*International Journal of Engineering & Technology*, 7 (4.35) (2018) 544-550

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***



# The Role of Organizational Factors to the Effectiveness of ISMS Implementation in Malaysian Public Sector

**Noralinawati Ibrahim[1]*, Nor'ashikin Ali[2]**

[1 2] *College of Graduate Studies, Universiti Tenaga Nasional, 43000 Kajang, Selangor, Malaysia*
**Corresponding author E-mail: noralinawati.ibrahim007@gmail.com*

## Abstract

Many organizations have initiated efforts to manage the security of their information by implementing an Information Security Management System (ISMS). ISMS is a set of guiding principles for managing organization's confidential information and minimizing risk for business continuity. However, information security remains a major challenge and the effectiveness of ISMS is often argued due to the exposure of organizations to information security threats, incidents, risks, and vulnerabilities. One of the reasons is the unsuccessful ISMS current practices amongst all employees and lack of ISMS awareness in organizations. Several critical success factors are identified from previous studies that lead to the ISMS success. Among the success factors are human, organizational and technical factors. This study explores the factors that contribute to the success of ISMS and identify the organizational factors that relate to the information security effectiveness. The conceptual model is developed and will be tested within the Malaysian Public Sectors (MPS) organizations to provide a preliminary insight, understanding, and clarification of the organizational factors, together with the significant effects on ISMS effectiveness. This study used a quantitative approach and data collected from personnel's that were directly involved with the ISMS implementation through a questionnaire survey.

***Keywords***: *Information Security Management System; Public Sector; Information Security; Organizational Factors; Success Factors*

## 1. Introduction

Information in the context of people, technology and process elements plays an important role in managing an organization's business operations [1]. Due to the valuable information to the organizations and overall business operations, it could be exposed to information security risks or threats that might cause potential losses in terms of financial, legal and reputations [1]–[5]. Thus, in order to ensure that information remains secure and continues to provide beneficial support to an organization's business operations, several key features of this information need to be preserved. These features include confidentiality, integrity and availability (CIA) that requires to be managed properly and make it worthwhile for the organization [6].

By adopting an official guideline, organizations can ascertain their commitment to address any information security related issues in business practices [7]. Consequently, many organizations have implemented the Information Security Management System (ISMS) involving information security processes, policies, procedures, controls and organizational structures as an effort in handling their information [8]. An ISMS is based on risk approach and governing all types of security measures in achieving the CIA of information assets [6]. The main objective of ISMS is to ensure that the security objectives are aligned with the business needs of the organization. This is important in order to protect the information assets, through management and technical actions against unauthorized disclosure by irresponsible people [7]. Apart from that, ISMS is a comprehensive approach to protect information assets from any intrusion, damage or abuse, which involves implementation of all security requirements and controls in the organization [9].

In order to facilitate the development of ISMS in organizations, ISO 27001 standard has been adopted by organizations worldwide [10]. A growing number of literatures have highlighted the issues concerning the information security in a technological context, but due to the increasing number of security incidents, researchers' have begun to explore the management role in ISMS. Within the Malaysian context, ISMS implementation in Malaysian Public Sector (MPS) has started since 2010. Accordingly, Malaysian Administrative Modernization Planning and Management Unit (MAMPU) has advised all agencies under public sector to get the ISO/IEC 27001:2005 ISMS certification, to ensure continuity in the service delivery with minimum impact of interruption in the business operations [11]. Despite the efforts made by the MPS to provide an efficient service delivery through the ISMS implementation, information security still remains a serious challenge and the effectiveness of ISMS has often been questioned due to the exposure of organizations to information security threats, incidents, risks and vulnerabilities. One of the reasons is due to the unsuccessful in carrying out ISMS practices amongst all employees and lack of ISMS awareness in organizations. The current ISMS approach in the MPS merely involves the Information Technology (IT) department and more towards the technical oriented tasks without involving the entire departments in the organization. Therefore, there is a need to assess the success factors that cause this phenomenon from the organizational perspective rather than looking only at the technical aspects.

Gathered from the previous analyses, the study discovered several key factors from various perspectives that contribute to the success of ISMS such as technological, strategic, tactical, operational, technical, organizational, formal, informal, people and processes [2], [9], [12], [13]. However, there is little evidence that empha-

**Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.**

sizes solely on the relationship of organizational factors and the significant effect on the ISMS effectiveness in the public sectors, especially in MPS. Hence, this research intends to fill up this gap by exploring the key factors that contribute to the success of ISMS, focusing on the role of organizational factors. The assessing factors will help MPS to understand the employees' intention towards ISMS compliance and will guide organizations to improve ISMS implementation in the future.

