Contributing Factors for Successful Information Security Management Implementation: A Conceptual Model

Rahayu Hashim, Rozilawati Razali

Abstract: ***Information security management is a comprehensive information management technique that is used as a strategic approach for addressing risks, breaches of information security incidents that threaten confidentiality, integrity and availability. Information Security Management has become an important initiative for organizations to manage and protect their information assets responsibly and effectively. One of the common problems in organisations is the lack of guidelines for the implementation of an effective and efficient ISM. As a result, incidents and threats to organisations continue to rise causing the organisations to suffer losses and their reputation jeopardised. Therefore, this study aims to identify the success factors that could assist organisations in the implementation of ISM. The methodology used in this study is a qualitative research technique whereby a theoretical study was reviewed through existing literature together with ISM international standards, frameworks, guidelines, best practices and previous studies in the IS field. The data from the theoretical study was then analysed using content analysis. Twelve success factors were identified and the relationships between these factors are proposed. These factors are derived and grouped into aspects of people and process. Each factor contains its own element that represents either the role to play or the activity to perform. In the process aspect, the factor was further divided into the Plan, Do, Check and Act phases. The aspects and factors were then formulated as a conceptual model for information security management implementation. The conceptual model acts as a guideline and an initial setup for organisations intending to implement ISM in the future. Furthermore, it could also act as a reference for future research in the information security domain.***

Keywords: information security, information security management, information security management implementation, success factor.

I. INTRODUCTION

Information security (IS) is the protection of information from a variety of threats to ensure business continuity, maximise the return on investment and business opportunities, and reduce business risks [1]. A lack of IS will result in security breaches and attacks on the information of the organisation. Hence, information security management (ISM) is applied in order to ensure IS. The main goals of ISM are to prevent and reduce
damage to assets, retain the information of the organisation, and strengthen the IS of the organisation.

Revised Manuscript Received on December 05, 2019.
***** Correspondence Author
Rahayu Hashim*, Research Centre for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Email: ayurahayu@siswa.ukm.edu.my
Rozilawati Razali, Research Centre for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Email: rozilawati@ukm.edu.my

However, IS incidents, risks, and threats are still prevalent in organisations [2]. One of the reasons for these phenomena is that the organisations do not know how to successfully implement ISM [3]. Besides, current ISM practices are less effective [4], [5] and do not suit the current needs of organisations [3], [6] which cause organisations to continue to face IS risks. Moreover, organisations tend to emphasise on the technical aspects,
[7] hence ignoring the non-technical aspects in implementing ISM [5]. As a result, the organisations' critical information has been attacked, leading to triggering major disruptions and enormous financial damage [8] and reputation loss [9]. Based on these facts, this study was conducted to determine the success factors of ISM implementation.

This paper is divided into five sections. Section II presents the available literature in the ISM field. Section III describes the research methodology of the study. Section IV discusses the results and discussion. Finally, section V outlines the conclusion and suggestions for future research.

II. LITERATURE REVIEW

This section discusses the success factors in implementing ISM as highlighted in previous related studies together with the available international standards, frameworks, best practices and guidelines in ISM, namely ISO/IEC 27001:2013 [10], COBIT 5 for Information Security [11], ITIL [12], and NIST 800-100 [13], respectively. ISO/IEC 27001:2013 was developed in 2013 by the International Organisation for Standardization (ISO). This standard consist of a framework used to guide any organisation in implementing ISM by designed to protect the organisation's critical information [14]. ISO/IEC 27001:2013 are intended to continuously manage and operate the information security system, in terms of technology, management and hardware for information security purposes to ensure the confidentiality, integrity and availability of the organisation's information. [1]. Meanwhile, the Control Objectives for Information and Related Technology (COBIT) 5 framework helps with the governance and management of IT processes [15]. As a framework of information technology (IT) governance, COBIT 5 is focused on developing clear policies and good practices for IT security and control for worldwide endorsement by commercial, governmental, and professional organisations

[16]. The National Institute of Standard and Technology (NIST) introduced a guideline, known as NIST 800-100, to help organisations improve their ISM. This guideline focuses on assisting managers in establishing and implementing an ISM programme. NIST 800-100 and COBIT 5 are the best practices for the organisations to apply and comply with their ISM practices. The Information Technology Infrastructure Library (ITIL), started as a collection of books that covered good practices [4]. Subsequently, it was transformed into a framework of best practices, which support organisations in managing their IT services effectively [17].

