each other. Business continuity plan should be developed, documented and approved by the top management. The plan must be tested to observe its effectiveness. "*- FG3
- *"Organisations whose adopt ISM standard must implement business continuity management. The purpose of business continuity management is to ensure the sustainability of organisation's operations during and after the unintended events. Business continuity plan should be activated when the unintended events occur. "* - FG1

Table 5 lists the significant ISM success factors together with their corresponding elements that were found in the theoretical and empirical data. The factors and elements that were gathered in the theoretical or agreed in the empirical data are marked with '√'. The factors and elements that were not supported by theoretical or empirical data are marked with 'x'. The numbers in the brackets represent the number of participants who agreed or supported the existence of the data. For example, 3/9 means three out of nine participants agreed on the factor and element. The factors and elements were categorised into three aspects, which are People, Organisation and Process.

The empirical study has confirmed that most factors found in the theoretical study are relevant to the success of ISM. There are several new factors and elements added in people, organisation, and process aspect. The new elements added in people aspect are the knowledge of top management, cooperation and willingness of ISM team, and cooperation and communication skills of the audit team. In addition, people aspect includes one new factor namely coordinator team. The elements under the coordinator team are knowledge, commitment and communication skills.

In terms of organisation aspect, reviewed procedures are the new element considered in IS procedures factor. Meanwhile, in the process aspect, follow-up audit is the new element of IS audit factor.

The finding indicates that IS policy, competency developments and awareness, and risk management are the most factors agreed by the participants. Simultaneously, majority agreed that leadership and commitments of top management; knowledge, skills and commitment of ISM team; and knowledge of IS audit team are essential for ISM initiatives. In addition, resources planning and business continuity management are also highlighted by the participants. On the other hand, the knowledge, commitment and communication skills of coordinator team, as well as the cooperation of IS audit team, are less supported in the empirical study.

TABLE V
ISM SUCCESS FACTORS AND ELEMENTS

Aspects	Factors	Elements	Theoretical	Empirical
People	Top Management	Leadership	√	√ (6/9)
		Commitment	√	√ (6/9)
		Knowledge	X	√ (4/9)
	ISM Team	Knowledge	√	√ (9/9)
		Skills	√	√ (6/9)
		Commitment	√	√ (6/9)
		Cooperation	X	√ (3/9)
		Willingness	X	√ (4/9)
	IS Audit Team	Knowledge	√	√ (8/9)
		Auditing Skills	√	√ (5/9)
		Commitment	√	√(6/9)
		Cooperation	X	√(1/9)
		Communication Skills	X	√(3/9)
	Employees	Awareness	√	√ (6/9)
		Motivation	√	√ (3/9)
		Compliance	√	√ (6/9)
	Third Parties	Awareness	√	√ (4/9)
		Compliance	√	√ (4/9)
	Coordinator Team	Knowledge	X	√ (1/9)
		Commitment	X	√ (1/9)
		Communication Skills	X	√ (1/9)
Organisation	IS Policy	Comprehensive	√	√ (8/9)
		Clear	√	√ (8/9)
		Communicated	√	√ (8/9)
		Reviewed	√	√ (8/9)
	IS Procedures	Clear	√	√ (7/9)
		Complete	√	√ (5/9)
		Communicated	√	√ (3/9)
		Reviewed	X	√ (3/9)
Process	Competency Development & Awareness	Training	√	√ (8/9)
		Awareness Programmes	√	√ (8/9)
	Resource Planning	Human Resources	√	√ (7/9)
		Financial Resources	√	√ (7/9)
	Risk Management	Risk Assessment	√	√ (8/9)
		Risk Treatment	√	√ (8/9)
	Business Continuity Management (BCM)	BCM Plan	√	√ (7/9)
		Testing	√	√ (7/9)
	IS Audit	Audit Programme	√	√ (7/9)
		Audit Findings and Reporting	√	√ (7/9)
		Follow-up audit	X	√ (3/9)

IV. CONCLUSIONS

This paper has discussed the ISM success factors together with their corresponding elements. The factors and elements were gathered qualitatively through the theoretical and empirical study. The factors and elements are considered as valid as they have been agreed and supported by at least one previous study or informant. However, these findings can be refined and strengthened further by confirming the factors and elements quantitatively through a large-scale survey. In the meantime, these findings could guide practitioners in implementing proper ISM by focusing on the key players and their attributes, processes that need to be performed, and organisation's strategic and technical documents.

