TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 3266- 3275

An Empirical Exploration of Information Security Management System (ISMS) in Malaysian Public Sector: A PLS-SEM Method

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

[1,2]*College of Graduate Studies, Universiti Tenaga Nasional (UNITEN)*
43000 Kajang, Selangor, Malaysia
[1]noralinawati.ibrahim007@gmail.com
[2]shikin@uniten.edu.my

Article Info
Volume 81
***Page Number:* 3266- 3275**
Publication Issue:
November-December 2019

Article History

Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *16 December 2019*

Abstract:
Many organizations have embarked on efforts to manage their organizational confidential information by implementing an Information Security Management System (ISMS). Due to organizational exposure to the information security threats, incidents, risks, and vulnerabilities, information security issues are still a major challenge and the effectiveness of ISMS has become a key concern. To improve the effectiveness of ISMS practices in organizations, several attempts have been made in the past to study the critical success factors of ISMS. However, few studies have made attempts to focus on organizational factors, which are essential in ISMS that involve not only technical but also organizational issues. While organizational factors were given emphasis in the literature as factors that should be given attention in security practices, their empirical studies are still lacking. Specifically, little is known about how the factors from the findings of the literature such as information security policy, information technology competency, management commitment, information security awareness and information security standard compliance affect the effectiveness of the ISMS. The conceptual model was proposed and tested to employees who involved with ISMS implementation in Malaysian Public Sector. The data was assessed via Partial Least Squares Structural Equation Modelling (PLS-SEM). The results of the data analysis revealed that information security awareness and information security standard compliance had a significant effect on ISMS effectiveness.

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

I. Introduction

Due to rapid evolution of information, communication and technology (ICT), more and more information are being produced every day to assist organizations in their business operations, and thus, it has become valuable assets to organizations [1]. Furthermore, through advanced network such as Internet, more information is being shared between agencies, within an organization and even between countries. This intense sharing of information may expose to threats or risks through its contact with people, information technology, and processes. Thus, information needs to be protected; failing to protect these assets may lead to potential financial, legal, and reputational losses [1]–[5]. Protection of assets is called information security, which has become the main concern of organizations in today's competitive environment. Information security is defined based on its three characteristics: confidentiality, integrity and availability [6]. To ensure the security of information, Information Security Management System (ISMS) has been implemented as a guideline to handle any issues regarding information security. ISMS is a set of policies and procedures put in place by organizations to ensure that computer software, hardware resources and information assets are safeguarded and secured to be used [7], [8]. Its main objective is to ensure that all security measures address these three elements of information security and thus, helps to reduce the risks [7].

II. Related Work

Many attempts have been made in previous studies to address critical success factors (CSFs) of ISMS implementation as a means to further enhance ISMS effectiveness. In the past, the security issues were mainly discussed from technical perspectives [9], [10] and the attention was therefore, given to technical solutions, which were proven to be insufficient [11]. Some studies suggested that security issues should also be viewed from organizational perspectives based on the fact that security problems arise from employees behavior and the attention should be focused on organizational factors [12], [13], [14]. The recent study by [15] provided findings from their comprehensive review on the holistic approach for ISMS that highlighted the information security management should be an integration and alignment of managerial and technical activities. The existing studies on information security practices tend to focus on weaknesses in technological assets such as hardware, software, and network, and less attention are given to organizational issues such as human, policies, culture and procedures. While focusing on technical issues such as software virus protection, and firewall are critical, ignoring security breaches that may be caused by the inside may have great impact to information security in organizations. Errors from human side were highlighted in many studies such as exposing their username and password to others, opening unknown emails and their attachments, downloading software from the Internet, and leave their computers unattended [14]. External and internal security threats may be caused by human negligence or sometimes by perpetrators such as hackers or employee misconduct [16]. Thus, understanding organizational factors as the complement to technical solutions may assist organizations to further enhance their ISMS effectiveness.

While organizational factors were given emphasis in the literature as factors that should be given attention in security practices, their empirical studies are still lacking. Specifically, there is insufficient evidence on the factors such as information security policy, information technology competency, management commitment, information security awareness and information security standard compliance impact ISMS effectiveness [2], [17]–[19]. The existing studies are mainly anecdotes and some are descriptive; they do not formally test which organizational factors actually affect the ISMS. Furthermore, these factors were not empirically tested in public sectors, which may result in a lack of validated guides for security practices in public sectors. This proposed research aspires to empirically study their effects on the effectiveness of ISMS in public sectors by focusing on Malaysian Public Sectors (MPS).