## 2. Methodology

This study was conducted in two (2) stages:
The first stage: A systematic approach and extensive search were carried out on a high-quality information systems journals databases including Emerald Insight, IEEEXplore, ScienceDirect, ACM Digital Library and Scopus. In addition, Google Scholar search engines and online articles related to information security were utilized using the same keywords. The searching keywords are: "ISMS", "information security", "information security management system", "information security effectiveness", "critical success factors", "organizational factors" and some other keywords. As a result, a total of 153 articles related to information security in general, has been downloaded for further processing. However, this study is limited to the critical success factors (CSFs) related to the success of the ISMS and information security effectiveness. Thus, nine (9) papers have been selected as the main references.
The second stage: The CSFs in existing studies were extracted to examine the organizational factors. The proposed constructs were extracted to identify five top constructs and the conceptual model was developed along with the hypotheses. Thus, these organizational factors as the independent variables will be tested in MPS to explore the role and its significant effect on the ISMS effectiveness. For this study, a quantitative approach was employed to collect data from personnel who directly involved with ISMS implementation through a questionnaire survey.

## 3. Literature Review

Information Security can be defined as a well-protected of information assets to ensure the CIA of information through risk management and application of security controls. CIA is the key elements of the Information Security aspects to avoid the threats and maintain business continuity. Confidentiality means protecting the information from unauthorized exposure by ensuring that the information is shared only to the permitted users. Meanwhile, integrity concerns the information accuracy including completeness, preserving its sources and precision from being modified, deleted or added; and availability means that information is allowed to be accessed by the right person and at the right time [14], [15].
Information security has traditionally been technology oriented [16]. In spite of many technical leading-edge solutions, information security remains as a challenge to manage due to threats and vulnerabilities found as a result of the emergence of IT/ICT media. Besides the technological aspects, non-technological aspects of information security should also be considered due to employees being a significant threat and essential resources to prevent incidents from happening [16]. This suggests that management of information security should be emphasized to incorporate business process and organizational issues beyond the technical controls [17].
Information security involves all employee's accountability from the top management, all management levels and the general employees [18]. Information security has a very essential role to support the activities of the organization. Hence, it is crucial to implement ISMS in organizations for managing information assets effectively. Through ISMS, organization puts in place a set of policies to define, structure, develop and sustain security of their information assets [19]. To this effect, it is crucial to implement the ISMS in order to protect the organization from potential threats and security breaches.

### 3.1. Information Security Management System (ISMS)

Effective information security management is increasingly attracting stakeholders attention since it has been a vital strategic subject in organizational management [5]. For this study, ISMS is defined as managing an organization's sensitive information through systematic policies and procedures to minimize risk and to ensure business continuity.
The core objective of ISMS is to ensure the information security objectives are aligned with the organization's business needs [20]. Apart from that, ISMS goal is to ensure that all personnel understand the information security policy, procedures, standards and other requirements up to an appropriate level when managing the organization's information assets. Successful implementation of ISMS is governed by analyzing and applying appropriate security controls as in ISO/IEC 27001 to safeguard the organizational information assets [10].

### 3.2. ISO/IEC 27001 Standard

This standard emerged in 1995 as BS-7799, and further revised in 2005 and the latest by 2013. The ISO 27001 standard has been in earlier versions ISO/IEC 27001:2005, which focused on the CIA protection of the information. The newer versions of ISO/IEC 27001:2013 replace the old version by focusing on information from a business perspective to ensure security objectives is aligned with the business needs of the organization [20]. ISO/IEC 27001 Information Security Management System (ISMS) – Requirements is the certification standard. Organization gets the certification to increase safeguard level of their information and information systems. Therefore, an ISO 27001 certification can be used as a mean of maintaining an effective ISMS in the public view, including current and future clients, and Industry Regulators.
Nowadays, ISO 27001 has already become a widely regarded standard for information security by organizations as the basis for the management of the organization's policy and information security implementation by both commercials and the government. It is being implemented across various business sectors be it small, medium and large organizations. Accordingly, in line with the implementation of ISMS, the Malaysian government have adopted this standard to preserve information and manage weaknesses in the delivery of IT-based services [13], [21]. In Malaysia, as of December 2015, 240 enterprises and organizations including government agencies have been certified by ISO/IEC 27001 [22].