In the preliminary stage of ISM, the top management of the organisation [5] needs to formulate sound strategic planning [6], [8], [11], [13], [18] including the business processes [7] and the organisation's IS requirements [6]. Realistic strategic planning needs to allocate enough resources [6], [18], [19] including financial resources [5] and human resources [3], [20]. Human resources which are needed as drivers of ISM activities and processes have substantial impacts on the ISM success [6]. Financial resources are required for the purpose of maintaining the existing assets, purchasing new assets or new technologies to achieve better productivity and improve performance, conducting courses or training for the technical team and auditors, and carrying out awareness programmes to all parties in the organisations [6], [19]. To complement the strategic planning, organisations need to create a strategic document at the highest level [21], known as the Information Security Policy (ISP) [11], [20], [22]. This document contains clear objectives, rules, and instructions and defines the roles and responsibilities of the parties involved [23]. Also, it is necessary to establish a committee in ensuring that the parties are clear about the tasks and responsibilities that need to be handled [21]. In ensuring the strategic direction of ISM is guided and the objectives of the ISM implementation are achieved, leadership [3], [21] and high commitment [20] from the top management are essential to motivate, influence, and encourage cooperation among the teams in the organisation [6].

The planning made by the top management should be carried out by the coordinating team [19] through management planning [10], [22], [24]. The team will coordinate and manage the matters related to the organisation's ISM, including the key documents and activities. This team acts as the intermediary between the top management, technical team, and audit team. The team is responsible for organising ongoing training and awareness programmes [5], [22], [23] managing resources appropriately, coordinating the ISM documents, and presenting the ISM implementation reports to the top management [19]. Ongoing training and education [23] will ensure the dedicated team members are competent by developing the right skills [6] with specific competencies concerning their job scope [19] and technology management is in place [6]. In addition, a culture of information security will be created with awareness programs among organisational members [25]. The awareness programme is to inform the organisational members so that they will understand the importance of IS and the level of security policy required by the organisation, thus driving them to act according to the security policy [9], [23]. Therefore, the coordinating team must be knowledgeable about ISM and committed to coordinating the ISM activities in addition to possessing excellent communication skills [19] when communicating at all levels.

Risk management is a core process in ISM [23], [26]. Risk management commences with two major components, which are risk assessment and risk treatment activities [23], [27] that are carried out by the technical team. Risk management is a protection strategy based on a risk assessment to avoid recurring risks. The main objectives of risk management are to identify, analyse, and assess the organisation's IS risks and then introduce proper controls to reduce and controls the risks [10]. Risk assessment is a fundamental first step that identifies assets and threats, examines the effects and probabilities of emerging risks [24], [28], and determines the level of risk [23]. Based on the risk assessment analysis, the technical team [22] will design appropriate risk controls [27] to control the operations so that the risk recurrence can be avoided [22]. In addition to the risk management process, business continuity management (BCM) is also a major contributing factor to the success of ISM [19], [21]. The main objective of BCM is to ensure that the organisation can continue to operate during or after an incident or a disaster. BCM is derived from risk assessment and business impact analysis [13]. The organisation should conduct periodic simulations or tests to ensure that the BCM works properly in the event of an incident or a disaster [20], [21].

IS document management [29] is crucial in the management of the operations, work processes, and technology [30]. The main objective of IS document management is to assist in the formulation of policies, operating procedures [31], guidelines, work instructions, control sensitive information [21] as well as the main functions and controls concerning the organisation's IS [32]. Therefore, a correct and clear document should be developed in ensuring that the work processes are more systematic [33]. This document is used as a guide by the process manager and the parties involved in carrying out the work operations and in developing the controls [10], [13] related to the IS procedure [34]. ISM technical and operational implementation is carried out by the technical team. This team is responsible for ensuring that the work processes are transformed into IS document. The IS document is usually developed by the technical team based on experience [11] and work routine. After developing the IS document, the team is responsible for implementing the ISM processes and controls by following the steps written in the IS document and procedures [19]. Thus, the procedures should be clear, complete, and communicated to the ISM team. The preparation and updating of the documented procedures and controls should be standardised and reviewed in terms of their suitability and adequacy [10]. Therefore, the technical team must have sufficient levels of experience, technical knowledge related to IT skills [19], and communication skills [11] to perform the processes and activities as well as handling the technology management in implementing ISM [6].

In ensuring that the organisation implements and

maintains the ISM properly, compliance tests are applied at regular intervals. Compliance is an organisational action that involves an internal audit technique in ensuring that the IS quality assurance is maintained [23]. Internal audit is a systematic process and a disciplined approach to assessing and enhancing the effectiveness of risk management and control [3], [19], [32]. It is a governance process that determines the organisational performance against non-compliance, errors, and inefficiencies [35]. Effective internal audit includes audit planning, execution, and reporting on the audit findings [10]. Audit planning involves collecting the organisation's background information and evaluating the resources and skills required to perform the audit. The data collection and processing activities are necessary for preparing the audit findings [18]. The audit findings and proposed corrective actions are reported to the top management, and issues raised by the audit team require the agreement by the top management. The audit team is an independent party that provides integrity assurance and consultation, designed to add value and improve organisational performance and operations. The audit team should be knowledgeable about the people and processes to be audited and skilled in analysing logic, evaluating business data and processes, and communicating at all levels within the organisation [19]. In strengthening the skills and the credibility of the internal audit team, technical competencies and ongoing training are essential as the basis for effective internal audit [35].

