Information Security Management System Success Measurement Indicator

Nurazean Maarop, Deden Witarsyah, Surya Sumarni Hussein, Ganthan Narayana Samy, Noor Hafizah Hassan, Doris Wong Hooi Ten, Roslina Mohammad, Norziha Megat Mohd Zainuddin

Abstract: Information security matter has become significant element to support digital transformation. The concern is even more vital in organizations as they need to warrant that their information systems are appropriately secured. Hence, the Information Security Management System (ISMS) has been formed to offer many benefits in improving overall organizational security performance, efficiency and management of information. Nevertheless, there is still limited indicator to be applied when assessing ISMS implementation success in organization. In most literature within the Information Systems domain, the success or failure of the implementation of technology is fundamentally measured by the indicator known as net benefit of individual or organization. This study presents the development of ISMS success measurement indicators based on the procedures and the statistical analysis of pilot study. The overall aim is to validate the items relevancy of ISMS implementation success. This study occupies an acceptable pilot sample size of thirty eight respondents through quantitative survey distributed purposively among Malaysian government agencies' employees who have experienced with ISMS implementation and application. As a result, this study proposes ISMS success model measurement indicators comprising thirty five measurement items.

Index Term: Information Security Management System; Success Model; Information Systems Success; Survey Indicator Development

1. INTRODUCTION

Nowadays, security measures and standards have been adopted widely in both private and government organization. A number of standard and best practice have been employed in assisting organization to measure their associated security issue including risk, control, compliance, privacy, information security and security regulations (Saint-G). The ISMS standard has been adopted worldwide. A statistic survey performed by International Standards Organization (ISO) in 2012 [1] regarding the ISMS implementation shows that at the end of December 2016, at least 33290 organization have been ISO/IEC 27001:2005 or ISMS certified compared to 27536 in 2015, thus a growth of 21%, had been issued in 103 countries [2]. The ISMS implementation in Malaysia also shows a significant growth from 2008 to 2016. In 2008 it was reported that only 34 agencies were ISMS certified [2]. An ISMS is a standard of information security that was originally established from the BS7799 that are published by the British Standards Institution (BSI) in 1995. Later, ISMS was used by the International Organization for Standardization (ISO) after a revision at the international level and was given the new ISO code which named as ISO/IEC 17799:2000 in the year of 2003. The latest version was published in 2013 with the code ISO 27001:2013.

- *Nurazean Maarop, Lecturer of Razak Faculty of Technology & Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia. E-mail : nurazean.kl@utm.my*
- *Deden Witarsyah, Lecturer of Department of Information System, Telkom University, Indonesia. E-mail : dedenw@telkomuniversity.ac.id*
- *Surya Sumarni Hussein, Lecturer of Razak Faculty of Technology & Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia.*
- *Ganthan Narayana Samy, Lecturer of Razak Faculty of Technology & Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia.*
- *Noor Hafizah Hassan, Lecturer of Razak Faculty of Technology & Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia.*
- *Doris Wong Hooi Ten*
- *Roslina Mohammad*
- *Norziha Megat Mohd Zainuddin*

The previous version of ISMS emphasizes on the Plan-Do-Check-Act (PDCA) management approach [4]. However, the latest version of ISMS did not emphasize on it anymore. The user of the standard is now given more freedom in choosing their management approach [2]. In broad terms, the ISMS is a part of the overall management system aimed to develop, operationalize, monitor, evaluate, maintain and improve the security of information in organization [2]. It is also regarded as a method in handling the risks of assets that is used in the business's information management, processing and storing [2]. An ISMS involves the collaboration and integration of the information security and business policy, establishment of an enterprise information security policy, and decision making on personal management and handling in organization. Among the advantages of ISMS are enabling focus on proactive measures, reducing client audit requirements, resulting in fewer incidents and disruption of services, less resource spent on finding new customers and investors, greater productivity, increasing the effectiveness of incident response management, resulting in less time and money spent on damage limitation measures, better understanding of business information processes and reassuring customers and internal parties [5-6]. However, despite of these benefits, there is still lack of assessment indicators to measure the success implementation of ISMS. Among the critical aspects in ISMS implementation are identifying the human elements in socio-technical context that affect the effectiveness of ISMS as this can minimize the weaknesses [7]. Thus, Maarop et al. [2] urge the need to identify these critical factors of ISMS in ensuring success of the project thus there is a need to establish ISMS implementation measurement indicators. Therefore, the aim of this study is to identify and propose the relevant indicators that can be used to measure ISMS success in organization thus exploring the reliability and validity of the identified items. Hence, this study has executed a pilot study occupying acceptable sample size incorporating all procedures deemed essential in pilot data analysis [8]. Pilot study yields reliability and validity of the measures which later can be used in the main study. Accordingly, in this study context, the reason of conducting the pilot work is to develop ISMS success measurement indicators which can be used to validate the ISMS success

