Factors Contributing to the Success of Information Security Management Implementation

Mazlina Zammani[1,] Rozilawati Razali[2], Dalbir Singh[3]
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia, 43600
Bangi, Selangor, Malaysia

***Abstract*—Information Security Management (ISM) concerns shielding the integrity, confidentiality, availability, authenticity, reliability and accountability of the organisation's information from unauthorised access in order to ensure business continuity and customers' confidence. The importance of information security (IS) in today's situation should be given due attention. Recognising its importance, organisations nowadays have devoted wide efforts in protecting their information. They establish information security policy, processes, and procedures as well as reengineer their organisational structures to align with ISM principles. Regardless of the efforts, security incidents continue to occur in many organisations. This phenomenon shows that the current implementation of ISM is still ineffective due to unaware of the factors contributing to the success of ISM. Thus, the objective of this paper is to identify ISM success factors and their elements through a large-scale survey. The survey involves 243 practitioners from statutory bodies, public and private organisations in Malaysia. The results of the survey indicate that top management, IS coordinator team, ISM team, IS audit team, employees, third parties, IS policy, IS procedures, resource planning, competency development and awareness, risk management, business continuity management, IS audit and IT infrastructure are the factors that contribute to the success of ISM implementation. These factors shall guide practitioners in planning and refining ISM implementation in their organisations.**

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

I. Introduction

Information security management (ISM) is a systematic preservation approach to protect the integrity, confidentiality, availability, authenticity, reliability and accountability of information [1],[2],[3]. Every single day, organisations and their information are exposed to security threats and incidents such as malware, virus, malicious spyware, spam, phishing and sabotage from an extensive range of sources [4],[5],[6],[7]. Researches have indicated that security incidents increase over the years [8]. For example, from the year 2010 to 2016, there were 60,000 security incidents occurred at large organisations in the United States [4]. In the Netherlands, 18% of all small and medium organisations are hit by cyber-attacks each year and in Malaysia, a total of 3280 security incidents have been reported in the half-year 2018 [9],[10].

The increasing number of security incidents has led organisations to enhance their ISM plans in order to shield their critical information [11]. Thus, organisations have begun taking systematic approaches in managing their information. However, there are still weaknesses in the implementation, which causes security incidents continue to occur [1], [12]. Organisations in general are seen as fail to manage their information security (IS) appropriately. One of the main reasons is that the organisations are not aware of the factors contributing to the success of ISM implementation [13]. In essence, these success factors should be given serious attention in order to ensure that ISM is effectively implemented [14]. Therefore, this paper aims to explore the success factors of ISM implementation. The factors shall be used as a guide to organisations in bettering their ISM practices.

This paper is organised as follows. Section 2 provides a brief review of the ISM factors that were gathered from the literature. Section 3 describes the methodology used to collect and analyse the empirical data. Section 4 presents the findings of the analysis and finally, Section 5 summarises the findings.

II. Background

An ISM is a method or approach to managing information securely and effectively. It involves various aspects such as people, process, organisational documents, and technology [15], [16]. The people aspect contains the key players of ISM, who shall own certain characteristics for implementing ISM process. The implementation of the process should be guided by organisational documents and supported by the latest technology [17].

A. People

In the people aspect, the key players involved are Top management, ISM team, IS coordinator team, IS audit team, employees and third parties. Top management is a key pillar for the ISM's accomplishment. Top management should portray high leadership qualities and have good knowledge of the security objectives and governance to ensure the goal of ISM is achieved [15]. In addition, the commitment of top management is required to make decisions, provide feedback and giving support to the whole security activities undertaken [14].

The ISM team is responsible for implementing security operations and activities. Hence, the team's knowledge in the security domain is required. Skills, commitment, and cooperation of team members are necessary to ensure that security operations run smoothly. Furthermore, the willingness of the whole team members to accept changes at any time is also expected [18].

Meanwhile, the IS coordinator team is responsible for managing and coordinating the main documents and security activities such as awareness and training programs. The team acts as a liaison between top management, ISM team, IS audit team and employees. Therefore, the members of the team need to be knowledgeable about the overall ISM scope and activities. They also need to give a full commitment in coordinating the ISM activities and have good communication skills [18].

On the other hand, employees and third parties should be aware of the latest security policy, threats and issues that occur in the organisation. In order to reduce the security incidents, the employees and third parties must comply with security policy, laws and agreements [19]. In addition, employees' motivation towards the implementation of IS controls is also needed.