Continuous improvements should be implemented to ensure that incidents, threats, and risks are always controlled. Improvement is an ongoing process that ensures the organisation's IS achieves its desired level and the service quality is continuously enhanced [10], [12], [21]. The organisation shall continually improve the suitability, adequacy, and efficiency of its ISM [10]. The two important elements of improvement are corrective and preventive actions as well as effectiveness review [23]. Corrective and preventive actions are taken based on the non-conformance highlighted in the audit report [13]. The organisation should identify the cause of non-conformance and study the steps that should be taken to control, prevent, and correct it so that there will be no recurrence [10], [12]. The corrective action should be appropriate to the effects and impacts on the non-compliance identified in the audit report [11]. Meanwhile, the effectiveness review should study the rules, laws, procedures, and operating processes in order to improve the controls [11], [13].

The top management should be more active in leading the management review at planned intervals [10] by providing feedback for future ISM improvements [29]. The purpose of the management review is to monitor the organisation' ISM and ensure that its objectives remain relevant, adequate, and effective for the organisation's goals, issues, and risks. An effective management review should explore opportunities for continual improvement [29] including ISP [11], review the information security objectives, inputs and outputs [25] and consider the current issues and trends that are affecting the external and internal aspects of the organisation[10]. The outcomes of the management review should relate to the strategic decisions that have material impacts in terms of continuous improvement opportunities and any need for change to the ISM.

III. METHODOLOGY

The methodology used in this study was a qualitative method. This study applied qualitative research methods to allow the researchers to get detailed data by gaining a deeper understanding of the subject issue. Figure 1 illustrates the research design, which involved the main activities in this study.

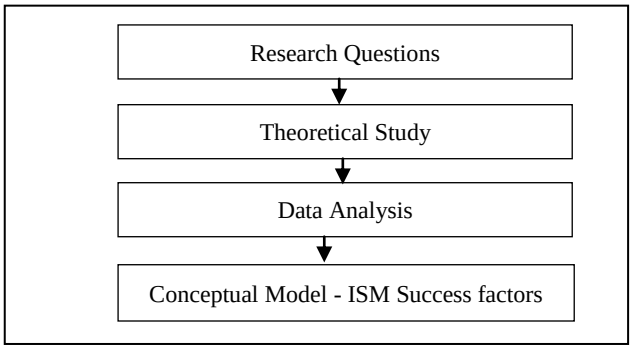

Figure 1: Research Design

A. Research Questions

The purpose of this study was to identify the contributing factors of ISM implementation by answering the following research question (RQ):

RQ1: What are the success factors that contribute to the implementation of ISM?

RQ2: How are those factors connected to produce a conceptual model?

The RQs above is to find the success factors (RQ1) and interconnection between the factors to form the conceptual model (RQ2). This RQs is a basic guideline for data collection during theoretical studies.

B. Theoretical Study

The theoretical study is to study the existing literature by obtaining data through sources derived from published and unpublished documents through various databases. The keywords used in the search include "information security", "information security framework", "information security management", "information security management framework", "best practices information security management", "information security standard", "information security management standard", "critical success factors in information security management" and "success factors in information security management". The document search was conducted in the following online databases: IEEE Explore, ACM Digital Library, Science Direct, Scopus, Springer Link, Google Scholar, and ISI Web of Science Proceedings. Two criteria were considered in the data search:

i. The articles were from 2010 until 2018 that covered both journals and conference proceedings and
ii. The articles describe the factors that contribute to the success of ISM

C. Data Analysis

The data obtained from theoretical studies was interpreted using content

analysis. Data were analysed and transcribed using content analysis starting from the word level to sentences and paragraphs through the process of identifying and categorising [36]. Content analysis is a qualitative research technique that analyses data from oral, written, and visual communication messages [37].

IV. RESULTS AND DISCUSSION

Table 1 shows the comparison of ISM factors that were included in five previous studies involving the ISM international standards, frameworks, best practices and guidelines. The table lists out the success factors along with their elements, categorised into People and Process aspects. Four factors are included in the People aspect, emphasising the key players in carrying out the ISM implementation activities. Meanwhile, the Process aspect outlines the key practices and activities that must be performed by the key players in the ISM programme.

Apparently, there is a new factor identified namely the coordinating team. The coordinating team comprises three important elements that support the team: knowledge, communication skill and commitment. The coordinating team is responsible in organising all the activities related to the organisation's ISM. The importance of this team is apparent when it acts as a liaison between the top management, technical team and the audit team.