ACKNOWLEDGMENT

The authors would like to thank Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia for supporting this research. This research is funded by Universiti Kebangsaan Malaysia under Research University Fund (GUP-2014-006). The authors also thank the practitioners who participated in this study.

REFERENCES

[1] S. E. Chang and C. B. Ho, "Organizational factors to the effectiveness of implementing information security management," *Ind. Manag. Data Syst.*, vol. 106, no. 3, pp. 345–361, 2006.

[2] Y. Bobbert and H. Mulder, "Governance practices and critical success factors suitable for business information security" in *International Conference on Computational Intelligence and Communication Networks.* 2015. p. 1097-1104

[3] L. Silva, A. Paula Costa, T. Poleto, and J. Moura, “An analysis of and perspective on the information security maturity model: A case study of a public and a private sector company,” in *18th Americas Conference on Information Systems AMCIS*, 2012, vol. 3, pp. 1684–1694.

[4] T.R. Peltier, *Information Security Policies, Procedures, and Standards: guidelines for effective information security management.* Florida, USA:CRC Press, 2016

[5] *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology (NIST), Gaithersburg, MD, 2006.

[6] M.A.M. Stambul & R. Razali, “An assessment model of information security implementation levels,” in *Proc. 2011 Int. Conf. Electr. Eng. Informatics*, 2011, July, p. 1–6.

[7] M. Kazemi, H. Khajouei, and H. Nasrabadi, “Evaluation of information security management system success factors: Case study of Municipal organization,” *African J. Bus. Manag.*, vol. 6, no. 14, pp. 4982–4989, 2012.

[8] A. N. Singh, M. P. Gupta, and A. Ojha, “Identifying factors of organizational information security management” *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 8, 2014.

[9] ISO/IEC 27001:20013 “Information technology - Security techniques - Information security management systems - Requirements: ISO/IEC 27001:20013”, Switzerland: ISO, 2013.

[10] “COBIT 5 for information security,” Illinois, US: ISACA, 2012.

[11] W. Al-Salihy, J. Ann and R. Sures, “Effectivess of information systems security in IT organizations in Malaysia,” in *The 9th Asia-Pacific Conference*, 2003, p. 716–720.

[12] V. Pathari, and R.Sonar, “Deriving an information security assurance indicator at the organizational level,” *Info. Management & Computer. Security*. vol. 215, pp. 401–419, 2013.

[13] S. E. Chang and C. S. Lin, “Exploring organizational culture for information security management,” *Ind. Manag. Data Syst.*, vol. 107, no. 3–4, pp. 438–458, 2007

[14] Z. Tu, "Information security management: A critical success factors analysis." PhD thesis, McMaster University, Hamilton, Ontario, Canada, 2016.

[15] H.K. Kong, "Will the certification system for information security management help to improve organizations’ information security performance? The case of K-ISMS." *Indian Journal of Science and Technology*, vol. 9, no.24, 2016

[16] O. Matrane and M. Talea, “Towards a new maturity model for information security management,” *IJCSI International Journal of Computer Science Issues*, vol. 4, no. 6, pp. 71–78, 2014.

[17] B. Shojaie and H. Federrath, “The effects of cultural dimensions on the development of an ISMS based on the ISO 27001,” in *10th International Conference on Availability, Reliability and Security, 2015*, pp. 159–167.

[18] S. Soltanmohammadi, S. Asadi, N. Ithnin, and C. Science, “Main human factors affecting information system security,” *Interdiscip. J. Contemp. Res. Bus.*, vol. 5, pp. 329–354, 2013.

[19] N. Maarop, N. Mustapha, R. Yusoff, R. Ibrahim, and N. M. M. Zainuddin, “Understanding success factors of an information security management system plan phase self-implementation,” *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, vol. 9, no. 3, pp. 884–889, 2015.