Apart from top management, ISM team, IS coordinator team, employees and third parties, the IS audit team equally plays a role in the success of ISM implementation [20]. The team should be committed in ensuring the security controls, processes, and activities are implemented properly [21]. The IS audit team must have knowledge of IS and the matters to be audited [22]. They need to possess the necessary auditing skills by applying appropriate auditing techniques. Additionally, communication skills are required to obtain useful information from auditees. Furthermore, the team's commitment and cooperation are also needed to ensure the effectiveness of the auditing process.

B. *Organisational Documents*

Organisational documents refer to the internal documents that need to be well-established and complied during the implementation of ISM. Two factors recognised under the organisational documents are IS policy and IS procedures.

IS Policy is a set of rules enacted by an organisation to ensure that all employees and third parties are complying with the IS prescription [23]. The policy should be comprehensive in covering the controls proposed by the international standards and must be in line with IS requirements and ISM scope. It must be clear in describing IS objectives and the responsibilities of the parties involved [19], [24]. In addition, the policy should be communicated and disseminated to the employees, third parties and stakeholders. It should also be periodically reviewed to ensure it is appropriate to the current needs [25]. Beside IS Policy, IS procedures also contribute to the success of ISM implementation. IS procedures are the operating guidelines that comprise a series of activities that explain how to execute IS processes. The procedure must be clear and complete in describing the work steps to be carried out. [25]. It must also be regularly reviewed and communicated among the individuals or teams involved. These features should be present in each procedure to ensure that the ISM processes can be implemented effectively.

C. *Process*

In the aspect of process, there are five identified factors involved in ISM namely Resource Planning, Competency Development and Awareness, Risk Management, Business Continuity Management, and IS Auditing. Resource planning contains financial and human resources to support and execute ISM processes and activities. The financial and human resources are necessary to guarantee the ISM processes and activities work efficiently [26]. In addition, competency development and awareness are also important for the success of ISM [19]. The competency development and awareness consist of training programs and awareness programs [25]. The goal of the training programs is to ensure that the individuals and teams involved in ISM operations acquire the knowledge and expertise for handling the tasks. The objective of the awareness programs is to ensure the employees, third parties and stakeholders are aware of IS policy, IS issues and IS threats as well as their responsibilities in protecting the organisation’s information [25]. Risk management is the crucial process in ISM [19]. Risk management focuses on assessing, analysing, mitigating, and controlling the risks [27]. Risk assessment and risk treatment are two main activities in risk management. Risk assessment is an activity of measuring and analysing the risk levels while risk treatment is an activity of implementing the suitable actions to control the risks [28].

Business continuity management (BCM) is another vital process in ISM [29]. It is a holistic management process to ensure the continuity of critical processes whenever disasters or unintended events happen [30],[31]. BCM requires a business continuity plan (BCP) that highlights the resources, activities, and responsibilities for managing the unintended events. In order to affirm the plan is feasible and effective, the organisation shall perform periodic tests on the plan. Beside risk management and BCM, IS audit is also another key process in ISM [25],[32]. Through the IS audit process, the compliance of IS policy, procedures and controls can be checked and evaluated [33]. The major items in the audit process are audit program, audit findings and reporting as well as follow-up audit to check the corrective and preventive actions that have been taken [20].

D. *Technology*

Another factor that contributes to the effectiveness of ISM implementation is the IT infrastructure that is listed under the technology aspect [34]. IT infrastructure includes the use of the latest software and hardware that support the implementation and monitoring of security operations. The review above indicates that there are various success factors that need to be considered when implementing ISM. The comprehensive explanation about the factors and their elements can be found in [18].

III. METHODOLOGY

This study adopts a mixed-method approach, which comprises qualitative and quantitative approaches. The purpose of combining these two approaches is to gain a better understanding of the phenomenon [35]. Fig. 1 illustrates the research design. The qualitative part consists of analysing the existing literature together with a series of interviews with experienced ISM practitioners. The results of the qualitative part have been reported in [18]. The study then further adopts a quantitative approach to confirm and refine the qualitative findings through a large-scale survey. The results are discussed in this paper.