model of relevant organization or government agencies in the later phase of study.

2. BACKGROUND

2.1 Information Systems Success Model

Implementation of ISMS in an organization requires a lot of resources allocation such as human, time and monetary [9]. As so, it is very important for an organization to assess the factors that influence the success of ISMS implementation. With an appropriate implementation of ISMS it may warrant the organization to be in line with the organization's goals and mission [10]. The underlying theoretical aspects used in this study is based on the Information Systems Success Model domain. The Information System Success Model was initially established by DeLone, & McLean in 1992 [11] and subsequently in 2003, they updated the model [12]. The original taxonomy of ISSM was developed by DeLone & McLean in 1992 [11] shown in Fig 1 whereby the updated model [12] is shown in Fig 2. The enhanced version comprises new variable labelled as service quality. The factors namely individual impact and organizational impact were merged into net benefits which are used as indicators to success in the Information Systems context. The updated D&M model has been used widely as it can be used to denote success of various ISs [13-14].

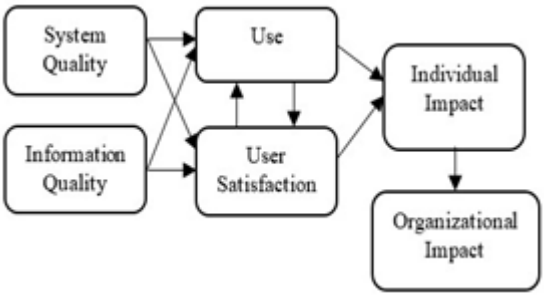

Fig. 1 *Original D&M IS Success Model [11]*

2.2 Previous ISMS Success Model

In the initial ISMS related research Maarop et al. [2] conducted a qualitative study focusing on Plan Phase of The Plan-Do-Check-Act (PDCA) domain [4]. Based on qualitative method research driven Maarop et al. [2] proposed a conceptual model of ISMS success model comprising key issues of ISMS Plan Phase Self Implementation Success Element shown in Fig 3. The model puts emphasis on ISMS Plan Phase Self Implementation and the authors have proposed three main factors influencing net benefit namely Management Commitment, Implementer Competency and Implementer Commitment. These three factors have shown significance of influence on the net benefits qualitatively [2]. However, the study has not surveyed and tested these three factors quantitatively. Another perspective of ISMS critical success study was performed by using data envelopment analysis, whereby a mathematical programming was used to characterize the efficiencies and inefficiencies of decision making department [16]. As a result the study highlighted the importance of factors from Policy and Management (e.g. commitment and leadership, and top management attention) and Execution and Management (e.g. effective training, awareness and competence) as these factors are always on the top level of management hierarchy thus mainly initiated the ISMS. However, unlike the original and updated D&M Success Model, the study [16] has not provided communication association among technical, semantic and effectiveness level.