In 2010, Malaysian Administrative Modernization Planning and Management Unit (MAMPU) has advised all agencies under the public sector to implement the ISMS and obtain the ISO/IEC 27001:2005 ISMS certification [20]. At present, the ISMS approach in the MPS is only implemented at Information Technology (IT) department and focuses on technical orientation tasks. To assist MPS in successful implementation of ISMS, this study aims to provide an understanding on the role of organizational factors and their significant effects to the ISMS initiatives.

A. *Organizational Factors*

Organizational factors have been argued by researchers as equally important as technological factors in the implementation of ISMS [21], [22]. Based on the findings of nine studies [2], [5], [12] [13], [17], [18], [19], [23], [24], organizational factors have been considered as one of the elements that affect employees' compliance with information security. These studies provide evidence that there is a consensus among experts that organizational factors play an important role that can lead to ISMS effectiveness. The conceptual model and hypotheses were developed by extracting the CSFs in existing studies to develop an understanding of the organizational factors [25].

B. *Conceptual Model and Hypotheses*

The conceptual model with five (5) constructs as per Fig.1 is derived from the literature findings as well as 5 hypotheses on the relationship between the constructs in the model [25]. Besides, the study by [2], found these five (5) organizational factors were amongst the CSFs that significantly impact the implementation of ISMS in MPS environment. However, the researcher empirically tested the CSFs through semi-structured interviews with experienced ISMS practitioners. The CSFs were validated by five (5) experts from the different agency who has three (3) to six (6) years of ISMS experience. The experts included one (1) Chief Information Technology Officer, two (2) Senior Information Technology Officer and two (2) Information Technology Officer. Therefore, this study refined and strengthened further by validating these five (5) factors that will be quantitatively tested through a large-scale survey in the MPS organizations. From the literature, five (5) hypotheses was formulated:

H1: Information Security Policy (ISP) significantly affects the effectiveness of ISMS

H2: Information Technology (IT) Competency (ITC) significantly affects the effectiveness of ISMS

H3: Management Commitment (MC) significantly affects the effectiveness of ISMS

H4: Information Security Awareness (ISA) significantly affects the effectiveness of ISMS

H5: Information Security Standard Compliance (ISC) significantly affects the effectiveness of ISMS

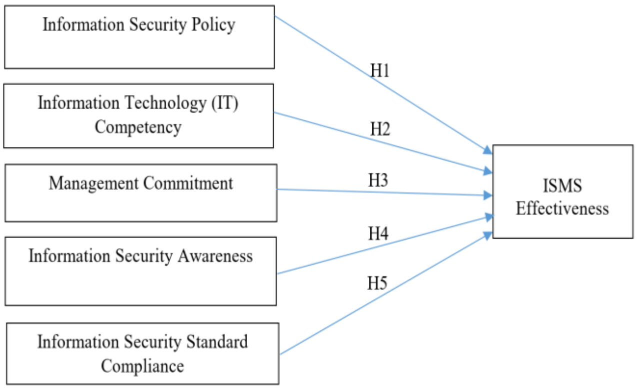
Information Security Policy
Information Technology (IT) Competency
Management Commitment
Information Security Awareness
Information Security Standard Compliance
H1
H2
H3
H4
H5
ISMS Effectiveness

Fig. 1 Conceptual Model

III. Methodology

This study aims to examine how organizational factors affect the effectiveness of ISMS implementation. As this study involves the examination of the relationships of the constructs that are examined, and the results involve the test of hypotheses that produce statistical evidence, the quantitative approach is appropriate for this study. This study used the stratified random sampling method. A sample size from 800 population were selected randomly from the entire population of MPS. The population is personnel from different target group who involved with the ISMS implementation in MPS located in Putrajaya and Klang Valley. They are Chief Information Officer (CIO), ICT Security Officer (ICTSO), ISMS Steering Committee, ISMS Implementer Committee, ISMS Lead Team, ISMS Coordinator, ISMS Auditor and employees who involved with the ISMS implementation.