### 3.3. ISMS in Malaysian Public Sector

ISMS was implemented in MPS since 2006 with the National Registration Department (NRD) was the first certified agency in 2008. The adoption of ISO/IEC 27001:2013 is one of the important approaches to deliver an efficient public services to the citizens [21]. The awareness of information security is important in the MPS, which then brings the MPS to include information security in one of The Public Sector ICT Strategic Plan (PSICTSA) strategic cores. The PSICTSA is a 5-year plan (2016-2020) that outlines the strategic direction of the implementation of ICT practices and policies in the public sector. From the six Strategic Thrusts in PSICTSA, ISMS falls under the Strategic Thrust 3: Optimize Shared Services and Strengthen Cyber Security.
The challenges in ISMS implementation can come from various aspects including individuals, managerial and organizational issues [13]. One of the key challenges is to recognize how organizational, technical and individual factors together, influencing information security outcomes in an organization [23]. According to Dzazali et al. [24], the challenges faced by the MPS in managing

information security are related to risks that have an impact on public confidence, national power, national security and service delivery. Key findings from The Malaysian Computer Emergency Response Team (MyCERT) indicated that, a total of 7,962 incidents in 2017 based on General Incident Classification Statistics [25]. Malicious codes, frauds and intrusions were among the top incidents reported to Cyber999, the helpline center for cyber incidents managed by MyCERT.

According to Tu and Yuan [5], identifying critical success factors is important to implement an effective ISMS in the organization. Finding by Zammani and Razali [2] also claimed that the lack of understanding of the success factors and lack of awareness on information security is the key factors to be emphasized for the ISMS effectiveness. Failing to understand these factors can cause a burden to government agencies because they have to allocate huge investment yearly for ISO/IEC 27001 certifications and yet the effectiveness of the ISMS still cannot be improved. Furthermore, lack of awareness and oversight of the vital factors may hinder the organization's efforts to understand the full benefits of ISMS. Therefore, there is a need to identify what are the factors that affect the success of ISMS implementation.

## 4. Critical Success Factors Contributing to the Success of ISMS

The Critical Success Factors (CSFs) can be defined as "the limited number of areas in which satisfactory results will ensure successful competitive performance for the organization" [26]. Defining the factors behind the successful implementation of ISMS has become a major research question in previous research. Thus, identifying CSFs that contribute to the success and effective ISMS can narrow the gap between literatures and the current practices of ISMS.

Effective information security entails focal point on identifying the CSFs on carrying out ISMS. In addition, organizations can streamline information security with business goals and improve forthcoming security, investment and policy enforcement preservation [12]. Based on the literatures, there are various CSFs of ISMS within an organization and for the purpose of this study, the CSFs are referred to as factors. Table 1 summarizes the factors that contribute to the success of ISMS discovered by previous researchers [2], [5], [9], [12], [13], [20], [27]–[29].

CSFs of ISMS implementation have been investigated from several diverse point of view. This study identified several CSFs related to the success of ISMS from the previous nine (9) studies. Among the finding of CSFs, organizational factor is one of the elements that gives an impact on employee compliance towards information security. The study by Ernest Chang and Ho [28] found that there were significant impacts between organizational factors such as environment uncertainty, IT competence of business managers, type of industry and size of organization, and the effectiveness of information security management.

In another study, Narain Singh et al. [20] categorized various organizational information security management functions into tactical, strategic and operational levels. Meanwhile, N. Waly et al. [30] discovered organizational factors, training factors and employee behavioral factors influenced the security breaches. Furthermore, Munira et al. [29] stated that the top management involvement and participation is one of the organizational factors that has an effect on the information security governance. In this regard, organizational factors are one of the utmost important issues to be looked into when implementing ISMS. Thus, the aim of this study is to determine the organizational factors for ISMS effectiveness in MPS domain.

## 5. Organizational Factors

A successful information security management can be seen as what the organization should do as an obligation due to the information security is an organizational and social problem [31], [32]. Organizational support originates from the organizational factors, which are interrelated to the organization structure involving all level of employees and managerial decisions of information security [33].

This study focuses on one of the CSFs that has the most significant effect on the effectiveness of ISMS implementation, which is the organizational factors. In a previous study conducted by Kankanhalli [27], the author proposed an integrative model that relates organizational factors and stressed on applying the controls of information security within organizations. The author concluded that a stronger management support initiates the engagement in more preventive efforts, compared to organizations with a weaker support from the top management.

Organizational factor can be regarded as the characteristics of an organization that might have a significant impact on their decision such as top management support, organizational size and technology readiness [34]. The challenge in implementing ISMS is to get management commitment and awareness in tackling the insider threats [18]. Experts now realize that organizational factor plays an important role and can lead to improvements in implementing and establishing ISMS [35]. Thus, to manage the problem of security breaches effectively, it is essential to focus on organization rather than to human factors [15].

In a different study, Ernest Chang and Ho [28] examined that the organizational factors influence the adoption of BS7799, an information security management (ISM) standard. From their 59 surveys on various organizations in Taiwan, the author concluded that organizational factors such as environmental uncertainty, IT competence of business managers, organization size and type of industry significantly influenced the implementation of ISM. In other studies, it is shown that the environmental uncertainty involving industry environment and macro environments such as competitors' behavior, technology rapid change, security requirements of customers' and changes in regulation have effects on security management [33]. In addition, the policy development, compliance, awareness and implementation of best practices, are organizational factors for basic measurements for information security [32], [36]. Literatures showed that ISMS implementation is heavily influenced by organizational factors and need to be explored.