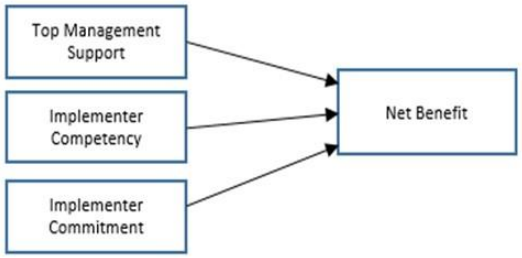

Fig. 3 *Conceptual Model of ISMS Plan Phase Implementation Success [2]*

Further study was proceeded by Maarop et al. [17] to review more relevant factors in a wider scope of ISMS implementation based on frequency analysis. As a result of their study, ten critical success factors were found to be significant in implementing ISMS in the organization. These include alignment of organizational mission, top management commitment, commitment of funding, organizational structuring, staff awareness and training, IT competence, risk management, security policy implementation, standards compliance, and performance evaluation [17]. However, their result presented some research limitation as the postulated factors were not tested either qualitatively or quantitatively in a specific context. Likewise, a study by AbuSaad et al. [18] have revealed the importance of handling obstacles namely asset identification, weak team experience, resistant to change, top management involvement and culture in order to increase success implementation of ISMS in Saudi Arabia context. Other researches of ISMS success in different contexts have also been reviewed. Another quantitative study considering critical success factors of ISMS continuous operation has yielded the importance of Information Security Culture [19]. Indeed by enhancing organizational security level would motivate the use of ISMS [18].

2.3 Proposed Model

Based on the synthesis of the relevant literature this study proposes a theoretical ISMS success model that takes into consideration the updated IS Success Model by selecting net benefit considering a merged individual and organizational impact as an indicator to success. The study also considers study by Maarop et al. [2] as the base model since the factors have been successfully proven qualitatively in the context of Malaysian government agencies. However, the respective study [2] has limited their research scope at the plan-phase implementation of ISMS. For that reason, this study has further considered a wider scope of ISMS implementation. The conceptualization of proposed ISMS model of this study also considers communication association among operational, semantic and effectiveness level. In regard to operation level, this proposed model was developed using a base model by Maarop et al. [2] by addressing their three contextual factors of ISMS success comprising Implementer Competency, Implementer Commitment and Top Management Support. In addition, other significant factors from the review are also considered and these are Awareness and Training [20-21], Information Security Culture [19, 22] and Business Alignment [2, 23]. These additional factors are considered in this study because

they are found to be high cited items in the review of ISMS implementation success study [17]. In relation with semantic and effectiveness level, this study suggests the dependent success indicator from both original [11] and updated IS Success Model [12]. The relationship among communication level and factors and factor description is shown in Table I and the conceptual model proposed by this study is shown in Fig 4.

TABLE I
Description of Factors

Communication Level	Factors	Description
Operational	Awareness & Training	Periodic educational and training programs in order to improve staff knowledge and skills on ISMS matters and improve compliance-related behaviors including safety at work.
	Implementer Competency	The ability of implementer towards implementation and change management at holistic view, understands the standard, procedures of asset identification, risk assessment, scope and project structure identification, an approach or framework to implement, maintain, monitor and improve IS and existing auditing regulation and infrastructure.
	Implementer Commitment	The willingness of implementer to put forth effort to pursue the strategic direction of the organization. This includes allocation of certain amount of time to concentrate on ISMS implementation, adhere to proper planning and striving in ensuring the success of the implementation.
	Top Management Support	Support and key-role played by the stakeholders in enabling good communication and cooperation between different departments and stakeholders. This also includes support of budget and manpower and consistently engaged and motivated in the lifecycle of the ISMS implementation.
	Organizational Information Security Culture	The way organization creates employees' behavior towards information security in the organization in supporting and guiding ISMS practice.
	Business Alignment	The shared efforts between information security and business managers in aligning ISMS practices with business plans of the organization to support organizational objectives.
Semantic	Individual Impact	An indication that an ISMS has improved individual decision-making productivity, has produced a change in user activity.
Effectiveness	Organizational Impact	An indication that ISMS has affected the organizational performance, facilitate organization strategy and increases security practice in organization.