Data for this study were collected by distributing questionnaire survey using Google Form to the target respondents via email and social media. The main part of the survey is the independent variables (IV - organizational factors) and dependent variable (DV – ISMS effectiveness) questionnaire that were measured using a five-point Likert scale. By end of April 2018, 138 questionnaire were used in the analysis (produced a response rate of 53.1 percent).

IV. Data Analysis And Results

Partial Lease Squares - Structured Equation Modelling (PLS-SEM) approach was employed in this study for the purpose of the measurement and structural model testing. The measurement model (outer) and the structural model (inner) are the two sub-models included in the SEM model [26]. All the data and findings gathered through quantitative methods were analysed using Smart PLS 3.

A. *Assessment of the Measurement Model*

The measurement model in PLS is assessed in terms of item reliability, internal consistency reliability, convergent validity and discriminant validity [27].

1) Item Reliability: Item reliability was assessed by examining the item loadings on their factor [28]. According to [26], the item loadings with a value of almost 0.5 or 0.6 or higher are acceptable. Items with loadings of less than 0.4 (a threshold commonly used for factor analysis results) or 0.5 should be dropped [29]. For this study, item loadings between 0.40 and 0.70 were removed from the scale by ensuring that the deleted items increased the Composite Reliability (CR) or the Average Variance Extracted (AVE) [30]. The updated model was re-assessed and the scales were revised repeatedly until the acceptable composite reliability or the average variance extracted were gained. Finally, the item loadings ranged from 0.629 to 0.908 were retained for further analysis.

2) Internal Consistency Reliability: Internal consistency of a scale refers to the degree of homogeneity among the items within the scale and is measured using Cronbach’s alpha coefficient. A level of 0.7 for the coefficient, as recommended by [31], would indicate adequate internal consistency. All reflective constructs in this model have their Cronbach’s alphas above the recommended level (refer Table I). To assess consistency reliability, the values of CR were examined. CR of each construct was evaluated based on the guideline for assessing the reliability coefficient and values of at least 0.8 are considered to be acceptable recommended by [32]. The CR values for the constructs exceeding the required minimum of 0.80, with ranged from 0.816 to 0.961 as shown in Table I. All constructs in the model above the recommended value, indicating that the measures of all the constructs had acceptable internal consistency reliability.

3) Convergent Validity: Convergent validity of the measures was assessed using three criteria proposed by [32]: (1) all reflective constructs must exceed 0.70 (internal consistency); (2) CR for each construct shall be greater than 0.8; and (3) AVE for each construct should exceed 0.50. All reflective constructs were above 0.70 and all Composite Reliability (CR) values were above 0.80. For AVE, the values were between 0.528 and 0.754, as shown in Table I, indicating the acceptable convergent validity [32].

TABLE I
RESULTS OF MEASUREMENT MODEL

Constructs	**Cronbach’s Alpha**	**Composite Reliability (CR)**	**Average Variance Extracted (AVE)**
DV	0.704	0.816	0.528
ISA	0.928	0.942	0.702
ISC	0.869	0.901	0.603
ISP	0.847	0.888	0.615
ITC	0.904	0.925	0.672
MC	0.953	0.961	0.754

4) Discriminant Validity: The next analysis, discriminant validity was assessed following [32] recommendation that the square root of AVE for each construct should exceed the correlations between the construct and other constructs in the model [32]. As seen in Table II, all constructs had good discriminant validity.

TABLE II
SQUARE ROOTS OF AVE COMPARED TO CORRELATIONS BETWEEN CONSTRUCTS

Constructs	**DV**	**ISA**	**ISC**	**ISP**	**ITC**	**MC**
DV	0.727					
ISA	0.422	0.838				
ISC	0.423	0.702	0.777			
ISP	0.279	0.708	0.650	0.784		
ITC	0.201	0.778	0.584	0.696	0.820	
MC	0.372	0.819	0.706	0.702	0.701	0.869

B. Assessment of the Structural Model

A satisfactory results for the measurement model is a prerequisite for evaluating the relationships in the structural model [30]. The structural model was tested for hypotheses significance and explanatory power. The test of the structural model and the hypotheses includes: (1) estimating the path coefficients (the strengths of relationship between the dependent and independent variables); (2) the R^2 value (the amount of variance in the dependent variables explained by the model); and (3) the statistical significance of the paths. The Smart PLS bootstrap resampling method was used to determine the significance of the paths within the structural model [33]. The resulting *p values* were interpreted as follows: (1) $p < 0.05$ implies a statistically significant relationship; (2) $p < 0.01$

implies highly statistically significant relationship; and (3) *p <0.001* implies very highly statistically significant relationship.

