International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:3, 2015

Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation

Nurazean Maarop, Noorjan Mohd Mustapha, Rasimah Yusoff, Roslina Ibrahim, Norziha Megat Mohd Zainuddin

***Abstract*—**The goal of this study is to identify success factors that could influence the ISMS self-implementation in government sector from qualitative perspective. This study is based on a case study in one of the Malaysian government agency. Semi-structured interviews involving five key informants were conducted to examine factors addressed in the conceptual framework. Subsequently, thematic analysis was executed to describe the influence of each factor on the success implementation of ISMS. The result of this study indicates that management commitment, implementer commitment and implementer competency are part of the success factors for ISMS self-implementation in Malaysian Government Sector.

***Keywords*—**ISMS Success Factors, IT Project Management, IS Success, Information Security.

I. Introduction

THE emergence of technology has broadened the information security threats to business organization. Many information security management models have been developed to help organization managing their information security practices. The commonly applied practices are COBIT, BS 17799, ISO/IEC 27001:2005 [1]. Currently, the only auditable information security management system is the International Organization of Standardization (ISO), Information Security Management System (ISMS) standard which provides an adequate information security control for managing business risk [2]. The ISMS implementation benefits the organizations in many ways. Some of the identified benefits of implementing ISO 27001 based on business risk are fewer incidents and disruption of services, more effective and faster incident response management, focus on proactive measures, lower client audit requirements, less time and money spent on damage limitation measures, less resource spent on finding new customers and investors, greater productivity, better understanding of business information processes and better able to reassure customers and internal parties [3], [4].

The cognizance in preserving and securing the critical and sensitive information, weaknesses in managing secure information as well as the increasing threat of gathering information discovery in government website have derived the Malaysian government to adopt this standard [5].

The implementation of ISMS standard in government sector started in 2006 [5]. The National Registration Department (NRD) was certified for ISMS in 2008 [5]. Subsequently the government had directed some public agencies to be engaged in CNII certified ISMS MS ISO/IEC 27001:2007 February 2013 which then led to the effort for self-implement [5]. All agencies were directed to self-implement the ISMS due to budget constraint [6]. One of the motivation factors of ISMS self- implementation is appointment of high cost of consulting firm [6]. NRD was directed to guide and help the Internal Affairs Agencies to get the certification within the time given. Unfortunately, to the authors' knowledge through problem background study, none of the agencies were able to be certified as scheduled.

It becomes a burden to the government agencies if the implementation has to consume more time to be implemented. Therefore, in order to ensure the success of ISMS implementation in government agencies, there is a need to identify what are the success factors and issues affecting the success of ISMS implementation.

II. Background

Ku et al. [7] indicate factors that influence the ISMS self-implementation are past experience of other standards, level of documentation, understanding the clause, understanding risk assessment procedure, top management support, culture of organization, auditing function, awareness and education and compatibility with existing procedure. The establishment and development of ISMS in an organization requires an in-depth understanding of the standard clause [7]. Hence, during the development of ISMS, the ISMS implementer must follow the PDCA cycle which provide an overall guidance in implementing ISMS. The most challenging process is the risk assessment because the process requires a comprehensive understanding and considerable knowledge in information security [8]. Risk assessment is done by the ISMS implementer team because they are the ones facing difficulties in engaging the asset owner in the risk assessment team.. The other challenge in the ISMS implementation is at organizational level [9]. ISMS implementation requires managerial awareness and commitment [9], [10]. The management commitment can be shown by providing

Nurazean Maarop and Rasimah Che Yusoff are senior lecturers at the Universiti Teknologi Malaysia (phone: 603-22031341; e-mail: nurazean.kl@utm.my, rasimah.kl@utm.my).

Noorjan Mustaffa is a Senior IT Officer at the Public Service Department of Malaysia (e-mail: janoki02@yahoo.com)

Roslina Ibrahim is a senior lecturer at the Universiti Teknologi Malaysia (phone: 603-603-21805215; e-mail: iroslina.kl@utm.my).

Norziha Megat Mohd Zainuddin is a senior lecturer at the Universiti Teknologi Malaysia (phone: 603-21805221; e-mail:norziha.kl@utm.my).

appropriate resource, establishing the ISMS, and providing training, awareness and competency. Proper project plan should be in place [10]. Without a well-defined and well-developed ISO 27001 project plan, the implementation of ISO 27001 would be such a time and cost - consuming exercise [11]. The ISMS implementation succession is highly depends on human factor [12]. Therefore, there is a need to have appropriate skill and knowledge of ISMS standard on government agency's implementer to ensure effectiveness of ISMS implementation.