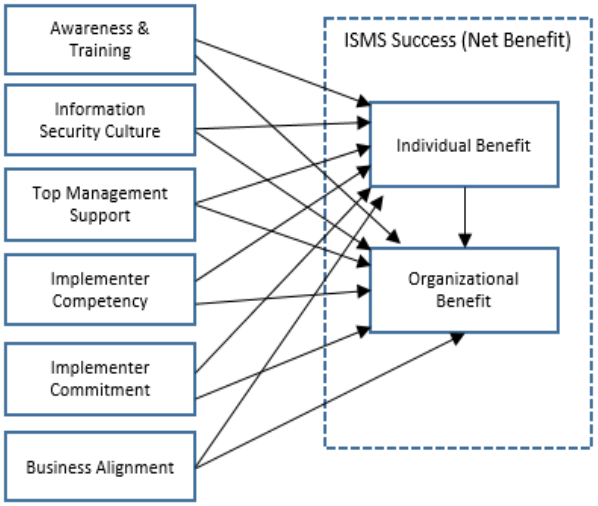

Fig. 4 *A Proposed ISMS Success Model*

3. RESEARCH METHODOLOGY

This study uses quantitative research method to test the validity and reliability of the ISMS success indicators. The questionnaire items were constructed by considering other relevant previous literature. The instrument of this study was distributed through online survey. All the deduced items of prior studies are then used to measure each of the latent variable as shown in Table II. The questionnaire was divided into two main sections. Section A consists of respondent's demographic profile and Section B indicates questions on ISMS success measures. PLS algorithm with SmartPLS 3.0 were used to perform inferential analysis and SPSS version 24 was used for descriptive analysis. The target population for this pilot was adequate. The respondents for this pilot study consist of 38 IT related employees of Malaysian government ranging from IT Officer to Top Manager whom officially have involved in ISMS implementation. According to Nunnally and Bernstein [24], minimum 30 respondents are required for a pilot study. Content validity was also confirmed through expert review. Prior to the pilot test, expert review session was done by employing three ISMS experts to validate the relevancy of the proposed instruments. Lynn [25] suggested a minimum of three experts for content validity requirement in the expert review. Subsequently, the test of content validity was performed on eight construct namely awareness and training (five items), implementer competency (seven items), implementer commitment (four items), top management support (five items), information security culture (six items), business alignment (four items), individual impact (two items), and organizational impact (three items). Items were refined based on reviewers' feedback. The indicators used for the survey are shown in Table II.

TABLE II
Items Used in The Pilot Test

Factor	Items	Authors
Awareness & Training	AT1: Employees are aware of information security policy and guidelines of the organization. AT2: Organization conducts regular information security training for employees AT3: Organization conducts programs to make employees aware of the importance of information security AT4: Employees are aware of the punishments or disciplinary actions for violating information security guideline AT5: Employees' roles and responsibilities for information security are properly communicated	[20-21, 26-29]
Implementer Competency	ICP1: ISMS implementer is able in understanding clause (project management and security clause) ICP2: ISMS implementer is competent towards Change Management ICP3: ISMS Implementer offers skill on Holistic View ICP4: ISMS Implementer is competent in Risk Assessment & Asset Identification ICP5: ISMS Implementer is competent based on the past experience ICP6: ISMS Implementer offers related approach & framework IC7: Ability to provide Documentation and Standardization by ISMS Implementer	[2, 27, 30, 31]
Implementer Commitment	ICM1: ISMS implementer is committed towards ISMS Project Management ICM2: ISMS implementer provides ISMS audit infrastructure ICM3: Overall team members of ISMS implementer are committed in the ISMS project ICM4: ISMS implementer is motivated in the ISMS project	[2], [30-33]
Top Management Support	TMS1: Top management publicly supports the project and calls it a top priority TMS2: Top management allocate budget and manpower for information security functions TMS3: Top management attend information security related meeting TM4: Top management approves the project related to ISMS matter TM5: Top management is actively engaged throughout thel life cycle of the implementation	[2, 29, 31, 34]
Information Security Culture	ISC1: Organization creates an information security focus among all employees ISC2: Organization makes sure that information security is the first thing on the mind of all employees ISC3: Organization makes information security the norm for all employees ISC4: Organization dedicates efforts to create an information security focused workforce ISC5: Organization provides security forum to offer input for management direction and support	[19, 29, 33,34, 35]
Business Alignment	BA1: Business and IT planning and management processes are tightly connected and integrated. BA2: There is adequate involvement of the business entity in	[17, 29, 35, 36]