## 6. Identifying The Organizational Factors to be Examined

The conceptual model and hypotheses were developed from the literature findings by extracting the CSFs in existing studies to develop an understanding of the organizational factors. Nine (9) studies were referred to as the main literature because these scholars have outlined various CSFs that have an impact on the effectiveness and success of ISMS. Based on the nine (9) studies in Table 1, the organizational factors have been examined from the list of CSFs, as illustrated in Table 2 to develop a construct. Hence, for this study, the constructs were calculated to extract the top five (5) constructs the organizational perspectives as shown in Table 3.

Table 3 shows the organizational factors as the independent variables in this study, which include: (1) Information Security Policy, (2) IT Competency, (3) Management Commitment, (4) Information Security Awareness, and (5) Information Security Standard Compliance.

A study by Alavi et al. [37] indicated that organizations often overlook the human factors for effective information security. The author concluded that human factors played a major function and lead people to make an error. Many security incidents are due to the human troubles who neglect the information security policy within their organizations rather than any technical problems. It should be noted that in spite of significant innovations in the tech-

nical solutions, organizations are still confronted with the security breaches. Many researchers claimed that the security violation was not related to technology but usually, occur because of non-technical in nature. As Eminağaoğlu et al. [38] noted, the success or failure of information security management in organizations depended on people. Most of the security breaches are not only because of technology but associated more or less with humans.

**Table 1:** List of ISMS Success Factors in Organization

| Source | | [27] 1. | [28] 2. | [5] 3. | [20] 4. | [12] 5. | [2] 6. | [13] 7. | [9] 8. | [29] 9. |
|---|---|---|---|---|---|---|---|---|---|---|
| **No.** | **Factors** | | | | | | | | | |
| 1 | IT Competencies/Information Security Training | | / | / | / | / | / | | | |
| 2 | Industry Type | / | / | | | | | | | |
| 3 | Uncertainty Environment | | / | | | | | | | |
| 4 | Organization Size and Type | / | / | | | | | | | |
| 5 | Top Management Support/Management Commitment/Organizational Support | / | | / | / | / | / | / | / | / |
| 6 | Business Alignment | | | / | | | | | | |
| 7 | Information security policy/ Information security procedures | | | / | / | | / | | / | |
| 8 | Information security awareness/ Organizational Awareness | | | / | / | / | / | | / | |
| 9 | Information security culture | | | | / | | | | | |
| 10 | Information security audit | | | | / | | / | | | |
| 11 | ISM best practices/Compliance with IS International Standard/Law Enforcement and Compliance | | | / | / | / | | | / | |
| 12 | Asset management | | | | / | | | | | |
| 13 | Information security incident management | | | | / | | | | | |
| 14 | IS Security Architecture | | | | | / | | | | |
| 15 | Business Connections | | | | | / | | | | |
| 16 | IS Security Strategy | | | | | / | | | | |
| 17 | Dynamic Evaluation of Information Security Effectiveness / Performance Evaluation | | | / | | / | | | | |
| 18 | Risk Assessment Process/Risk Management | | | / | | / | / | | | |
| 19 | Information Security Integration | | | | | / | | | | |
| 20 | Project Accomplishment | | | | | / | | | | |
| 21 | Budget/Resources Planning | | | | | / | / | | | |
| 22 | ISM Team | | | | | | / | | | |
| 23 | IS Audit Team | | | | | | / | | | |
| 24 | Employee/Job Responsibilities/Motivation | | | | | | / | | / | |
| 25 | Third Parties Compliance | | | | | | / | | | |
| 26 | Business Continuity Management | | | | | | / | | | |
| 27 | Implementer Competency | | | | | | | / | | |
| 28 | Implementer Commitment | | | | | | | / | | |
| 29 | Using the services of the information security external advisors | | | | | | | | / | |

**Table 2:** List of Organizational Factors

| **Organizational Factors** | **Number of cited** | **Source** |
|---|---|---|
| IT Competencies/Information Security Training | 5/9 | [28], [5], [20], [2], [12] |
| Industry Type | 2/9 | [27], [28] |
| Uncertainty Environment | 1/9 | [28] |
| Organization Size and Type | 2/9 | [27], [28] |
| Top Management Support/Management Commitment/Organizational Support | 8/9 | [27], [5], [20], [12], [2], [13], [9], [29] |
| Business Alignment | 1/9 | [5] |
| Information security policy/ Information security procedures | 4/9 | [20], [2], [9], [5] |
| Information security awareness/ Organizational Awareness | 5/9 | [5], [20], [12], [2], [9] |
| Information Security Culture | 1/9 | [20] |
| ISM best practices/Compliance with IS International Standard/Law Enforcement and Compliance | 4/9 | [20], [12], [9], [5] |
| IS Security Strategy | 1/9 | [12] |
| Dynamic Evaluation of Information Security Effectiveness / Performance Evaluation | 2/9 | [12], [5] |
| Information Security Integration | 1/9 | [12] |
| Project Accomplishment | 1/9 | [12] |
| Budget/Resources Planning | 2/9 | [12], [2] |
| ISM Team | 1/9 | [2] |
| IS Audit Team | 1/9 | [2] |
| Employee/Job Responsibilities/Motivation | 2/9 | [2], [9] |
| Third Parties Compliance | 1/9 | [2] |
| Business Continuity Management | 1/9 | [2] |