[20] N.F. Fakhri and J. Ibrahim. "Information security aligned to enterprise management." *Middle East Journal of Business*, vol 10. no 1 pp 62-66,2015

[21] V. Pathari, and R.Sonar, "Identifying linkages between statements in information security policy, procedures and controls", *Inf. Manag. Comput. Secur*, vol. 20 no. 4 pp. 264 – 280, 2012

[22] M. Chander, S. K. Jain, and R. Shankar, “Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach,” *J. Model. Manag.*, vol. 8, no. 2, pp. 171–189, 2013.

[23] M. A. Alnatheer, “Information Security Culture Critical Success Factors,” in *12th International Conference on Information Technology - New Generations*, 2015, pp. 731–735.

[24] L. Yang, “Study on the improvement of the internal audit work in it environment,” in *2011 Fourth Int. Symp. Knowl. Acquis. Model*, 2011, pp. 233–236.

[25] J. Mayer and L. Lemes Fagundes, “A model to assess the maturity level of the Risk Management process in information security,” *2009 IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, no. 5, pp. 61–70, 2009.

[26] P. Choejey, C. C. Fung, K. W. Wong, D. Murray, and H. Xie, “Cybersecurity Practices for E-Government : An Assessment in Bhutan,” in *10th Int. Conf. E-bus.*, 2015, pp. 1–8.

[27] K. Randeree, A. Mahal, and A. Narwani, “A business continuity management maturity model for the UAE banking sector,” *Bus. Process Manag. J.*, vol. 18, no. 3, pp. 472–492, 2012.

[28] N. H. Mansol, N. Hayaati, M. Alwi, and W. Ismail, “Embedding Organizational culture values towards successful Business Continuity Management (BCM) implementation,” in *2014 International Conference on Information Technology and Multimedia (ICIMU)*, 2014, p. 31–37.

[29] N. Bajgoric, “Business continuity management: a systemic framework for implementation,” *Kybernetes*, vol. 43, pp. 156–177, 2014.

[30] N. Aisyah, S. Abdullah, N. L. Noor, E. Nuraihan, and M. Ibrahim, “Contributing Factor To Business Continuity Management (BCM) Failure – a Case of Malaysia Public Sector,” in *Proceedings of the 5th International Conference on Computing and Informatics, ICOCI*, 2015, no. 077, p. 530–538.

[31] W. S. Chow and W. O. Ha, “Determinants of the critical success factor of disaster recovery planning for information systems,” *Inf. Manag. Comput. Secur.*, vol. 17, pp. 248–275, 2009.

[32] ISO/IEC 27002:2013 “Information technology – Security techniques – Code of practice for information security management” Geneva: ISO, 2013.

[33] S. Woodhouse, “Critical success factors for an information security management system,” in *5th Int. Conf. Inf. Technol. Appl. ICITA* 2008, pp. 244–249.

[34] M. Nancylia, E. K. Mudjtabar, S. Sutikno, and Y. Rosmansyah, “The measurement design of information security management system,” in *Telecommunication Systems Services and Applications (TSSA), 8th International Conference*, 2014.

[35] J. M. Hagen, E. Albrechtsen, and J. Hovden, “Implementation and effectiveness of organizational information security measures,” *Inf. Manag. Comput. Secur.*, vol. 16, no. 4, pp. 377–397, 2008.

[36] Zammani, M. and Razali, R. “Information security management success factors”. *Advanced Science Letters*, vol. 22, no. 8, pp.1924-1929, 2016

[37] S. Dzazali and A. H. Zolait, “Assessment of information security maturity: An exploration study of Malaysian public service organizations,” *J. Syst. Inf. Technol.*, vol. 14, pp. 23–57, 2012.

[38] Q. Hu, T. Dinev, P. Hart, and D. Cooke, “Managing employee compliance with information security policies : The Critical role of top management and organizational culture,” *Decision Sciences Journal* , vol. 00, no. 00, pp. 1–45, 2012.

[39] K. Krippendorff, "Content Analysis: An Introduction to Its Methodology", 3rd ed., Los Angeles, USA: SAGE Publications, 2013.

.

.