When an empirical *t value* is larger than the critical value, it can be concluded that the coefficient is statistically significant [30]. Basically, *t value* higher than 1.96 supposed to be significant. According to [30], "commonly used critical values for two-tailed tests are 1.65 (significance level = 10%), 1.96 (significance level = 5%), and 2.57 (significance level = 1%). Critical values for one tailed tests are 1.28 (significance level = 10%), 1.65 (significance level = 5%), and 2.33 (significance level = 1%)".

A hypothesized relationships were accepted or rejected based on magnitudes and statistical significance of the corresponding path coefficient. The total effect is the sum of direct and indirect effects. The magnitude of a path coefficient indicate the strength of the relationship between the variables and carries meaning based on statistically significance. The magnitude of 0.2 should be considered meaningful as suggested by [26]. The effect size suggested by path coefficient values was interpreted according to [34] as follows: (1) path coefficient values close to 0.5 or greater were interpreted as equivalent to large effect size; (2) path coefficient values around 0.3 were interpreted as equivalent to medium effect size; and (3) path coefficient values close to 0.1 and below were interpreted as equivalent to small effect size. From the results, out of five hypotheses, two hypotheses were supported as summarised in Table III.

C. *Variance Explained*

R^2 value of the dependent variable represent the predictive power of the structural model [26]. A larger R^2 indicates better predictive power of the model. The amount of variance are shown in Fig. 2. From five paths, two paths were significant at the 0.05 level; and three path were not practically significant. ISA and ISC were positively related to an effective of ISMS (H4 and H5 were supported), while ISP, MC and ITC was negatively related to an ISMS (H1, H2 and H3 was not supported). According to [34], the amount of variance explained (R^2) above the 10 percent cut-off is acceptable for explanatory power. Thus, the amount of variance explained (R^2 = 25.8%) for dependent variables in this model is considered acceptable.

TABLE III
SUMMARY OF THE STRUCTURAL MODEL ANALYSIS

Hypotheses	**Path coefficient (β)**	***t value***	***p value***	***Significance Level***	**Results**
H1:	- 0.035	0.254	0.800	NS	Not Supported
H2:	- 0.343	2.282	0.023	**	Not Supported
H3:	0.048	0.351	0.726	NS	Not Supported
H4:	0.484	2.183	0.029	**	Supported
H5:	0.273	2.002	0.046	**	Supported