**Table 3:** Construct of Organizational Factors

| Constructs | Number of cited out of 9 studies |
|---|---|
| Information Security Policy | 4/9 |
| IT Competency | 5/9 |
| Management Commitment | 8/9 |
| Information Security Awareness | 5/9 |
| Information Security Standard Compliance | 4/9 |

The literature highlighted that the problem remained for years. Therefore, the exploration of the organizational factors is essential to improve the information security management. Thus, from the CSFs that contributed to the success and effective ISMS, five (5) organizational factors were identified to test the significant effect of that factors on the effectiveness of implementing ISMS. These five (5) factors were chosen, as it is able to represent most of the organizational factors from the past studies.

## 7. Development of Conceptual Model

The conceptual model with five (5) construct as per Figure 1 is derived based on the literature reviews. The conceptual model is developed in order to investigate the significant effects of organizational factors on the ISMS effectiveness. The model has five constructs: information security policy, IT competency, management commitment, information security awareness and information security standard compliance. The model will be tested in the MPS organization to identify the relationship between organizational factors and the effectiveness of ISMS implementation in an organization.

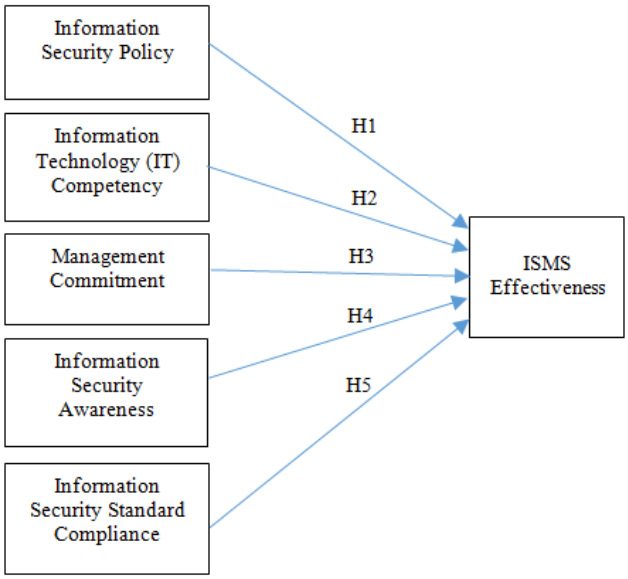



**Figure 1:** Conceptual Model of ISMS Effectiveness

### 7.1. Information Security Policy

Information Security Policy is the main or top-level policy, which outlines other support policies for ISMS implementation. Content guides of information security policy document are stated in the ISO/IEC 27002. Information Security Policy can be defined as a declaration of employees' roles and responsibilities to defense the IT resources of their organizations [39]. Information security policy documentation is supposed to be reviewed regularly to guarantee that it remains up to date and pertinent to the information security objectives including employees, stakeholders and external parties [2], [40].

A well-written information security policy must be clear and brief, easy to understand and free from legal and technical jargon [16]. In addition, it must be practical, functional, well disseminated to employees and enforceable as policies and procedures associated with information security often vary depending on the workplace changes on an ongoing basis.

Recent research indicated that the compliance of employee behaviors against information security policy from the social-organizational views reduce the risk of information security violations in organizations [41]. Therefore, the following hypothesis is formulated:

H1: Information Security Policy has a significant effect on the effectiveness of ISMS implementation.

### 7.2. Information Technology (IT) Competency

Dealing with the whole aspects of ISMS, IT competency plays an important key role in effective information security management and enables the organization to design, arrange, execute, and make an investment pertaining to the information security [5], [28]. IT competency refers to the interrelated ability of constant elements that are essential in meeting IT or business objectives [5]. Employees are required to have sufficient skills to deal with the requirements of information security policy [37]. In addition, employees with adequate competence in managing information security issues are more likely to comply with organizational information security management [41].