Almost all previous studies agreed that the top management, strategic planning, management planning and risk management are the main success factors for ISM implementation. They also support the importance of technical and operational implementation, business continuity management, and compliance as the contributing factors towards a successful ISM implementation. However, the previous studies paid little attention to factors such as technical team, audit team, improvements and management review. The technical team is the implementer who performs technical operations in the process related to the ISM while the audit team is an independent body that conducts audits to ensure that the quality assurance of the organisation complies with IS procedures, controls, processes and activities in compliance with established standards. Besides, improvements are the continuous process to ensure service process and progress of organisation are monitored while management review is the monitoring activity conducted by top management to ensure the consistency, adequacy, effectiveness and the smooth running of ISM.

All ISM international standards, frameworks, best practices and guidance agree that the technical team is a factor in ISM implementation. ISO 27001, Cobit 5 and NIST SP 800-100 cover almost all factors in people and process aspects. These three standards, frameworks and guidelines are ideal guides for organisations in developing ISM when focusing more on information security in their implementation. However, the NIST SP 800-100 guidelines is more specific to its use, as a guide to the organisation's managers. In contrast to ITIL, ITIL places less emphasis on documentation. This situation causes many organisations to spend more money when it comes to consulting services in implementing ITIL in their organisations.

Through previous studies, only one article covers almost all aspects except for the improvement and management review factors. All articles agreed that commitment of top management in People aspect is an important element. Top management commitment is essential to assist in ISM implementation through adequate financial allocation, support and monitoring of ISM organisations. However, the experience element is not important in the technical team. Experience required by a technical team to develop IS documents. In the early stages, the technical team develops work-related documents by transforming practical practices into documented forms. Without experience, it is difficult for the technical team to develop ISP, IS documents and procedures for reference and guidance in ISM implementation.

From the observation above, there is an imbalance in the success factors between ISM standards, frameworks, best practices and guidelines compared to previous studies. The ISM standard, framework, best practices and guidance place equal emphasis on the People and Process aspects. Meanwhile, previous studies focus on the Process aspect more compared to the People aspect.

Figure 2 depicts a conceptual model of implementing ISM. The conceptual model is derived from the factors categorized into two main aspects: People and Process. There are twelve factors, along with the corresponding elements. Respective people will carry out their activities through process indicated by the arrows. In the Process aspect, the factors are categorized into Plan, Do Check and Act phases. The details of each factor and its corresponding elements according to the respective aspects are described in the following paragraphs.

A. People

The people aspect is the driving force behind the ISM activities and processes, which encompasses the planning, implementation, improvement, and monitoring of the ISM processes. These key players can be a sole individual or a team. The four factors identified in the people aspect are top management, coordinating team, technical team, and audit team. These four factors are discussed in detail below.

1. Top Management

The solid support from the top management is a key pillar of ISM. The leadership and commitment shown by the top management are two of the key drivers of success in implementing ISM. Direct involvement by the top management not only facilitates the smooth implementation of the organisation's ISM but also motivates staff to work for it. The top management is responsible for leading the organisation and working together to ensure the ISM objectives are met. Putting ISM at the forefront of the organisation shows a strong commitment by the top management. Suggestions and decisions are made, followed by instructions for all levels of the organisation to follow. Monitoring is also done by the top management to ensure the ISM implementation is always on the right track.

2. Coordinating Team

The coordinating team should have comprehensive knowledge about the ISM implementation. The team is responsible for coordinating all the ISM-related activities so that ISM can be implemented according to the plan. The team also serves as a liaison between the senior management, technical team, and audit team. Therefore, this team should have effective communication skills to ensure that information is delivered correctly to all the levels involved. The team also

requires extensive knowledge of governance to manage the organisation's ISM efficiently and effectively. High commitment is needed from the team members as the implementation of ISM takes a long time.

3. Technical Team

The technical team, as the implementer, plays a major role in the ISM implementation process. The technical team should have extensive and up-to-date knowledge of technical and security issues. Moreover, the team should be skilful in identifying risks, handling technology, managing documents, controlling and monitoring incidents and disasters, and analysing the effectiveness of controls in driving improvements. Besides, the technical team's experience will help in handling security issues as their daily tasks. Accepting the new directed tasks will improve their knowledge, skill, and experience as well.

4. Audit Team

The audit team is an independent body or organisation responsible for the quality assurance process, which ensures that the procedures, IS control, processes and activities comply with the organisation's standard through the auditing process. The auditor should be knowledgeable about the people, processes, and procedures in the organisation that needs to be audited. This team needs to have profound skills in data analysis and audit process. Furthermore, effective communication skills will assist the auditor in obtaining the necessary information during the audit and informing the results to the relevant parties. Also, the audit team's commitment is required in ensuring that the audit implementation meets the objectives, timelines, and organisational requirements.

B. Process

Process refers to specific, detailed activities and practices that consist of a series of actions or steps in order to achieve a particular end. The process aspect should be handled by the people in the organisation. In this study, the process aspect consists of eight factors, which are strategic planning, management planning, risk management, technical and operational implementation, business continuity management, compliance, improvements, and management review.