TABLE. I. DETAILS OF THE QUESTIONNAIRE

Aspect	**CSFs**	**Number of Items**	**Items**
People	Top Management	5	Knowledge of top management regarding ISM objectives and governance.
			Knowledge of top management on ISM issues and problems
			The leadership of top management in leading the ISM.
			The commitment of top management in supporting the financial and human resources.
			The commitment of top management in giving feedback on any ISM issues and problems
	IS Coordinator Team	3	Knowledge of coordinator team on overall ISM scope and activities.
			The commitment of coordinator team in coordinating ISM activities
			Good communication skills.
	ISM Team	5	Knowledge of IS team in the information security domain.
			Skills of ISM team in handling and operating procedures of information security.
			The commitment of IS team towards information security operations that are being carried out.
			The IS team's willingness to accept additional assignments based on current needs.
			Cooperation between IS team members in carrying out security operations.
	IS Audit Team	5	Knowledge of IS Audit team regarding the ISM scope that needs to be audited.
			Skills of IS Audit team in applying auditing techniques.
			The commitment of IS Audit team throughout the auditing process.
			Cooperation between IS Audit team members.
			Good communication skills with the auditee.
	Employees	3	Awareness of employees regarding the importance of information security.
			Employees' compliance with the requirements outlined in the information security policy.
			Employees' motivation towards the implementation of information security controls
	Third Parties	3	Awareness of third parties regarding the importance of information security.
			Third parties' compliance with the requirements outlined in the information security policy.
			Third parties' compliance on information security agreement that has been signed.
Organisational Documents	IS Policy	4	Clear in defining IS objectives, the roles, and responsibilities of the employees, third parties, and stakeholders.
			Comprehensive which covers the requirements and controls set by the ISM standards and aligns with the ISM scope.
			Communicated to all employees, third parties, and other stakeholders.
			Reviewed/revised periodically or according to current needs.
	IS Procedures	4	Clearly explain the objectives and responsibilities of the individuals and team involved in the execution of procedures.
			Complete in describing the work steps to be carried out.
			Reviewed/revised periodically or according to current needs.
			Communicated to individuals or team involved.
Process	Resource Planning	2	Financial Resources for purchasing new assets and maintaining existing assets, the cost of manpower and the cost to perform IS activities.
			Human Resource for implementing IS processes and operation.
	Competency Development & Awareness	2	Awareness programs for all employees, third parties, and stakeholders.
			Training programs for individuals and teams involved in ISM processes and operation.
	Risk Management	2	Risk Assessment
			Risk Treatment
	Business Continuity Management	2	Business continuity plan that outlines the resources, procedures, activities, and responsibilities of the individuals and teams involved.
			Simulation (testing) on the business continuity plan
	IS Audit	3	Audit programs which consists of audit planning, audit training, and audit execution.
			Audit findings and reporting.
			Follow-up audit to check the corrective and preventive actions that have been done.
Technology	IT Infrastructure	2	Software to support the implementation and monitoring of information security.
			Hardware to support the implementation and monitoring of information security.

A. Sampling

The sampling method used for the survey was a stratified random sampling. A stratified random sampling is one obtained by separating the population into non-overlapping groups (e.g., ISM Team, IS Audit Team, ISMS Coordinator Team) and then applying a simple random sample from each stratum. This technique was chosen to ensure the presence of the key subgroups within each sample. The samples used in the study were ISM experts and practitioners from statutory bodies, public and private organisations in Malaysia.

B. Instruments

A set of questionnaire was developed based on the findings obtained from the earlier qualitative study. The contents of the questionnaire were reviewed by two experts from ISM field. A pilot study involving 30 ISM practitioners was conducted to ensure the reliability of the questionnaires. The questionnaire was then amended based on the feedback received from the experts and pilot study.

The questionnaire was divided into two sections. The first section consisted of the respondent's demographic profile. Meanwhile, the second section comprised questions regarding ISM factors and their items, as outlined in Table I. Respondents were required to respond to the questions on a 5-point Likert scale (1-Strongly Disagree, 2-Disagree, 3-Somewhat Agree, 4-Agree, 5-Strongly agree). In total, there were fourteen ISM factors and forty-five items all together to be confirmed.

C. Protocol

For distributing the questionnaires, the study hired fifteen enumerators and used online forms in order to ensure they were efficiently collected. A total of 400 questionnaires were disseminated to potential respondents among the statutory bodies, public and private agencies in Malaysia, based on the predetermined criteria set by the researchers. A two-week period was given to the enumerators to distribute and follow up with the respondents.