The challenges of ISMS implementation can occur from many aspects including managerial, individual and organizational. Challenges in assessing organization risk can occur due to lack of tools in the automation of risk identification which requires human expertise with comprehensive understanding and appropriate knowledge in information security [13].

Previous research shows that organizational factor [7], [14], [15] and human factor [12], [16] plays an important role in establishing and implementing ISMS.

As the concern of information security rise, the adoption of ISMS standard grows too. However, the need of extensive human resourcing and lack of understanding of ISMS effectiveness become major issues [17]. The processes involved in the plan phase are most crucial components in ISMS establishment as these include policy making and distribution, assets management, risk management, document management and control selections [11]. Apart from this, a structured security organization landscape from top management need to be established to ensure the information security governance [18].

Basically, the ISMS standard provides a common base for effective security management [3]. The Plan-Do-Check-Act (PDCA) model proposed by the standard ensures the continual improvement of the ISMS [16]. The Plan Phase activities are essential to ISMS implementation because the activities in this phase will determine how to control and manage the information security in the organizations [19]. The Do, Check and Act (PDCA) Phases activities will ensure that the planned activities will be carried out appropriately and improved necessarily [19].

Since, the study has focused on the Plan phase of the PDCA model, so the selected success factors were deduced accordingly from the literature review. These elements were selected as the basis for exploring and understanding the factors that may influence ISMS implementation in the government agencies in Malaysia. In summary, the derived success factors for ISMS implementation are shown in Table I. Based on theory-driven and prior-research driven design qualitative method [20], a conceptual framework comprising key issues of ISMS Plan Phase Self Implementation Success Element addressed in Table I was developed. The framework puts emphasis on highlighted issues and organized into four tentative themes including the Net Benefit as an indicator of success implementation of ISMS. The proposed model for ISMS Plan Phase implementation Success is illustrated in Fig. 1.

TABLE I
DEDUCED RELATED FACTORS

Element	Factors	Reference
Management Commitment	Management commitment, involvement and support, stakeholder communication, structured project, access to external expertise, awareness of information security and education, structured organization mission, budgetary and financial	[7], [15], [21]-[24]
Implementer Competency	Motivated project team, capabilities on project, management, commanding, analytic, communicative, level of documentation and standardization	[7],[15], [23]-[25]
Implementer Commitment	Project management, implementation and change management skill, holistic view, degree of understanding the clauses, procedures of asset identification and risk assessment, past experience of implementing other standards, present of framework to implement, maintain, monitor and improve IS, existing auditing regulation and infrastructure.	[7],[15], [22]-[24]
Net Benefit	Organizational performance, effect on work practices, perceived usefulness	[26]

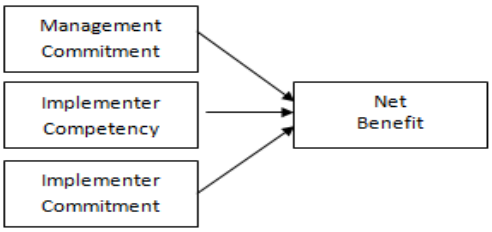

Fig. 1 Conceptual Framework of ISMS Plan Phase Self-Implementation Success

III. METHODOLOGY

A purposive sampling was applied involving key informants to respond to qualitative survey. Eight ISMS implementer team members in the Immigration Department who had actively experienced and involved in ISMS Plan Phase Self Implementation were invited to participate in this study and only five officers agreed to participate. The semi structured interviews were conducted which took an average of forty-five minutes for every participation. Narrative analyses were performed based on the themes deduced from the literature review. In line with a deductive qualitative approach, a start-list of codes was developed and used to facilitate the analysis and documentation of findings. In this regard, the generation of start-list of code for interview questions was based on Table II.

Preliminary study was conducted with three expert participants to seek relevancy of the variables used in the interview schedule before the actual interviews were held in the respective agency office. There were five participants involved in the interviews and the profile is shown in Table III.

IV. RESULT

A. Net Benefit

It is proven in the context of the study that ISMS self-implementation has affected organizational performance by reducing cost on ISMS implementation, managing information security systematically, increasing implementers competency

and improving data center infrastructure.