5. Strategic Planning

Strategic planning is the highest level of planning that is pioneered by top management. The plan is developed holistically, systematically, and clearly to support the overall strategic implementation and organisational performance activities by providing the ISP. The ISP needs to be scrutinised to ensure alignment with the scope and constraints of the organisation. As a top-level document, the ISP contains guidelines and regulations that need to be complied with and disseminated to all levels of the organisation. The policy should explain the objectives of IS along with the duties and roles of the parties involved. In this regard, the establishment of a committee will facilitate better implementation of the duties and responsibilities of the parties. Sufficient resource allocation includes financial and human resources is the key driver of the ISM activities. A stable financial position is needed for critical decision making and activities that cover human resource management and technological needs. Allocation of financial resource is crucial to maintain existing assets, acquire assets and up-to-date technology, pay for the manpower cost, and cover the cost of performing IS activities and changing current trends.

6. Management Planning

Management planning is driven by strategic planning through the coordinating team. The effectiveness of ISM is supported by optimal management resources in line with current trends. In Management planning financial allocation approved by top management must be managed wisely and optimally. Financial resource should be manage efficiently regulated based on the implementation of ISM activities, technology requirements, and teamwork requirements and expertise. Human resource refers to individuals or teams that are engaged in the ISM activities. In ensuring that management plans successfully achieve the organisation's IS goals, training and awareness programmes should be held. These programmes will improve the level of competence and awareness of the coordinating team, technical team, and audit team. The main objective of the training programmes is to ensure the teams have the knowledge and skills for every task handled. Meanwhile, awareness programmes are carried out to ensure that the people in the organisation know about the IS aspects encompassing the policies, threats, risks, and roles and responsibilities.

7. Risk Management

Risk management is a crucial ISM activity. Focusing on risk management will help organisations to identify the strengths and weaknesses of their ISM and take steps to improve them in the future. Risk management is the process of measuring and analysing the level of risk of an asset as well as taking appropriate actions to control the risk. Risk assessment and risk treatment are two important risk management activities. Risk assessment is a process that recognises assets and threats including the expected frequency and possibility of risk occurrence by identifying the risk acceptance criteria, deciding the risk levels, and defining the impacts. Risk treatment activities are formulated to implement control (safeguard) or protection strategies based on a risk assessment decision. An effective control strategy that can be implemented is to accept the risks and their assets without protection (safeguard) or control, prevent or avoid risks, apply controls to mitigate risks, or transfer risks to third parties. However, the selection of controls is based on management practices that are optimally based on resources and control of security solutions in line with the organisation's business activities and current trends.

8. Technical and Operational Implementation

The implementation of systematic operations will ensure that the organisation's business goes smoothly. Operational and technical documents are included in the IS procedures developed based on the ISP. As a guide in the operational implementation, the IS procedure needs to be complete and clearly details out the procedures or steps that explain how to implement the IS process. The technical team is responsible for the preparation of documents related to operations and technical handling procedure. The operational implementation covers technical processes and operations such as infrastructure and technology, which are documented based on work experience, current work processes, and work procedures that meet the safety features. This document serves not only as a guideline in operations but also as a third-party reference in carrying out the relevant tasks.

9. Business Continuity Management

Business continuity management (BCM) is an essential activity that ensures the information system services or processes can operate as usual during and after an incident or a disaster within the prescribed time frame. A comprehensive business continuity plan will activate resources, processes, and responsibilities to manage and control incoming incidents or disasters. When incidents and disasters occur, the technical team will be responsible for addressing these problems. Simulations and testing should be carried out to test the validity, effectiveness, accuracy, and availability of the business continuity plan. BCM needs to be reviewed at regular intervals based on technological changes, current issues on security continuity controls, as well as changes in operations, organisations, and legislation.

10. Compliance

Compliance is achieved through audits, which ensure that the ISM implementation is in line with plans. Through the auditing process, the ISP, procedures, controls, processes and activities will be assessed, measured, and supervised. Two major components in audit are the audit programme and audit reporting activity. An audit programme consists of audit planning and audit implementation. At this stage, the selection of auditors, scope, methods, and audit criteria should be carefully considered. Meanwhile, the audit reporting process refers to reporting to the top management based on the recorded audit results. Corrective and preventative actions based on the audit findings will be conducted by the technical team.

11. Improvements

Improvements are an ongoing process to ensure the service process and progress are monitored, corrective and preventative actions are taken, there are controls over the IS effectiveness, and performance evaluation and risk management are conducted. The technical team is responsible for ensuring the improvements are carried out. Two important tasks regarding improvement are corrective and preventive actions and the effectiveness review. For the corrective and preventative actions, the organisation should review the effectiveness of controls through periodic self-assessments and auditing. The corrective actions taken shall be consistent with the findings of non-compliance in the audit report. Meanwhile, the effectiveness review is done by examining the corrective and preventive actions on controls. The effectiveness review evaluates the corrections and the need to eliminate the cause of non-conformance so as not to repeat or allow it to happen elsewhere. Effectiveness reviews are conducted by reviewing non-conformances and their causes, the potential for recurrence, and the effectiveness of any corrective actions made. The effectiveness of controls can be assessed through the performance appraisal of the documentation procedures, operations, and continuous treatment of risks.