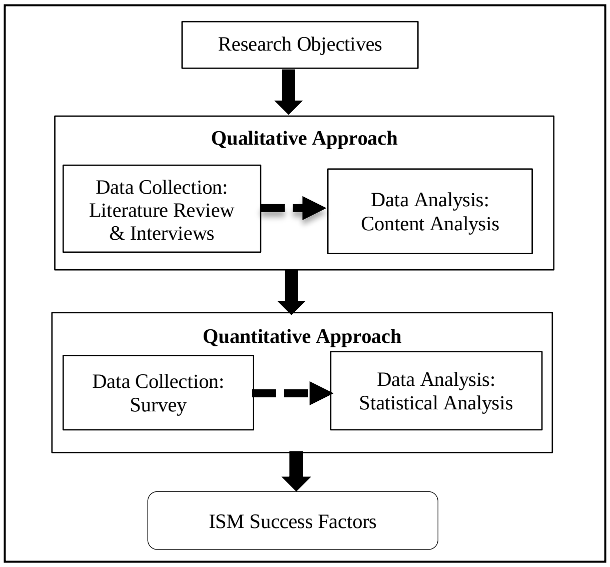

Research Objectives
Qualitative Approach
Data Collection: Literature Review & Interviews
Data Analysis: Content Analysis
Quantitative Approach
Data Collection: Survey
Data Analysis: Statistical Analysis
ISM Success Factors

Fig. 1. Research Design.

D. Analysis

From 400 questionnaires that were distributed, only 255 questionnaires were returned, which makes the response rate is 64%. However, only 243 questionnaires were considered for the data analysis, as the remaining were incomplete. The collected data was then analysed by using statistical analysis, as described in the later section.

IV. Result and Discussion

A test of scale reliability is executed to guarantee the measurement scales have consistently and accurately captured the meaning of the constructs. There are several common methods used in measuring reliability. The method used in this study is the internal consistency by determining the Cronbach alpha coefficient (α). Cronbach alpha values must be above 0.6 to confirm the consistency and reliability of the constructs [36]. The higher the value of Cronbach's alpha coefficient (α), the greater the reliability of the internal consistency. Table II shows the results of the Cronbach alpha coefficient (α) analysis. The values of the Cronbach's alpha coefficient of all the constructs range from 0.798 to 0.939, suggesting that the entire scale has a good level of internal consistency.

Table III shows the demographic characteristics of the respondents. Most respondents participated in this study are from government agencies (92.6%), followed by private agencies (4.1%) and statutory bodies (3.3%). Majority of the respondents have been in the industry for 5-15 years. 44.9% of the respondents have less than 3 years of experience in ISM while 51% have over 3 years of experience in ISM. In terms of ISM specialisation, 46.1% of respondents are in the ISM team, 9.9% from the coordinator team, 4.1% are in the audit team, and 10.7% are involved in multiple categories.

TABLE. II. Internal Consistency

Factors	**Number of Items**	**Value of Cronbach's Alpha (α)**
Top Management	5	.884
IS Coordinator Team	3	.843
ISM Team	5	.906
IS Audit Team	5	.939
Employees	3	.897
Third Parties	3	.903
IS Policy	4	.905
IS Procedures	4	.926
Resource Planning	2	.798
Competency Development & Awareness	2	.855
Risk Management	2	.923
Business Continuity Management	2	.884
IS Audit	3	.922
IT Infrastructure	2	.875

TABLE. III. RESPONDENTS' DEMOGRAPHIC CHARACTERISTICS

Respondent characteristics	**Frequency**	**Percentage (%)**
Agency Type		
Government	225	92.6
Statutory Body	8	3.3
Public Agency	10	4.1
Length of Service		
Not stated	2	.8
Less than 5 years	26	10.7
5 – 10 years	92	37.9
11-15 years	77	31.7
Over 15 years	46	18.9
ISM experience		
Not stated	10	4.1
Less than 3 years	109	44.9
3 - 6 years	69	28.4
Over 6 years	55	22.6
ISM specialization		
Not specified	5	2.1
Top management	5	2.1
Coordinator team	24	9.9
ISM team	112	46.1
Audit team	10	4.1
Employees	52	21.4
Others	9	3.7
Combined categories	26	10.7

The distribution of respondents' feedback on the ISM success factors are shown in Table IV. The findings indicate that most respondents agreed that the fourteen factors contribute to the success of ISM implementation. This is demonstrated by the number of respondents (N) who chose "Agree" and "Strongly Agree" values are higher than the number of respondents who chose "Strongly disagree" and “Disagree”. This indicates positive agreements towards all factors. These findings confirm the previously gathered qualitative data.

Table IV shows that Top Management is the most highly agreed factor concerning the success of ISM implementation, followed by IS Policy, IS Procedures, ISM Team, IT Infrastructure, Risk Management and IS Coordinator Team (N for “Strongly Agree” > 50%).