Note: NS = Not Significant ** Statistically significant at p < 0.05

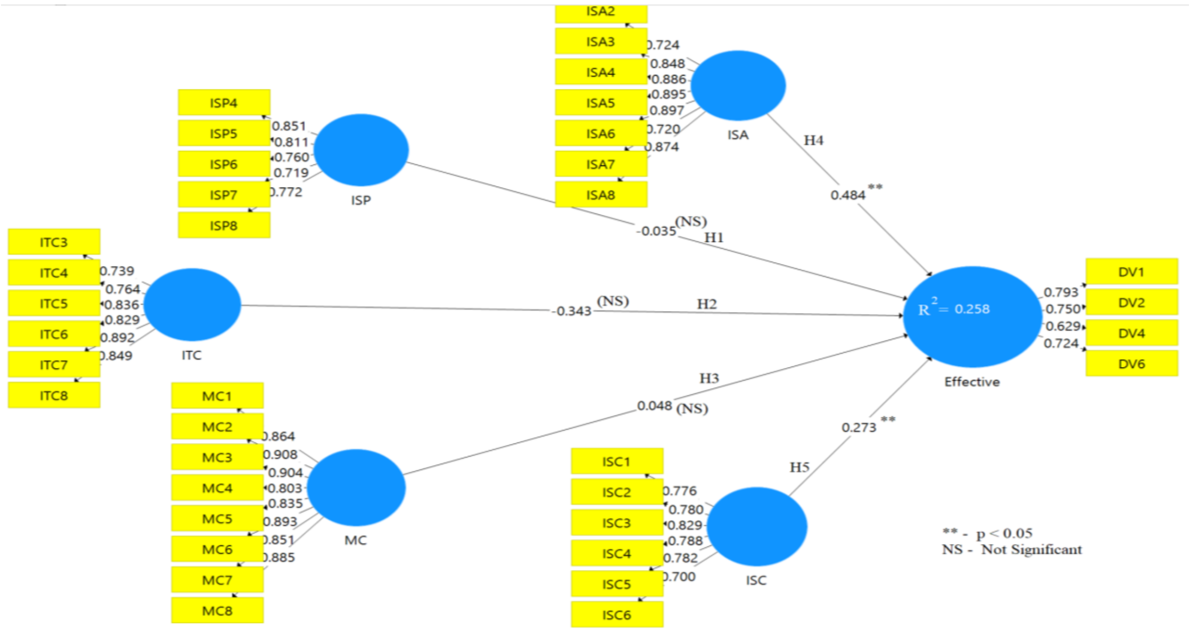

Fig. 2 Results of Structural Model Assessment

V. Discussions

From the findings, ISA and ISC were found to have significant contributions to the effectiveness of ISMS. However, ISP, ITC and MC have no significant effect to the ISMS effectiveness.

A. *ISA*

ISA had the strongest effect than the other factors. This finding is in agreement with the previous study by [18], who examined that awareness and training programs are the most important success factors in ensuring employees roles and responsibilities in handling threats. The result is also consistent with the researches about the effect of ISA in both ISMS effectiveness and employee's attitude toward compliance with the ISP [14], [35], [36], [37]. Furthermore, it verified empirical evidence that human behaviour is more important than security controls in the organization contexts [11], [38]–[40].

This indicated that the effort for ISA programmes is important in ISMS to educate personnel and must be done at all levels to improve compliance-related behaviours, be aware of possible security threats as well as have basic knowledge on information security [2].

B. *ISC*

ISC was found to have a positive direct effect and the relationship was practically significant on ISMS effectiveness. The findings are in line with [37], who proposed that ISMS complies with international information security standards can lead the organizations to adopt general rules, and enables to assess their level of safety. The results suggested that with ISC, a set of fundamental security controls was identified and introduced, that meet the minimum level of information security. In the context of MPS organizations, information security audit is one of the requirements in ISMS standard compliance that acts as a regular assessment of employees' information security knowledge and compliance. Internal as well as external audit is important for an organization to check the compliance of its security policies, guidelines, procedures, processes, controls and activities can be monitored, measured and evaluated [2], [13]. Therefore, there is an urgent need for ISC, which provide the best information security practice in the organization.

C. MC

MC was found to have no significant effect on ISMS effectiveness. This finding is not strongly supportive of previous studies [13], [18], [23], [39], [41], [42] indicates that in MPS, MC may not be critical as other factors for the success of ISMS. The finding in this study implies that the employees feel that the MC is already in place when the funding was allocated for ISMS. The result suggests that top management demonstrates their commitment through the ISMS committee, who plays a major role in coordinating ISMS activities and present the progress of ISMS to the top management [2]. Therefore, it is less influential in the effectiveness of the ISMS.

D. ISP

ISP was found to have no significant effect on ISMS effectiveness. These findings are not consistent with prior studies [2], [13], [18], [36], [43], [44]. This finding implies that there are other factors that are better than ISP to be considered in this study. ISP or known as Dasar Keselamatan ICT (DKICT) already established in MPS, which indicates that ISP is not an issue. The only suggestion is to disseminate DKICT contents among the employees in the MPS organizations, in conjunction with the ISA, so they are aware of the policies and clear of their responsibilities when managing the information assets.

E. ITC

ITC was found to have no significant effect on the ISMS effectiveness. A possible explanation is that ITC in MPS is most relevant to the ISMS implementer team in terms of IT-related-knowledge, skills, experience and abilities in handling the information security issues in general and tackling the ISMS implementation issues specifically [2]. Furthermore, in MPS, ITC was not significant due to the growing trend of outsourcing in managing the IT systems and infrastructure as well as security aspects. Therefore, ITC is not the main concern in MPS. Meanwhile, in private sector, ITC is the most important factor in achieving cost reductions and maintaining competitive edge.

F. Implications

The implications of these factors if not tested is the lack of validated guides for security practices in public sectors while MPS organizations have invested heavily in ICT assets in the form of infrastructure, technology, applications and processes.