Studies have found that there are two categories of people exists when involving ISMS implementation in the general government organizational structure [2]. The author highlighted that ISMS processes such as planning, implementing, monitoring and improvising ISMS embrace the individual and teams in the organization. It consists of the Top Management, Employees, Third Parties, Coordinator Team, Information Security Team and the Information Security Audit Team. All of these people is required to have the competencies including knowledge, leadership, responsibility, skills, cooperation and awareness associate to the information security policy, threats, risks and controls. For instance, employee as an individual should aware and comply with the policies and procedures as stated in the Information Security Policy, in order to reduce security incidents. While, the Information Security Team is a team consists of several nominated staffs involved in most of information security activities with knowledge, expertise, commitment, willingness and teamwork to run the ISMS processes. Furthermore, scholars also have emphasized the importance of integrating a strategy with technical competence to improve security alignment between social and organizational component [42]. Moreover, the heightening of IT competency can help strengthen the strategies of organizational information security management. Therefore, the following hypothesis is formulated:

H2: IT Competency has a significant effect on the effectiveness of ISMS implementation.

### 7.3. Management Commitment

Prior studies had paid most attention on management support, which can be seen very essential to the success of information security in the organization including actively supports, the commitment of funding, and organizational structuring [1], [27], [33], [42]. Allocation of resources including human and financial, promotion of buy-in and highlighting the importance of security to other groups in the organization is one of the ways of support that can be demonstrated by the top management [42]. Moreover, the success of ISMS is strongly related to the top management knowledge, leadership and their commitments to the organization. Therefore, it is important that the top management is clear about their roles and understanding of information security objectives, so that they are able to establish an ISMS governance in order to shape the security compliance behavior among the employees [2]. Similarly, research finding by Hu et al. [23] concluded that the top management plays a proactive role and have a significant impact in forming employee's compliance behavior.

A formal information security organizational structure that centralized all security functions is enormously crucial to the success of ISMS in order to develop and deploy organization-wide policies and standards [42]. Thus, there is a need for a stronger management commitment to ensure that a clear direction and strong support against the security efforts. Therefore, the following hypothesis is formulated:

H3: Management commitment has a significant effect on the effectiveness of ISMS implementation.

### 7.4. Information Security Awareness

Information security awareness can be defined as the extent to which employees understand the importance of information security, the realization of the levels of information security in the organization, knowing their individual roles against security, and acts accordingly [43]. Given the broad increase in reliance on IT systems and information stored electronically, organizations should focus on human's attention to the security process through education, training, and awareness rather than focusing purely on technologies and policies [44]. This is fundamental to ensure that all employees' acts in an appropriate manner to keep sensitive information secure and aware of the possible security threats.

Having and promoting information security awareness programs in place is one of the socio-organizational roles to increase the information security compliance in organizations [45]. The wide-ranging awareness programs features including web portals, advertisement campaigns, guidelines booklets, posters, awareness training workshops, newsletters, security awareness programs, forums to enable users to interact, alert and news sections, online surveys and statistics [42], [44]. All relevant groups in the organization including all managers and employees should be catered with adequate training and awareness in order to protect information assets effectively.

Employee's skills and understanding on information security are increased through trainings, while awareness programs ensure that they are aware of their roles and responsibilities in handling threats as well as understanding the information security policy [2]. The study by N. Waly et al. [30] examined that it is vital to increase the effectiveness of trainings and awareness programs by inspiring the employees and improving their motivation to practice the skills learned in their workplace. Therefore, it should be noted that a sufficient awareness of the roles and responsibilities among all level of employees is needed and this is a focal point of attention in ISMS [37]. Therefore, the following hypothesis is formulated:

H4: Information Security Awareness has a significant effect on the effectiveness of ISMS implementation.

### 7.5. Information Security Standard Compliance

Information security compliance refers to the information security standards and policies applied by the organization in order to safeguard the information assets [14]. One of the key factors to the successful ISMS is the effectiveness of information security compliance to the international standard. An international standard is a benchmark to regulate information security governance since information security has a very essential role in supporting the activities of the organization [46]. There are many related information security governance standards that are widely used by organizations such as BS 7799, ISO 27001, PCIDSS, ITIL and COBIT [47]. Amongst them, ISO 27001 is the most widely used standard in the ISMS domain.

It is widely recognized that, through the compliance of ISO 27001 Standard, the organization may fulfill and get certified in increasing protection level of their information [48]. Apart from that, adopting a compliance standard increases users confidence, trust and satisfies the security requirements of organizations of public services [14]. Information security audit is the necessities in ISO 27001 Standard. The audit process will establish the compliance to the information security policy, procedures, processes, controls, and activities that can be monitored, measured and evaluated [2]. Thus, with the periodical audit, all the process is continuously monitored, performance was measured, ISMS was reviewed effectively and finally, the application of corrective and preventive actions are taken to achieve continual improvement of information security practices [49]. Therefore, the following hypothesis is formulated:

H5: Information Security Compliance has a significant effect on the effectiveness of ISMS implementation.