Fig. 2 shows the median values for the whole factors. Seven factors, namely Top Management, IS Coordinator Team, ISM Team, IS Policy, IS Procedures, Risk Management, and IT Infrastructure have a median value of 5 while other factors have a median value of 4.

TABLE. IV. DISTRIBUTION OF RESPONDENTS' FEEDBACK ON ISM SUCCESS FACTORS

ISM Success Factors	**Strongly disagree**	**Disagree**	**Somewhat agree**	**Agree**	**Strongly agree**
	N	**N**	**N**	**N**	**N**
Top Management	0 (0.0%)	3 (1.2%)	17 (7.0%)	71 (29.2%)	152 (62.6%)
IS Policy	0 (0.0%)	0 (0.0%)	15 (6.2%)	79 (32.5%)	149 (61.3%)
IS Procedures	0 (0.0%)	0 (0.0%)	13 (5.3%)	85 (35.0%)	145 (59.7%)
ISM Team	0 (0.0%)	0 (0.0%)	10 (4.1%)	89 (36.6%)	144 (59.3%)
IT Infrastructure	0 (0.0%)	0 (0.0%)	17 (7.0%)	90 (37.0%)	136 (56.0%)
Risk Management	0 (0.0%)	1 (0.4%)	14 (5.8%)	101 (41.6%)	127 (52.3%)
IS Coordinator Team	0 (0.0%)	2 (0.8%)	11 (4.5%)	104 (42.8%)	126 (51.9%)
Competency Development & Awareness	0 (0.0%)	0 (0.0%)	22 (9.1%)	104 (42.8%)	117 (48.1%)
Employees	0 (0.0%)	2 (0.8%)	24 (9.9%)	105 (43.2%)	112 (46.1%)
Resource Planning	0 (0.0%)	3 (1.2%)	21 (8.6%)	108 (44.4%)	111 (45.7%)
Business Continuity Management	0 (0.0%)	1 (0.4%)	20 (8.2%)	115 (47.3%)	107 (44.0%)
IS Audit	0 (0.0%)	2 (0.8%)	24 (9.9%)	111 (45.7%)	106 (43.6%)
IS Audit Team	0 (0.0%)	4 (1.6%)	26 (10.7%)	110 (45.3%)	103 (42.4%)
Third Parties	0 (0.0%)	5 (2.1%)	54 (22.2%)	106 (43.6%)	78 (32.1%)

Fig. 3 shows mode value for the whole factors. Ten factors have the mode value of 5 and four factors have the mode value 4. Based on the mode and medium values obtained, it clearly verifies that all the factors affecting ISM's success.

Meanwhile for the items analysis, the minimum, maximum, median and mode values for each item are tabulated as in Table V. Generally, 45 items were analysed from a total of 243 respondents.

The findings demonstrate that all the items have a maximum value of 5. For the minimum value, there are three items that have a minimum value of 1, which are commitment-feedback of top management, communication skills of audit team, and awareness programmes, while the rest of the items have the minimum value of 2 and 3. In addition, all the items have a median and mode value of 4 and 5. In short, these findings indicate that the respondents agreed that all the factors and their items contribute to the success of ISM implementation.

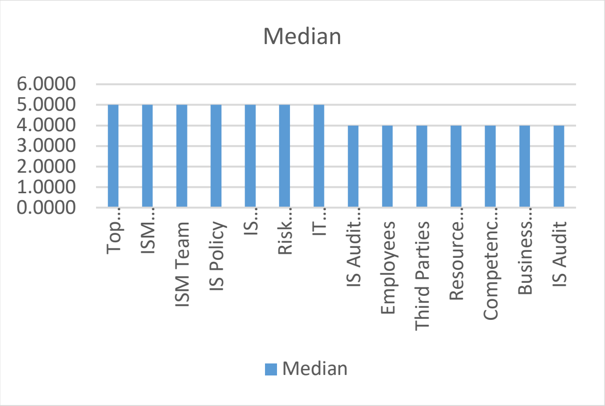


Fig. 2. Median Values for ISM Implementation Success Factors.

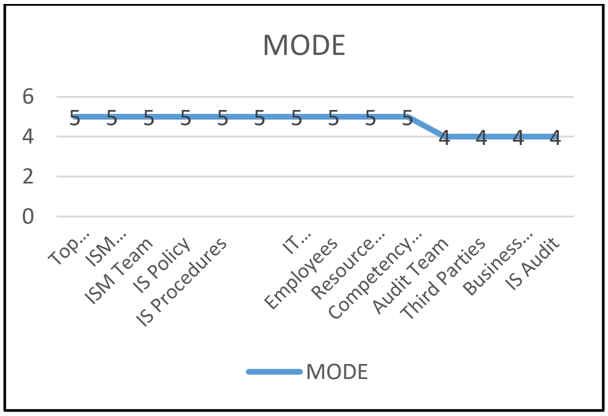


Fig. 3. Mode Values for ISM Implementation Success Factors.