	security and privacy matters BA3: Business management has a good understanding of the impact of IT on the business BA4: Business key-users participate in the implementation of ISMS	
Individual Impact	II1: ISMS increases my job satisfaction II2: Overall ISMS makes my job easier	[2, 11, 12, 29]
Organizational Impact	OI1: ISMS facilitates organizational achievement OI2: ISMS improves business performance OI3: ISMS enhances security practice	[2, 11, 12, 29]

4. FINDINGS

A pilot analysis study is a miniature version of the main study to examine whether the components of the main study can all work together [37]. It is suggested that a pilot study analysis should be mainly descriptive thus the objectives of the analysis must be clear [38]. Furthermore, one of the pilot study statistical objectives is to provide a range of values for the parameter under study and this includes mean and standard deviations before an event occurs [38]. Hence, the pilot study is not a hypothesis testing with p-values but solely to investigate crucial components of the main study. The findings of this study are arranged into descriptive analysis and validity and reliability testing. Thus, pilot study procedures may help improve the internal validity of a questionnaire [39].

4.1 Descriptive Analysis

With regard with descriptive data, demographics information such as gender, work experience, designation category and ministry work placement are reported. A sample of 38 Information Technology related employees completed the survey. The majority of the respondents are female (n=26, 68.4%) and only 31.6% (n=12) are male. The breakdown of participants' working experience are as follows: 44.7% are between 5-10 years, 39.5% are between 11-15 years, 5.3% are between 16-20 years, 5.3% are between 21-25 years, and 5.3% are between 25-30 years. The breakdown of participants' job designation are as follows: 39.5% as IT Manager, 26.3% as IT Officer, 10% as Technical and IT Support and 7.9% as Top Manager. The participants working for mainly MAMPU represents 44.7% whereby the remainder of 55.3% work in other various ministries.

4.2 Item Analysis and Reliablity Test

This study has applied item analysis, reliability and validity measurement testing in order to infer whether or not the items proposed in this study are considered reliable and valid to be used in the main study. Item analysis was done through factor loadings to measure indicator reliability. According to Hair et al. [40], scale with higher loading on a construct indicates a better reliability. In addition, items with at least 0.50 or more are considered to be significant [40]). In regard to reflective measurement perspective, Hair et al. [41] suggested a removal of an indicator with outer loading of below 0.70 if only the deletion of the item may increase the above threshold which are based on two criterion namely composite reliability (CR) (must be above 0.7) and average variance extracted (AVE) (must be above 0.50). All corrected-item total correlation values were above 0.70 except for item ICP6 (0.551) and ICM4 (0.650). However since all items loadings (corrected-item total correlation) were still above the threshold values for both criterions, this study suggested that all reflective indicators of the proposed ISMS Success Model to be retained and used for the next stage of study. Table III shows factor loadings of each item along with the respective mean and standard deviation.