12. Management Review

The management review is an assessment and monitoring activity that ensures the consistency, adequacy, effectiveness and the smooth running of ISM. The top management is responsible for ensuring that the management reviews are done within the specified timeframe. The two key activities to be considered in the management review are identifying changes to the internal and external issues and examining the opportunities for improvement. Research on external and internal issues is made concerning the goals and issues that can affect the ability to achieve the desired ISM outcomes. It includes an understanding of stakeholders' confusion and expectations as well as the relationship and dependency between the organisation's activities and the activities conducted by other organisations. Meanwhile, examining the opportunities for improvement considers the current issues including the latest technological changes and current IS trends. Finally, decisions are made as a sign of approval, support, and direction for further action.

Table 1: Comparison of the Success Factors for the Implementation of Information Security Managements

Aspects	Factors	Elements	ISO 27001	COBIT 5	ITIL	NIST SP 800-100	Zammani & Razali (2016)	Singh & Amitabh Ojha -2014	P. Drljaca & Latinović (2016)	Prislan et al. (2017)	Chowdhury & Salahuddin -2017
People	Top Management	Leadership	√	√			√			√	
		Commitment	√	√		√	√	√	√	√	√
	Coordinating Team	Knowledge					√				
		Communication Skill					√				
		Commitment					√				
	Technical Team	Knowledge	√	√	√	√	√		√		
		Skill	√	√	√	√	√	√			
		Experience	√	√		√					

	Audit	Knowledge	√	√			√				
	Team	Skill	√	√		√	√				
		Commitment	√	√			√	√			
	Strategic Planning	Information Security Policy	√	√	√	√	√	√		√	
		Resource Allocation	√	√	√	√	√	√			√
		Committee Establishment	√	√	√	√	√	√			
	Management Planning	Resource Management	√	√	√	√	√	√			
		Training & Awareness Programmes	√	√	√	√	√	√		√	√
	Risk Management	Risk Assessment	√	√	√	√	√	√	√	√	
		Risk Treatment	√	√	√	√	√	√			
	Technical & Operational Implementation	Preparation & Execution of Operational Document	√	√	√	√	√			√	
		Technology Handling	√	√	√	√				√	√
	Business Continuity Management	Incident & Disaster Recovery Plan Implementation	√	√	√	√	√	√			
	Compliance	Audit Programme	√			√	√	√			
		Audit Reporting	√			√	√		√		
	Improvements	Corrective & Preventive Actions	√	√		√					
		Effectiveness Review	√	√	√	√					
	Management Review	Current Issues Identification	√	√	√	√					
Process		Opportunities for Improvements Evaluation	√	√	√	√					