TABLE II
START LIST OF CODES

Theme	Code	Description
Management Commitment	MC1	Management Commitment & Support
	MC2	Stakeholder communication
	MC3	Structured Project
	MC4	Awareness on Information Security
	MC5	Organization mission
	MC6	Access to external expertise
Implementer Commitment	ICM1	Committed team
	ICM2	Capabilities on Project Management
	ICM3	Motivation
	ICM4	Documentation and Standardization
Implementer Competency	ICP1	Skill on Change Management
	ICP2	Skill on Holistic View
	ICP3	Ability towards Understanding Clause
	ICP4	Risk Assessment & Asset Identification
	ICP5	Past Experience
	ICP6	Approach & Framework
	ICP7	Audit infrastructure
Net Benefit	B1	Organizational Performance
	B2	Perceived Usefulness
	B3	Effect on Work Practice

TABLE III
PARTICIPANTS PROFILE

Participant	Post	Role and Experience
1	IT Senior Officer	7 years as ISMS Implementer
2	IT Senior Officer	3 years as ISMS Implementer
3	IT Manager	3 years as ISMS Coordinator
4	IT Officer	2 years as ISMS Coordinator
5	IT Officer	4 years as ISMS Implementer

Participant 1 claims that "…firstly, from cost perspective, not much was spent, we only pay for certification audit fee. Other costs such as for training purpose and others are mostly sponsored by MKN and MAMPU. Further there is an agency in the ministry, provides unpaid training. Secondly, for data security in immigration, we feel that all the processes related to data center are in compliant to the standard..."

Participant 3 also claims that "…firstly, cost reduction for the government has improved the department image and the management is happy with what we had done…I believe that the ISMS implementer competency level has increased compared to when we started the ISMS implementation especially in regard to filing and record management…"

Participant 4 points out that "…very beneficial, we audit the data center and received comment on CCTV, so there is an improvement. We did procurement tender evaluation process to improve the security at the data center..."

Three participants claim that by self-implement ISMS, the work practices have changed significantly. The major change was on the documentation of standard operating procedure which brings uniformity and understanding in executing each procedure. Furthermore, documentation helps the implementer to enforce changes in work practices. Both parties understand their responsibility and record tracking are more structured and manageable. For example, participant 3 remarks "…all the work we do in day to day basis was unrecorded, but now there is a SOP as a reference. There are documents to be referred to, there is a standard in documentation, and the document was reviewed and updated…"

B. Management Commitment

All of the participants expressed that management commitment is the most influencing factor in ISMS self-implementation. Management commitment plays an important role to ensure that the ISMS implementer have a clear direction in implementing ISMS. Therefore, management commitment must include activities such as ensuring that the proper resources are available to work, all employees affected by the ISMS structuring have proper training, awareness program need to be held, and ISMS competency must be monitored. In addition, management also can demonstrate their commitment by conducting management review at the planning interval. Management commitment affects the duration of ISMS self-implementation as remarked by the participant 1 as *"…If there are any problems that cannot be resolved in the ground, then the implementer will refer to the management and management will give other instruction on how to execute ISMS..."*

All participants claim that the management demonstrates their commitment by addressing all related activities given. Moreover management commitment and support was showed by giving approval for ISMS activities, attending courses, budget allocation and allocation of time of discussing the ISMS implementation issues. For example, Participant 1 claims that "…*improvement can be seen in the process of approval, scope identification, approval for guidelines, SOP compliance, fast approval for attending courses and most importantly budget allocation…"*

This study indicate that for stakeholder communications, the management provide various channel to discuss the ISMS self-implementation issues as well as transferring ISMS direction to the agency. Regular meetings were held at the low ranked operation discussing ISMS self-implementation activities as well as high ranked level for giving directions and approval as mentioned by Participant 1, "…*we have a number of channels. Firstly we have a meeting, IT Division management meeting, then we have for higher officials, we have Immigration's ICT committee. So through the meeting we reported the ISMS implementation constraint and status to the management.* Participants 3, "…*We comply with the directions of KDN and MAMPU and we try to follow the timeline given…"*

In ensuring the ISMS self-implementation success or any projects, a proper structured project should be developed and approved by the management. Majority of participants agree that the management has demonstrated their commitment by revising the structure of the project before giving approval to it. This is due to their obligation in ensuring that the selected ISMS implementer can perform their responsibility appropriately. One of the participants mention *"…yeah right, in terms of implementation, we only draft the governance*

structure of ISMS, ISMS implementation team, so everything is approved by our CIO..".

All participants claim that the ISMS self-implementation is one of the activities which required by the management to achieve organization mission as mention by two of the participants; Participant 2 states that *"… especially, when immigration priorities security…."* and Participant 3 claims that *"…there is a reason, ISO (ISO 9000) was long implemented in immigration, so ISMS is an additional requirement …"*

Awareness is one of the activities related closely to the management commitment. Participants admitted that the management has provided sufficient awareness and training to all personnel involved in ISMS self-implementation including third party even though there is a constraint in the budget allocation. The awareness and training provided covers not only for ISMS standards and processes but also to respective technical process. This is to ensure that the ISMS implementer can easily adapt the ISMS standard to their work practices.