TABLE III
Factor Loadings and Items Analysis

Item	Factor Loading	Mean	Standard Deviation
AT1	0.943	4.395	0.745
AT 2	0.933	4.289	0.824
AT 3	0.877	4.316	0.831
AT 4	0.721	4.105	0.882
AT 5	0.890	4.395	0.709
ICP1	0.833	4.342	0.804
ICP 2	0.822	4.289	0.792
ICP 3	0.848	4.184	0.823
ICP 4	0.833	4.447	0.785
ICP 5	0.551	4.079	0.774
ICP 6	0.868	4.079	0.774
ICP7	0.843	4.368	0.741
ICM 1	0.706	4.237	0.741
ICM 2	0.779	4.105	0.788
ICM 3	0.921	4.526	0.678
ICM4	0.650	4.447	0.594
TM1	0.920	4.579	0.674
TM2	0.950	4.536	0.786
TM3	0.761	4.421	0.674
TM4	0.833	4.526	0.678
TM5	0.731	4.368	0.741
ISC1	0.926	4.368	0.741
ISC2	0.935	4.237	0.741
ISC3	0.937	4.105	0.788
ISC4	0.900	4.526	0.678
ISC5	0.832	4.447	0.594
BA1	0.892	4.368	0.741
BA2	0.884	4.158	0.744
BA3	0.910	4.316	0.798
BA4	0.892	4.395	0.670
II1	0.856	4.158	0.892
II2	0.905	3.868	0.934
OI1	0.771	4.737	0.440
OI2	0.863	4.395	0.670
OI3	0.835	4.605	0.540

An instrument would only be valid if it is reliable. As the estimate of reliability increases, the segment of the cause of error decreases [42]. Accordingly reliability test was performed after item analysis. Cronbach's alpha (CA) was used to measure internal consistency as it quantifies the degree to which items on instrument are correlated with each other [43]. Hence, CA may range from 0.0 to 1.0 and is generally used to measure the reliability of construct. CA assumes that all indicators are equally reliable such as all indicators have equal outer loadings on the construct. It is calculated based on indicator inter-correlations. Higher coefficients indicates reliable measuring instruments [32]. There are different opinions about acceptable range of CA. The minimum adequate value recommended for CA is above 0.70 to achieve reliability by ensuring internal consistency of the survey instruments [24]. However in exploratory research the minimum threshold for CA may be at 0.60 [40]. In this study, convergent validity procedures were also performed

as to test construct validity. According to Fornel and Larckel [44], convergent validity can be assessed by factor loading, composite reliability and Average Variance Extracted (AVE) [44]. CR provides a better indicator for measuring internal consistency as CR relies on standardized regression weights and measurement correlation errors for each item and therefore may yield consistent results [40]. An internal consistency reliability is considered satisfactory when the value of CR is at least 0.7 [24, 40]. On the other hand, AVE is the degree to which a latent construct explains the variance of its indicators (Hair 2016). Thus, AVE value should be more than 0.50 to reflect adequacy for convergent validity [44]. The result shown in Table IV indicates that all the constructs have met the acceptable CA, CR and AVE values which are above the recommended threshold value. Therefore, the instruments are regarded reliable which can be further used and can be recommended to be adopted by other related studies.

TABLE IV
Reliability Test

Construct	Cronbach Alpha	CR	AVE
Awareness & Training (5-items)	0.937	0.943	0.768
Implementer Competency (7-items)	0.916	0.927	0.679
Implementer Commitment (4-items)	0.782	0.852	0.594
Top Management Support (5-items)	0.913	0.924	0.712
Information Security Culture (5-items)	0.946	0.959	0.822
Business Alignment (4-items)	0.919	0.941	0.800
Individual Impact (2-items)	0.714	0.874	0.776
Organizational Impact (3-items)	0.763	0.863	0.679

5. CONCLUSION

This study presents the development of ISMS success measurement indicator and the item measurement analysis based on the pilot testing procedures. The overall objective of this study is to validate the items relevancy of ISMS implementation assessment. Thirty-eight responses were analyzed using statistical software. Most of the prior research of ISMS critical success factors are still in the review work status and qualitatively presented thus there is a lack of studies in ISMS success research domain occupying statistical testing procedures to measure their claimed items or indicators. Hence, this paper has presented the validated measurement indicators to be considered by other studies that intend to measure success of ISMS implementation. Overall, the result of this study has suggested thirty-five measurement items from eight constructs can be used to measure ISMS success particularly in the domain of government sector. Furthermore, this study has shown a contribution to the existing literature by proposing the ISMS success model as the model was developed based on the consideration of the interrelationship among three communication level namely operational, semantic, and effectiveness of ISMS implementation.