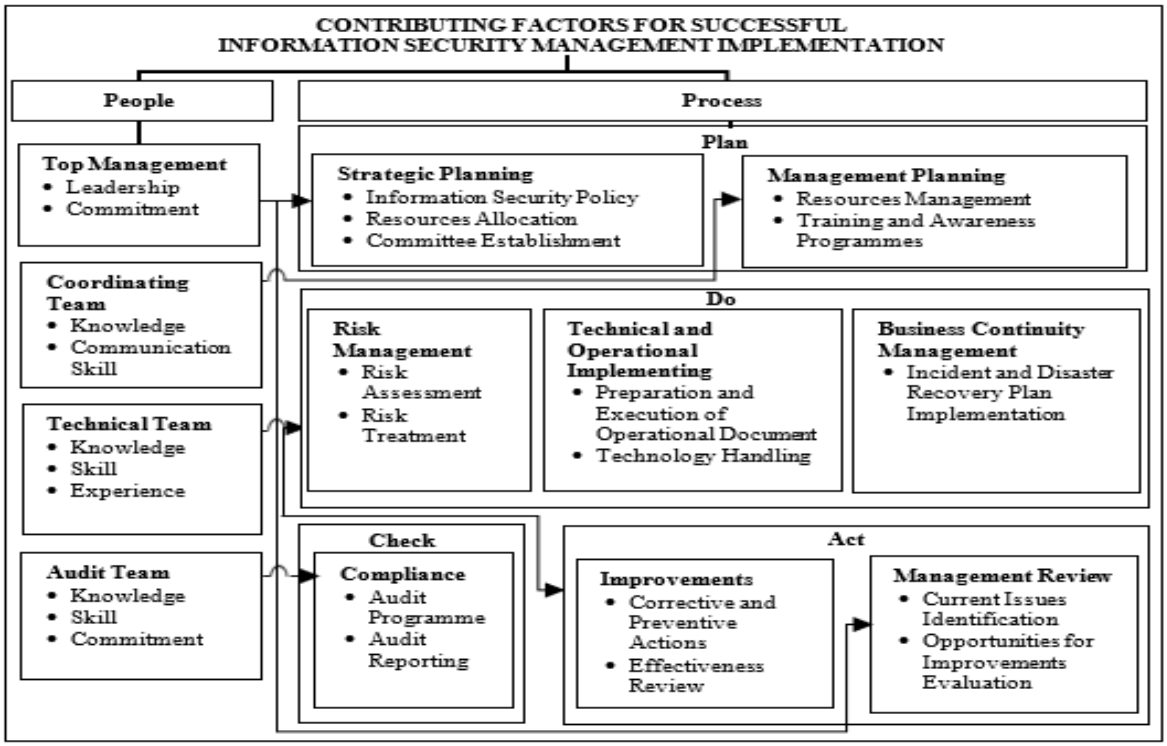

Figure 2: A Conceptual Model of Implementing Information Security Management

V. CONCLUSION AND FUTURE WORK

This study has outlined twelve success factors that influence the ISM implementation together with their corresponding elements. These success factors were derived from ISM international standards, frameworks, best practices, guidelines and studies on general information on ISM implementation. In this study twelve factors were identified, namely; top management, coordinating team, technical team, audit team, strategic planning, management planning, risk planning, technical and operational implementation, business continuity management, compliance, improvement and management review. The conceptual model proposed comprises of these factors which were then categorized into people and process aspects along with their elements. This model also reflects the individual's responsibility in carrying out activities in the process. For future work, this conceptual model needs to be validated through empirical studies. In the meantime, these findings could provide practitioners with preliminary guidance for the implementation of ISM. By focusing on the key players and their elements, these findings can be used as a guide for organisations to formulate their initial strategies for ISM initiatives.

ACKNOWLEDGMENT

The authors like to thank to University Kebangsaan Malaysia (UKM) for supporting this study under fund (PP-FTSM-2019).

REFERENCES

1. R. Sheikhpour and N. Modiri, "An approach to map COBIT processes to ISO/IEC 27001 information security management controls," *Int. J. Secur. its Appl.*, vol. 6, no. 2, pp. 13–28, 2012.
2. CyberSecurity Malaysia, "CyberSecurity, Malaysia 2018," 2018.
3. N. Maarop, N. Mohd Mustapha, R. Yusoff, R. Ibrahim, and N. M. Mohd Zainuddin, "Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation," vol. 9, no. 3, pp. 884–889, 2015.
4. V. R. Palilingan and J. . Batmetan, "Incident Management in Academic Information System using ITIL Framework Incident Management in Academic Information System using ITIL Framework," 2018, pp. 0–9.
5. K. Prislan, B. Lobnikar, and I. Bernik, "Information Security Management Practices: Expectations and Reality," *Adv. Cybersecurity 2017*, no. November, pp. 5–22, 2017.
6. S. Chowdhury and K. M. Salahuddin, "A Literature Review of Factors Influencing Implementation of Management Information Systems in Organizations," vol. 12, no. 8, pp. 72–79, 2017.
7. A. Ghazvini, Z. Shukur, and Z. Hood, "Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 8, pp. 410–423, 2018.
8. I. Bernik and K. Prislan, "Measuring information security performance with 10 by 10 model for holistic state evaluation," *PLoS One*, vol. 11, no. 9, pp. 1–33, 2016.
9. D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Comput. Secur.*, vol. 70, pp. 663–674, 2017.
10. S. ISO, "ISO/IEC 27001:2013," 2013.
11. ISACA, *COBIT 5 for Information Security*. 2012.
12. L. itSMF UK, *An Introductory Overview of ITIL 2011*. 2012.
13. P. Bowen, J. Hash, and M. Wilson, *Information Security Handbook : A Guide for Managers*, no. October. 2006.
14. Z. Mukhtar and K. Ahmad, "Internal Threat Control Framework Based On Information Security Management System," *J. Theor. Appl. Inf. Technol.*, vol. 70, no. 9056, pp. 924–925, 2014.
15. T. Huygh, S. De Haes, A. Joshi, and W. Van Grembergen, "Answering Key Global IT Management Concerns Through IT Governance and Management Processes: A COBIT 5 View," *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, vol. 9, 2018.
16. I. N. Putra, A. Hakim, S. H. Pramono, and H. Tolle, "Adopted COBIT-5 framework for system design of Indonesia navy IS/IT: An evaluation," *Int. J. Appl. Eng. Res.*, vol. 12, no. 17, pp. 6420–6427, 2017.
17. M. Gërvalla, N. Preniqi, and P. Kopacek, "IT infrastructure library (ITIL) framework approach to IT governance," *IFAC-PapersOnLine*, vol. 51, no. 30, pp. 181–185, 2018.
18. D. P. Drljaca and B. Latinović, "Frameworks for Audit of an Information System in Practice," *JITA - J. Inf. Technol. Appl. (Banja Luka) - APEIRON*, vol. 12, no. 2, 2016.
19. M. Zammani and R. Razali, "An Empirical Study of Information Security Management Success Factors," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 8, pp. 904–913, 2016.