VI. Conclusions

This study shows that the trend of information security as the responsibility of technical professionals has changed, and organizations should solve the effectiveness issue of ISMS by adopting the integrated approach that is, to include organizational factors to complement the technical solutions. ISA and ISC is the most important predictor in determining the top management decision, implies that further allocation is needed to support the ISA and ISC. The findings would be useful to the MPS to formulate a more appropriate awareness program and give a more effective focus on information security standard compliance activities that are really relevant to ISMS with the sufficient allocation. For future research, a single case study for selected ministry is suggested to achieve in depth and qualitative understanding of the ISMS effectiveness.

Acknowledgment

I would like to express my gratitude to Associate Prof. Dr. Nor’ashikin Ali for her guidance and support to complete my Master's journey. I also thank the Public Service Department (PSD) for sponsoring my studies.

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. 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.
7. G. Pavlov and J. Karakaneva, "Information Security Management System in Organization," *Trakia J. Sci.*, vol. 9, no. 4, pp. 20–25, 2011.
8. 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.
9. S. Ernest Chang and C. Lin, *Exploring organizational culture for information security management*, vol. 107, no. 3. 2007.
10. A. N. Singh, A. Picot, J. Kranz, M. P. Gupta, and A. Ojha, "Information Security Management (ISM) practices: Lessons from select cases from India and Germany," *Glob. J. Flex. Syst. Manag.*, vol. 14, no. 4, pp. 225–239, 2013.
11. N. Sohrabi *et al.*, "ScienceDirect Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.
12. 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.
13. 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.
14. 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.
15. 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.
16. S. E. Chang, "Exploring the relationships between IT capabilities and information security management Shiou-Yu Chen Chun-Yen Chen," vol. 54, 2011.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. N. S. Waly, *Organisational information*

security management: The impact of training and awareness. 2013.
23. a Kankanhalli, "An integrative study of information systems security effectiveness," *Int. J. Inf. Manage.*, vol. 23, no. 2, pp. 139–154, 2003.
24. R. Munira, N. A. Molok, and S. Talib, "Exploring the Factors Influencing Top Management Involvement in Information Security," *PACIS 2017 Proc.*, 2017.
25. N. Ibrahim, "The Role of Organizational Factors to the Effectiveness of ISMS Implementation in Malaysian Public Sector," vol. 7, pp. 544–550, 2018.
26. W. W. Chin, "The Partial Least Squares Approach to Structural Equation Modeling," *Mod. Methods Bus. Res.*, 1998.
27. B. R. Lewis, G. F. Templeton, and T. A. Byrd, "A methodology for construct development in MIS research," *Eur. J. Inf. Syst.*, vol. 14, no. 4, pp. 388–400, 2005.
28. J. Henseler, C. M. Ringle, and R. R. Sinkovics, "The use of partial least squares path modeling in international marketing," *Adv. Int. Mark.*, vol. 20, no. 2009, pp. 277–319, 2009.
29. J. Hulland, "Use of partial least squares (PLS) in strategic management research: a review of four recent studies," *Strateg. Manag. J.*, vol. 20, no. 2, pp. 195–204, 1999.
30. J. F. Hair Jr, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications, 2017.
31. J. Nunnally, *Psychometric Theory*. 1978.
32. C. V. Fornell and Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Mark. Res.*, vol. 18(3), pp. 39–50, 1981.
33. D. Goodhue, W. Lewis, and R. Thompson, "Research Note—Statistical Power in Analyzing Interaction Effects: Questioning the Advantage of PLS with Product Indicators," *Inf. Syst. Res.*, vol. 18, no. 2, pp. 211–227, Jun. 2007.
34. R. Kline, "Principles and practice of structural equation modeling 2011 3rd ed. New York," *NY Guilford Press Google Sch.*, 2011.
35. [35] 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.
36. I. Benbasat, "Special Issue Information Security Policy Compliance : An Empirical Study of Rationality - Based Beliefs," vol. 34, no. 3, pp. 523–548, 2010.
37. 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.
38. A. B. Shahri, Z. Ismail, and N. Z. A. Rahim, "Security culture and security awareness as the basic factors for security effectiveness in health information systems," *J. Teknol. (Sciences Eng.*, vol. 64, no. 2, pp. 7–12, 2013.
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.