## 8. Discussion

By applying the critical success factors approach, this study explored the factors that contributed to the success of ISMS and identified the organizational factors related to the information security effectiveness. By reviewing the literatures in the information security field, five (5) organizational factors are identified and the relationship of these factors with the ISMS effectiveness is proposed. These five (5) factors were selected because they represent most of the organizational factors from the previous studies.

The results from the literatures reveal that information security policy, IT competency, management commitment, information security awareness and information security standard compliance are the organizational factors for effective information security management. Thus, a conceptual model along with the hypotheses were proposed and will be tested in MPS to investigate the significant effect of organizational factors on the effectiveness of ISMS.

## 9. Conclusion

The role of organizational factors need to be explored to ensure that employees comply with the information security policy, standard, procedures, laws and regulation in order to reduce security breaches and increase business performance in the organization. Previous studies clearly stated that organizational factors might influence the ISMS effectiveness. Thus, the researcher tried to identify these factors and the significant effect on the success of ISMS.

Understanding the significant effect of the organizational factors would assist MPS organizations in formulating a more effective information security strategic planning and designing the deployment of information security awareness tailored for all employees, from top management to the subordinates.

## Acknowledgement

Special appreciation to my supervisor, Associate Prof. Dr. Nor'ashikin Ali for her supervision, guidance and continuous support throughout the preparation of this paper. Special thanks to the Public Service Department (PSD) for sponsoring my Master's studies at UNITEN.

## References

[1] S. Posthumus and R. Von Solms, "A framework for the governance of information security," *Comput. Secur.*, vol. 23, no. 8, pp. 638–646, 2004.

[2] M. Zammani and R. Razali, "An Empirical Study of Information Security Management Success Factors," *Adv. Sci. Lett.*, vol. 22, no. 8, pp. 904–913, 2016.

[3] R. Razali, "An assessment model of information security implementation levels," *Proc. 2011 Int. Conf. Electr. Eng. Informatics*, no. July, pp. 1–6, 2011.

[4] M. R. Fazlida and J. Said, "Information Security: Risk, Governance and Implementation Setback," *Procedia Econ. Financ.*, vol. 28, no. April, pp. 243–248, 2015.

[5] Z. Tu and Y. Yuan, "Critical Success Factors Analysis on Effective Information Security Management : A Literature Review," *Inf. Secur. Manag.*, pp. 1–13, 2014.

[6] G. Pavlov and J. Karakaneva, "Information Security Management System in Organization," *Trakia J. Sci.*, vol. 9, no. 4, pp. 20–25, 2011.

[7] J. H. P. Eloff and M. Eloff, "Information security management: a new paradigm," in *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, 2003, pp. 130–136.