20. A. N. Singh and M. P. G. Amitabh Ojha, "Identifying factors of ' organizational information security management ,'" *J. Enterp. Inf. Manag.*, vol. 27, no. 5, pp. 644–667, 2014.
21. S. Stahl, K. Pease, and D. Lam, "The Citadel Way to Information Security Management," no. April. 2017.
22. M. Burdon, J. Siganto, and L. Coles-Kemp, "The regulatory challenges of Australian information security practice," *Comput. Law Secur. Rev.*, vol. 32, no. 4, pp. 623–633, 2016.
23. M. A. Alnatheer, "Information Security Culture Critical Success Factors," *2015 12th Int. Conf. Inf. Technol. - New Gener.*, pp. 731–735, 2015.
24. 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. 644–667, 2014.
25. H.-L. Hai and K.-M. Wang, "The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability," *African J. Bus. Manag.*, vol. 8, no. 17, pp. 705–716, 2014.
26. Z. Ismail, M. Masrom, D. S. Hamzah, and Z. Mohammed Sidek, "Information security considerations for higher learning institutions," in *2010 International Symposium on Information Technology*, 2010, vol. 3, pp. 1537–1542.
27. A. Alwi and K. A. Zainol Ariffin, "Information Security Risk Assessment for the Malaysian Aeronautical Information Management System," in *Conference, CRC Cyber Resilience*, 2018, pp. 1–4.
28. G. Wangen, N. Hellesen, H. Torres, and E. Braekken, "An Empirical Study of Root-Cause Analysis in Information Security Management Gaute," *11th Int. Conf. Emerg. Secur. Information, Syst. Technol.*, no. c, pp. 26–33, 2017.
29. R. Tatiara, A. N. Fajar, B. Siregar, and W. Gunawan, "Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001," *J. Phys. Conf. Ser.*, vol. 978, no. 1, 2018.
30. R. Alavi, S. Islam, and H. Mouratidis, "A conceptual framework to analyze human factors of Information Security Management System (ISMS) in organizations," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8533 LNCS, pp. 297–305, 2014.
31. H. Elachgar and B. Regragui, "Information Security , new approach," pp. 51–56, 2012.
32. B. Borgman, S. Mubarak, and K.-K. Raymond Choo, "Cyber security readiness in the South Australian Government," *Comput. Stand. Interfaces*, vol. 37, pp. 1–8, Jan. 2015.
33. M. A. Mohamad Stambul and R. Razali, "An assessment model of information security implementation levels," *Proc. 2011 Int. Conf. Electr. Eng. Informatics*, no. July, pp. 1–6, 2011.
34. T. Lucio-Nieto, R. Colomo-Palacios, P. Soto-Acosta, S. Popa, and A. Amescua-Seco, "Implementing an IT service information management framework: The case of COTEMAR," *Int. J. Inf. Manage.*, vol. 32, no. 6, pp. 589–594, 2012.
35. M. Alkebsi and K. A. Aziz, "Information Technology Usage, Top Management Support and Internal Audit Effectiveness," vol. 8, no. 123–132 (2017) Special Issue, pp. 123–132, 2017.
36. M. R. Che Abdul Rahman, "Practical Challege of Content Analysis: An Illustrative Example from Recording IC Informaton in the UK's Companies Annual Reports," *Asian J. Account. Res.*, vol. Vol 1, no. 2, pp. 32–43, 2016.
37. K. Krippendorff, *Content Analysis: An Introduction to Its Methodology*. 2018.

AUTHORS PROFILE

Rahayu Hashim is a researcher at the Research Centre for Software Technology and Management (SOFTAM), Faculty of Information Science and Technology, (FTSM), Universiti Kebangsaan Malaysia (UKM), Malaysia. She holds bachelor's in Information Technology from University Technology MARA (UiTM), Malaysia. Currently, she is a candidate master's in Information Technology (Management Information System). Her research interest is Information Security Management (ISM).

Rozilawati Razali (Ph.D.) is an Associate Prof. and researcher at the Research Centre for Software Technology and Management (SOFTAM), Faculty of Information Science and Technology, (FTSM), Universiti Kebangsaan Malaysia (UKM), Malaysia. She received her PhD in Computer Science from University of Southampton, United Kingdom. Prior to joining Universiti Kebangsaan Malaysia, she used to work in industry as a Software Engineer. Her research interests include Requirements Engineering, Empirical Software Engineering, Software Management and Information Security Management. She is also recognized as a Certified Tester - Foundation Level (CTFL), Certified Tester Advanced Level, Test Manager (CTAL-TM) by International Software Testing Qualifications Board (ISTQB) and Certified Professional Requirement Engineer (CPRE) by the International Requirement Engineering Board (IREB).