A. *Factor Analysis*

Factor analysis is used to confirm the contributing factors of ISM implementation. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity were first conducted to determine the sampling adequacy. Fig. 4 shows that the score of Bartlett’s Test is 91 (significance 0.000), which means there is a real inter-variable correlation (significance < 0.05). The score of KMO is 0.936, which means all variables in this study could be used for further analysis.

Table VI shows the Measure of Sampling Accuracy (MSA) value obtained by each factor. Any factor that has the score of MSA > 0.5 will be seen as valid. The findings show that the MSA scores for all factors are greater than 0.5.

Table VII displays the result of the factors loading. It shows that the result of all factors were > 0.3. The factors were grouped into two components; component 1 and component 2. Component 1 includes the factors in the aspect of process, organisational documents and technology which are Business Continuity Management, Risk Management, Competency Development & Awareness, Resource Planning, IS Audit, IS Policy, IS Procedures and IT Infrastructure. Meanwhile components 2 represent the factors in the aspect of people which are IS Coordinator Team, Top Management, ISM Team, Employees, IS Audit Team and Third Parties. Based on the analysis, it can be concluded that all fourteen factors contribute to the success of ISM implementation.

TABLE. V. ITEMS ANALYSIS OF ISM SUCCESS FACTORS

Factors	Items	Min.	Max.	Median	Mode
Top management	knowledge-objectives	3	5	5	5
	knowledge-issues	3	5	5	5
	leadership	3	5	5	5
	commitment-resources	2	5	5	5
	commitment-feedback	1	5	5	5
IS Coordinator team	knowledge	3	5	5	5
	commitment	2	5	5	5
	communication skill	3	5	5	5
ISM team	knowledge	3	5	5	5
	skill	3	5	5	5
	commitment	2	5	5	5
	readiness	2	5	4	4
	cooperation	3	5	5	5
IS Audit team	knowledge	3	5	5	5
	auditing skill	2	5	5	5
	commitment	2	5	5	5
	cooperation	3	5	4	5
	communication skills	1	5	4	4
Employees	awareness	2	5	5	5
	compliance	2	5	5	5
	motivation	2	5	4	4
Third Parties	awareness	2	5	4	4
	compliance – IS policy	2	5	4	5
	compliance – agreement	2	5	4	5
IS Policy	clear	3	5	5	5
	comprehensive	2	5	5	5
	communicated	3	5	5	5
	reviewed	3	5	5	5
IS Procedures	clear	2	5	5	5
	complete	2	5	5	5
	reviewed	2	5	4	5
	communicated	2	5	5	5
Resource Planning	financial resources	2	5	4	5
	human resources	3	5	5	5
Competency Development & Awareness	awareness program	1	5	4	4
	training	2	5	5	5
Risk Management	risk assessment	2	5	5	5
	risk treatment	2	5	5	5
Business Continuity Management	business continuity plan	3	5	5	5
	simulation (testing)	3	5	4	5
IS Audit	audit programs	3	5	4	4
	audit findings and reporting	3	5	4	5
	follow-up audit	2	5	4	4
IT Infrastructure	software	3	5	4	4
	hardware	3	5	4	5

B. Kruskal-Wallis H test

A non-parametric test Kruskal-Wallis H is carried out to investigate any significant differences in the respondents' views among various sectors (public, private and statutory bodies). Fig. 5 shows the results of Kruskal-Wallis H test analysis. The results indicate that there is no significant difference in the view of the ISMS success factors among public, private and statutory bodies respondents [x2 (2, N = 243) = .154, p> 0.05]. In other words, respondents of the public, private and statutory bodies have similar views on the factors that contribute to the success of ISM implementation.

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.936
Bartlett's Test of Sphericity	Approx. Chi-Square	3093.826
	df	91
	Sig.	.000

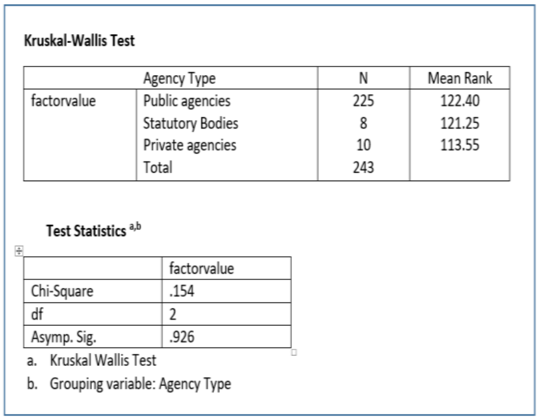
Fig. 4. KMO and Bartlett's Test.