Participants have acknowledged that the present of external expertise is important to ensure the success of ISMS self-implementation. Due to this, since they are facing budget constraint, the management has directed the ISMS implementer team to seek for external expertise within the ministry and other government agencies which provide consultancy on ISMS implementation. For example, Participant 1 mentions that *"… agency in ministry are blessed because one of the agency was certified earlier, then the government direction through MAMPU can provide free training for agencies that want to implement ISMS…"*

During the analysis, all of the participants agreed that they gained enough management commitment to pursue the ISMS self-implementation. The findings of this study illustrate that the management commitment is one of the most critical success factor that drive the ISMS implementer team to lead the success of ISMS self-implementation. Participants acknowledge that the management clearly provides appropriate action for each related activities in order to ensure the success of ISMS self-implementation.

C. Implementer Commitment

This study identifies that the implementer commitment requires the ISMS implementer team to allocate certain amount of time to concentrate on ISMS implementation regardless of their daily basis work schedule. It is a practice in government agency that the person who responsible for ISMS is also responsible for other scope as well. So, the ISMS implementer need to have a proper planning in their daily work schedule to ensure that an appropriate time should be allocated to focus on ISMS processes in ensuring the success of ISMS implementation.

The participants disclose that throughout ISMS implementation in their agency, the ISMS implementer team gives their full commitment in each ISMS processes. In addition to that, they meet on weekly basis to resolve any issues that can cause ISMS implementation failure. The result of this study show that that implementer commitment is critical to self-implement ISMS as mentioned by these participants; Participant 1 claims that *"…Very impressive, we divided the tasks for each implementer, then if there is any problem we will hold weekly meetings, especially at the very beginning of the ISMS implementation. Weekly meeting was held to resolve any pending issues. It is very important, because if the team does not perform their duties, they cannot move on to implement ISMS. For example, during the internal audit, we get an observation for improvement (OFI) or non-conformance, we ask the implementer to address the non-conformance of OFI. If the con-conformance and OFI are not properly addresses, we cannot proceed with the certification audit…*". Participant 2 expresses that "*…Indeed. Then it needs to be emphasized on the responsibility of the implementer to ensure that ISMS implementation can move seamlessly. If not, it feels that ISMS implementation will fail…*". Participant 3 points out that *"…because they are the ones who developed the SOP and ensure that the documented SOP was implemented accordingly…"*

This study shows that all participants acknowledge that having a committed team, level of documentation and standardization and motivated project team can improve implementer commitment. However, identified capabilities of implementer commitment are more seen to be towards specific area such, technical, standard, management and documentation.

ISMS implementation requires a dedicated team who are committed to focus and execute each process at every phase. Thus, the person involved must give full co-operation in every activity such as attending meetings, briefing, audit session, awareness program, etc. Apparently, this will help to smoothly execute the PDCA cycle because the team are fully aware of the ISMS implementation status as mentioned by Participant 3: "*…very important because we do not want the implementers team to substitute to someone else when we call for a meeting…*" . The study also found that the implementer team was motivated by their management commitment and the success of ISMS implementation in other agencies which dealt with external expertise. Despite the difficulties to self-implement ISMS, the implementer teams accept the challenges, motivate themselves and finally able to self-implement the ISMS successfully. Participant 1 states that "*…first we have committed team then we have management that gives good motivation to the implementers…*"

Implementing any other ISO standards requires standard documentation. The participants were asked about how does the level of documentation in their agency help in implementing ISMS. Surprisingly, in their agency, there is no proper standard documentation. Thus, the implementer's team was struggling at first, to start documenting all their procedure to meet the ISMS requirements. The participants agree that if they have the standard documentation, the ISMS implementation would be much easier. Thus, the ISMS implementers spend a lot of effort in documenting their procedures and policy. Participant 1 explains that "*...they were directed by their management to focus on the documentation by giving them approval to do the document development and*

review in other places…" Participant 4 claims that "…*because all of the SOPs come from ISMS implementer themselves, and they understand well their SOPs content*…"

D.Implementer Competency

This study reveals that the required competency are implementation and change management skill, 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. In addition they commented that the implementers must acquire at least three competencies to obtain appropriate skill and knowledge in order to comprehend the complete cycle of ISMS implementation and these are implementation and change management skill, understanding of the standard and present of an approach or framework to implement, maintain, monitor and improve IS. For example, some remarks are:

"…one of them about understands the ISMS, then skill, for example, the implementer who is responsible for ICT department needs to have skill on how to adapt his daily operations to be included in the ICT SOP. There is a need to have change management skill…" (Participant 1)

"…if it is for beginner basic knowledge was ok, meaning that firstly, give him chance to read the standard even though he might not understand it. Send him for awareness fresh course, to gain knowledge on ISMS…" (Participant 3)

The study reveals that most of the participants acknowledge that having a holistic view of the ISMS gave them an overall understanding about PDCA cycle, knowledge on involved processes in every phase in and develop skill on how to link business processes with information use and information technology infrastructure. In addition, the ISMS also needs to consider and be integrated with the organization's other policy and management processes. In this way ISMS is considered as a business solution in response to the organization's information security management.