[8] W. Ismail, N. M. Norwawi, and K. Saadan, "The Challenges in

Adopting Information Security Management System for University Hospitals in Malaysia," *Proceeding Knowl. Manag. Int. Conf. 2014, Vols 1 2*, no. August, pp. 902–907, 2014.
[9] 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.
[10] ISO/IEC 27001, "ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements," *ISO/IEC 27001*. p. 23, 2013.
[11] M. MAMPU, Jabatan Perdana Menteri, "Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam," *Unit Pemodenan Tadbiran dan Peranc. Pengur. Malaysia*, vol. MAMPU.BPIC, no. November, p. 1, 2010.
[12] J. M. Torres, J. M. Sarriegi, J. Santos, and N. Serrano, "Managing Information Systems Security : Critical Success Factors and Indicators to Measure Effectiveness," *Inf. Secur. S. Katsikas, J. López, M. Backes, S. Gritzalis B. Preneel (eds.), Springer Berlin Heidelberg*, pp. 530–545, 2006.
[13] N. Maarop, N. Mustapha, R. Yusoff, and R. Ibrahim, "Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation," *World Acad.*, 2015.
[14] A. Alkalbani, "A Conceptual Framework for Information Security in Public Organizations for E-Government Development," no. 2010, 2014.
[15] N. S. Waly, *Organisational information security management: The impact of training and awareness*. 2013.
[16] M. N. Masrek, Q. N. Harun, and M. K. Zaini, "Information Security Culture For Malaysian Public Organization : A Conceptual Framework," *Proc. INTCESS 2017 4th Int. Conf. Educ. Soc. Sci.*, no. February, pp. 156–166, 2017.
[17] J. Choobineh *et al.*, "Management of information security: challenges and research directions," *Commun. AIS*, vol. 20, no. December, pp. 958–971, 2007.
[18] E. Humphreys, "Information security management standards: Compliance, governance and risk management," *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 247–255, 2008.
[19] H. Susanto, M. Almunawar, and Y. Tuan, "Information security management system standards: A comparative study of the big five," *Int. J. Electr. Comput. Sci. IJECS-IJENS*, vol. 11, no. 5, pp. 23–29, 2011.
[20] A. Narain 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.
[21] MAMPU, "Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO / IEC 27001 : 2007 dalam Sektor Awam," no. November, 2010.
[22] ISO Survey Report, "ISO Survey Report 2006-2016." 2016.
[23] 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," *Decis. Sci.*, vol. 43, no. 4, pp. 615–660, 2012.
[24] S. Dzazali, A. Sulaiman, and A. H. Zolait, "Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations," *Gov. Inf. Q.*, vol. 26, no. 4, pp. 584–593, 2009.
[25] MyCERT Incident Statistics, "Reported Incidents based on General Incident Classification Statistics 2017," *Rep. Incidents bas ed Gen. Incid. C las s ification Statis tics 2 014*, p. 11918, 2017.
[26] C. V. Bullen and J. F. Rockart, "A primer on critical success factors," *Work. Pap.*, no. 69, pp. 1–64, 1981.
[27] a Kankanhalli, "An integrative study of information systems security effectiveness," *Int. J. Inf. Manage.*, vol. 23, no. 2, pp. 139–154, 2003.
[28] S. Ernest 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.
[29] R. Munira, N. A. Molok, and S. Talib, "Exploring the Factors Influencing Top Management Involvement in Information Security," *PACIS 2017 Proc.*, 2017.
[30] N. Waly, R. Tassabehji, and M. Kamala, "Improving Organisational Information Security Management: The Impact of Training and Awareness," in *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, 2012, pp. 1270–1275.
[31] C. Hsu, T. Wang, and A. Lu, "The impact of ISO 27001 certification on firm performance," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2016.
[32] S. Ernest Chang and C. Lin, *Exploring organizational culture for information security management*, vol. 107, no. 3. 2007.
[33] R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of IT security management," *Inf. Manag. Comput. Secur.*, vol. 17, no. 1, pp. 4–19, 2009.
[34] N. Alkhater, G. Wills, and R. Walters, "Factors Influencing an Organisation's Intention to Adopt Cloud Computing in Saudi Arabia," *2014 IEEE 6th Int. Conf. Cloud Comput. Technol. Sci.*, pp. 1040–1044, 2014.
[35] B. AbuSaad, F. A. Saeed, K. Alghathbar, and B. Khan, "Implementation of ISO 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes, and Lessons Learned," in *Proceedings of the 9th Australian Information Security Management Conference*, 2011, pp. 1–9.
[36] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, 2016.
[37] R. Alavi, S. Islam, H. Jahankhani, and A. Al-Nemrat, "Analyzing Human Factors for an Effective Information Security Management System," *Stand. Stand.*, no. January 2015, pp. 1253–1278, 2013.
[38] M. Eminağaoğlu, E. Uçar, and Ş. Eren, "The positive outcomes of information security awareness training in companies - A case study," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 223–229, 2009.
[39] I. Benbasat, "Special Issue Information Security Policy Compliance : An Empirical Study of Rationality - Based Beliefs," vol. 34, no. 3, pp. 523–548, 2010.
[40] K. Höne, J. H. P. Eloff, and P. Eloff, "Information security policy – what do international information security standards say?," *Comput. Secur.*, vol. 21, no. 5, pp. 402–409, 2002.
[41] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, 2014.
[42] T. Kayworth and D. Whitten, "Effective Information Security Requires a Balance of Social and Technology Factors," *Mis Q. Exec.*, vol. 9, no. 3, pp. 163–175, 2010.
[43] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories," *African J. Bus. Manag.*, vol. 5, no. 26, pp. 10862–10868, 2011.
[44] M. Mackay, A. Maqousi, and T. Balikhina, "An Effective Method for Information Security Awareness Raising Initiatives," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 63–72, 2013.
[45] A. Alkalbani, H. Deng, and B. Kam, "Investigating the role of socio-organizational factos in the information security compliance in organizations," *Australas. Confrence Inf. Syst.*, no. 2010, 2015.
[46] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Information Security Challenge and Breaches : Novelty Approach on Measuring ISO 27001 Readiness Level," *Int. J. Eng. Technol.*, vol. 2, no. 1, pp. 67–75, 2012.
[47] H. Rehman, A. Masood, and A. R. Cheema, "Information security management in academic institutes of Pakistan," *Conf. Proc. - 2013 2nd Natl. Conf. Inf. Assur. NCIA 2013*, pp. 47–51, 2013.
[48] M. . Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard," *Int. J. Cyber-Security Digit. Forensics*, vol. 1, no. 4, pp. 280–288, 2012.
[49] D. I. Kossyva, K. V. Galanis, K. K. Sarri, and N. B. Georgopoulos, "Adopting an information security management system in a co-opetition strategy context," *Int. J. Appl. Syst. Stud.*, vol. 5, no. 3, p. 215, 2014.