TABLE. VI. ANTI-IMAGE CORRELATION MATRIX OF ITEMS

Factors	**MSA Score**
Top Management	.930
IS Coordinator Team	.918
ISM Team	.942
IS Audit Team	.917
Employees	.952
Third Parties	.964
IS Policy	.892
IS Procedures	.904
Resource Planning	.969
Competency Development & Awareness	.960
Risk Management	.937
Business Continuity Management	.949
IS Audit	.930
IT Infrastructure	.963

TABLE. VII. FACTORS LOADING

Rotated Component Matrix[a]		
	Component 1	Component 2
Business Continuity Management	.828	
Risk Management	.814	
IS Procedures	.792	
Competency Development & Awareness	.783	
Resource Planning	.763	
IT Infrastructure	.746	
IS Policy	.743	
IS Audit	.711	
IS Coordinator Team		.843
Top Management		.777
ISM Team		.773
Employees		.723
IS Audit Team		.715
Third Parties		.688



Kruskal-Wallis Test

	Agency Type	N	Mean Rank
factorvalue	Public agencies	225	122.40
	Statutory Bodies	8	121.25
	Private agencies	10	113.55
	Total	243	

Test Statistics a,b

	factorvalue
Chi-Square	.154
df	2
Asymp. Sig.	.926

a. Kruskal Wallis Test
b. Grouping variable: Agency Type

Fig. 5. Kruskal-Wallis H Test.

V. CONCLUSION AND FUTURE WORK

This study has confirmed fourteen factors and forty-five items that contribute to the success of ISM implementation. The factors and items were confirmed quantitatively through a survey. The fourteen factors are Top Management, IS Coordinator Team, ISM Team, IS Audit Team, Employees, Third Parties, IS Policy, IS Procedures, Resource Planning, Competency Development and Awareness, Risk Management, Business Continuity Management, IS Internal Audit, and IT infrastructure. All these factors and items are classified into four aspects, namely, Human, Organisational Documents, Process and Technology that should be taken into account in order to ensure the effectiveness of ISM implementation. These findings shall be used by practitioners to strategise ISM initiatives in their respective organisations. As ISM initiatives are indeed continuous, future work may need to look into ways on how to measure ISM implementation level based on these factors.

ACKNOWLEDGMENT

The authors would like to thank Universiti Kebangsaan Malaysia for supporting the research. The authors also thank the respondents who participated in the study.

REFERENCES

[1] J. D. E. Lange, R. V. O. N. Solms, and M. Gerber, "Information Security Management in Local Government," pp. 1–11, 2016.

[2] M. Dhingra, "Review on Information Security Management," Int. Conf. Futur. Trends Eng. Sci. Humanit. Technol., pp. 1–4, 2016.

[3] A. Kurnianto, R. Isnanto, and A. Puji Widodo, "Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs," in E3S Web of Conferences, 2018, vol. 31, p. 11013.

[4] M. a Kuypers, T. Maillart, and E. Paté-cornell, "An Empirical Analysis of Cyber Security Incidents at a Large Organization," pp. 1–22, 2016.

[5] K. Hajdarevic and P. Allen, "A new method for the identification of proactive information security management system metrics," in Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on, 2013, pp. 1121–1126.

[6] R. A. Abbas, M. R. Mokhtar, R. Sulaiman, Z. A. Othman, and A. M. Zin, "Impact of disasters in Southeast Asia on Malaysian computer networks," J. Theor. Appl. Inf. Technol., vol. 37, no. 2, pp. 188–198, 2012.

[7] M. I. Alshar'e, R. Sulaiman, M. R. Mukhtar, and A. M. Zin, "A user protection model for the trusted computing environment," J. Comput. Sci., vol. 10, no. 10, pp. 1692–1702, 2014.

[8] Y. Bobbert and H. Mulder, “Governance Practices and Critical Success factors suitable for Business Information Security,” in International Conference on Computational Intelligence and Communication Networks Governance, 2015, pp. 1097–1104.