ACKNOWLEDGMENT

We would like to thank Universiti Teknologi Malaysia, Ministry of Education Malaysia under the Vote 17H73 and University of Telkom Indonesia.

REFERENCES

[1] The ISO Survey of Management System Standard Certifications. (2015). Retrived 10 April 2018, from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/the_iso_survey_of_management_system_standard_certifications_2015.pdf

[2] N., Maarop, N. Mohd Mustapha, R. Yusoff, R. Ibrahim, N.M.M. Zainuddin. “Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation”, Vol. 9, No. 3, pp. 884-889, 2015.

[3] H. K., Kong, J. H., Woo, T. S., Kim, & H. Im, “Will the Certification System for Information Security Management Help to Improve Organizations’ Information Security Performance? The Case of K-ISMS”, Indian Journal of Science and Technology, Vol 9, No. 24, 2016.

[4] E., Humphreys. “Information security management standards: Compliance, governance and risk management”, Information Security Technical Report, Vol 1, No 4, pp. 247–255, 2008.

[5] R., M., van Wessel, H.J de van Vries, “Business Impacts of International Standards for Information Security Management. Lessons from Case”, Vol. 1, pp. 25–40, 2013.

[6] J., S., Broderick. “ISMS, security standards and security regulations. Information Security Technical Report”, Vol 11, No. 1, pp. 26–31, 2006.

[7] S., M., Alfawaz. “Information Security Management: A Case Study of an Information Security Culture”, PhD Dissertation, QUT, Australia, 2011.

[8] D.R. Monette, T.J. Sullivan, C.R. DeJong, “Applied social research: A tool for the human services”, Cengage Learning, 2013.

[9] C., Pelnekar, “Planning for and Implementing ISO 27001,” ISACA Journal, Vol. 4, No. 4, pp. 1-8, 2011.

[10] ISACA, “Information Security Governance: Guidance for Boards of Directors and Executive Management”, IT Governance Institute, 2006.

[11] W., H., DeLone and E.,R., McLean, “Information systems success: the quest for the dependent variable”, Information Systems Research, Vol. 3, No. 1, pp. 60–95, 1992.

[12] W.,H., DeLone and E.,R., McLean, “The DeLone and McLean model of information systems success: a ten-year update”, Journal of Management Information Systems, Vol. 19, No. 4, pp. 9–30, 2003

[13] H. Jin Yeo, “Information System Success Disparity between Developer and Users”, Indian Journal of Science and Technology, Vol. 9, No. 20, 2016.

[14] Y. Hagos, M. Garfield, and S. Anteneh, “Measurement factors model for e- learning systems success”, Tenth