[9] F. Mijnhardt, T. Baars, and M. R. Spruit, “Organizational Characteristics Influencing Information Security Maturity,” J. Comput. Inf. Sci., vol. 56, no. 2, pp. 106-115, 2016.

[10] MyCERT, “Reported Incidents based on General Incident Classification Statistics 018,” 2018. Available at https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=e49c91c1-4b04-4748-8152-294764f9c8dc

[11] H. Kong, J. Woo, T. Kim, and H. Im, “Will the Certification System for Information Security Management Help to Improve Organizations' Information Security Performance ? The Case of,” vol. 9, no. June, pp. 1–12, 2016.

[12] M.S. Mohd Asri and R. Rozilawati, “An assessment model of information security implementation levels,” in Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, 2011, pp. 1–6.

[13] M. Zammani and R. Razali, “Information security management success factors,” Adv. Sci. Lett., vol. 22, no. 8, pp. 904–913, 2016.

[14] N. Maarop, N. Mustapha, R. Yusoff, R. Ibrahim, and N. M. M. Zainuddin, “Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation,” Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng., vol. 9, no. 3, pp. 884–889, 2015.

[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] M. M. Edwards, “Identifying Factors Contributing Towards Information Security Maturity in an Organization,” Nova Southeastern University, 2018.

[17] S. Yulianto, C. Lim, and B. Soewito, “Information Security Maturity Model: A Best Practice Driven Approach to PCI DSS Compliance,” in In Region 10 Symposium (TENSYMP), 2016, pp. 65–70.

[18] M. Zammani and R. Razali, “An Empirical Study of Information Security Management Success Factors,” Int. J. Adv. Sci. Eng. Inf. Technol., vol. 6, no. 6, pp. 904–913, 2016.

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

[20] R. Z. W. S. M.S, “CyberSecurity Malaysia: Towards Becoming a National Certification Body for Information Security Management Systems Internal Auditor,” vol. 10, no. 8, pp. 2907–2910, 2016.

[21] M. Suomu, “Automated ISMS control auditability,” no. May, 2015.

[22] L. Yang, “Study on the Improvement of the Internal Audit Work in IT Environment,” in 2011 Fourth International Symposium on Knowledge Acquisition and Modeling, 2011, pp. 233–236.

[23] M. Razilan, A. Kadir, S. Norwahidah, S. Norman, S. A. Rahman, and A. Bunawan, “Information Security Policies Compliance among Employees in Cybersecurity Khalid S . Soliman International Business Information Management Association (IBIMA),” no. November 2016, 2017.

[24] W. Sung and S. Kang, “An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness,” Proc. 18th Annu. Int. Conf. Digit. Gov. Res., pp. 84–93, 2017.

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

[26] K. Haufe, “Maturity based approach for ISMS,” Universidad Carlos III de Madrid, 2017.

[27] A. Singh, “Improving information security risk management,” ProQuest Diss. Theses, p. 121, 2009.

[28] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, “Current challenges in information security risk management,” Inf. Manag. Comput. Secur., vol. 22, no. 5, pp. 410–430, 2014.

[29] N. H. Mansol, N. Hayaati, M. Alwi, and W. Ismail, “Success Factors towards Implementation of Business Continuity Management in Organizations,” Int. J. Digit. Soc., vol. 5, no. 1/2, pp. 869–871, 2014.

[30] N. H. Mansol, N. Hayaati, M. Alwi, and W. Ismail, “Embedding Organizational Culture Values towards Successful Business Continuity Management (BCM) Implementation,” in 2014 International Conference on Information Technology and Multimedia (ICIMU), 2014, pp. 31–37.

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

[32] A. Tsohou, S. Kokolakis, C. Lambrinoudakis, and S. Gritzalis, “A security standards' framework to facilitate best practices' awareness and conformity,” Inf. Manag. Comput. Secur., vol. 18, no. 5, pp. 350–365, 2010.

[33] R. Valverde, M. Wolden, R. Valverde, and M. Talla, “The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Change Management System,” IFAC-PapersOnLine, vol. 48, no. 3, pp. 1846–1852, 2015.

[34] A. A. Norman and N. M. Yasin, “Information Systems Security Management (ISSM) Success Factor: Retrospection From the Scholars,” Proceedings of the 11th European Conference on Information Warfare and Security, no. July 2012. pp. 339–344, 2012.

[35] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 2013.

[36] H. D. Ghazali, “Kesahan dan kebolehpercayaan dalam kajian kualitatif dan kuantitatif,” J. Pendidik. Maktab Perguru. Islam, no. 1985, pp. 61–82, 2005.