International Conference on Research Challenges in Information Science (RCIS), IEEE, pp. 1–6, 2016.
[15] R., Boyatzis ."Transforming qualitative information: Thematic analysis and code development", Thousand Oaks, CA, Sage, 1998.
[16] H., L., Hai and K., M., Wang, "The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability, African Journal of Business Management, Vol. 8, No. 17., pp. 705-716, 2014.
[17] N., Maarop, K. Thamadaran, G., N., Samy, A., Azmi, O., Mohd-Yusof, A., Azizan, "Information Security Management System Implementation Success Factors: A Review", Advanced Science Letter, Vol. 22, No. 10, pp. 3023-3026, 2015
[18] B., AbuSaad, F., A., Saeed, K., Alghathbar and B., Khan, "Implementation of ISO 27001 in Saudi Arabia-obstacles, motivations, outcomes, and lessons learned", Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western, Australia, 5th -7th December, 2011
[19] S., Woodhouse, "Critical success factors for an Information Security Management System", Proceeding 5th International Conference on Information Technology and Application, pp. 244-249, 2008.
[20] T., Aksorn, and B., H., W., Hadikusumo. "Critical Success Factors Influencing Safety Program Performance in Thai Construction Projects," Safety Science, Vol. 46, No. 4, pp 709-727, 2008.
[21] T., Kayworth and D., Whitten, "Effective Information Security Requires a Balance of Social and Technology Factors," MIS Quarterly Executive (9:3), pp 163-175, 2010.
[22] A., N., Singh and M.P. Gupta, "Identifying factors of organizational information security management", Journal of Enterprise Information Management Vol. 27 No. 5, 2014 pp. 644-667, 2010.
[23] J., L., Spears and H., Barki, "User Participation in Information Systems Security Risk Management," MIS quarterly (34:3), pp 503-522, 2010
[24] J. C. Nunnally and I. H. Bernstein, Psychometric theory. New York: McGraw-Hill, 1994.
[25] M.R. Lynn, "Determination and quantification of content validity", Nursing Research, Vol. 35, pp.382– 385, 1986.
[26] Tu, Z., & Yuan, Y. Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. Proceedings of the 20th Americas Conference on Information Systems (AMCIS), USA, Georgia, Savannah, 2014
[27] Alshitri, K.I. & Abanumy, A.N., Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. In International Conference on Information Science and Applications (ICISA), pp. 1-4, 2014
[28] Lisiak-Felicka. D., & Szmit, M. Information security management systems in Marshal Offices in Poland. Information Systems in Management, Vol 3, No. 2, pp. 134-144, 2014
[29] M. Hasan, H.I. Baharun, G.N. Samy, N. Maarop, W.Z. Abidin, and N.H. Hassan, "Developing a success model of Research Information Management System for research affiliated institutions", in 5th International Conference on Research and Innovation in Information Systems: Social Transformation through Data Science, ICRIIS 2017
[30] Werlinger, R., Hawkey, K., & Beznosov, K. An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management, Information Management & Computer Security, Vol 17, No.1, pp 4-19, 2009
[31] Kim, J. & Rhee, J. An empirical study on the impact of critical success factors on the balanced scorecard performance in Korean green supply chain management enterprises. International Journal of Production Research, Vol 50, No. 9, pp.2465-2483, 2012
[32] Kayworth, T., & Whitten, D. Effective Information Security Requires a Balance of Social and Technology Factors, MIS Quarterly Executive 9(3), 2010, pp 163-175.
[33] Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. African Journal of Business Management, 6(14), 4982–4989.
[34] Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. Factors Influencing Information Security Management in Small-and Medium-Sized Enterprises: A Case Study from Turkey, International Journal of Information Management 31(4), 2011, pp 360-365.
[35] Van Niekerk, J. F., & Von Solms, R. Information Security Culture: A Management Perspective, Computers & Security, 29(4), pp 476-486, 2010.
[36] Spears, J. L., & Barki, H. User Participation in Information Systems Security Risk Management," MIS quarterly, 34(3), 2010, pp 503-522.
[37] M., Arain, M., J., Campbell, C., L., Cooper and G., A., Lancaster, "What is a pilot or feasibility study? A review of current practice and editorial policy", BMC Medical Research Methodology, Vol 10., No.67, 2010
[38] G., A., Lancester, S., Dodd and P., R., Williamson, "Design and analysis of pilot studies: recommendations for good practice", Journal of Evaluation in Clinical Practice, Vol 10, No. 2, pp 307-312, 2004.
[39] E., van Teijlingen & V., Hundley, " The importance of pilot studies", Vol. 16, No., pp.33-36, 2002.
[40] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, "A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)", SAGE Publications, 2013.
[41] J., F., Hair, B., J., Babin and N., Krey, "Covariance-Based Structural Equation Modeling in the Journal of Advertising: Review and Recommendations, Vol. 46, No. 1, pp. 163-177, 2017
[42] M., Tavakol & R., Dennick, "Making sense of Cronbach's alpha", Vol. 2, pp. 53-55, 2011
[43] L.,M., Connelly, " Research Roundtable, Cronbach's Alpha", MEDSURG Nursing, Vol. 20, No. 45, 2011.
[44] C., Fornell, & D., F., Larcker, "Evaluating structural equation models with unobservable variables and measurement error. Journal of marketing research", Vol.18, No. 1, pp. 39-50, 198