Participant 1 believes that "…*holistic view help us in implementing ISMS. In our department, we divided the tasks, we have implementers team, project team and ISMS coordinator so the most important thing is in every department there is a coordinator who understands every department processes. Then, the coordinator will inform the project/implementers team what is required to be done at a time..."*

Participant 3 agrees that "…*some will ignore as if they don't know what to do. Hence, the implementer needs to see the overall ISMS and then relate to his/her job scope…"*

In the Plan Phase of the PDCA cycle, the study reveals that risk assessment, scope and project structure identification requires a competent implementer. Based on that, two of the participants agreed that risk assessment was a challenge to them as ISMS implementers as they must be competent enough in this activity to ensure the success of ISMS implementation. Risk assessment was done to assess the possible risk toward each asset and proposed mitigation for each identified risk. Thus, the implementer needs to have the knowledge in identifying risk for each asset, assessing risk and identifying mitigation process.

In government sector, risk assessment was rarely done in an ICT environment. MyRAM was introduced by MAMPU to help agency assess their organizational risk but very few government officers involve in this assessment. Thus, risk assessment in ISMS becomes a burden to the implementers who does not have any experience in assessing risk. Participant 1 asserts that *"…for me the most problematic is to prepare risk assessment and risk treatment plan, it takes a long time and if the auditor find that it is wrong , we have to redo..."*.

In addition to that, another participant claims that defining the scope also requires implementer competency. The definition of the scope should determine the extent to which you want the ISMS to be applied in your organization. At the beginning, the implementers thought that they would begin with a small scope involving only three officers. Later, they realized that that the defined scope is not sufficient enough and covers only small percentage of their data center operations. As required by the ISMS standard, the scope should have a list comprises the areas, locations, assets, and technologies of the organization that will be controlled by the ISMS. One participant remarks *"…need to define the scope in the first place as the scope was changed several times until* it *is finalized…"*

E. Summary of Interview Result

Apart from narrative analysis, the result of the coding analysis has also included the influential rating for each of sub-themes towards ISMS self-implementation. In order to rate the influence, the participants answers were categorized into three codes "2 = Influence", "1 = Not Influence" and "X = Neither". The finding shows that most of the success factors deduced earlier have influenced the ISMS self-implementation except for capabilities on project management. Table IV shows the influenced success factor for ISMS self-implementation.

TABLE IV
SUMMARY OF INTERVIEW RESULT

Theme	Description (Sub-Themes)	Participant				
		1	2	3	4	5
Management Commitment	Management Commitment & Support	2	2	2	2	2
	Stakeholder communication	2	2	2	2	2
	Structured Project	2	2	2	2	2
	Organization Mission	2	2	2	2	2
	Access to External Expertise	2	2	2	2	2
Implementer Commitment	Committed team	2	2	2	2	2
	Capabilities on Project Management	1	1	1	1	2
	Motivation Documentation and Standardization	2	2	2	2	2
	Skill on Change Management	2	2	2	2	2
	Skill on Holistic View	2	2	2	2	2
Implementer Competency	Ability towards Understanding Clause	2	2	2	2	2
	Procedures of Asset Identification & Risk Assessment	2	X	1	1	2
	Past Experience	X	X	X	2	X
	Approach & Framework	2	2	2	2	2
	Audit infrastructure	2	1	2	1	2

V. Discussion and Conclusion

The awareness of information security is critical in government sector which then has led the Malaysian government to impose information security international standard in the respective agencies. To date, the available standard used by the Malaysian government is ISO 27001: Information Security Management System. The direction for ISMS implementation began in 2010 and since then every government agency which was earlier identified as Critical National Information Infrastructure (CNII) needed to implement ISMS. The government agency was experiencing some hardships and trial for ISMS certification due to lack of knowledge and skill. Many agencies certified with the help of third party and very few able to self-implement the ISMS.

This study has focused on finding success factors for ISMS self-implementation from qualitative standpoint. The proposed conceptual model was used to illustrate the study result. This study verified that the management commitment, implementer commitment and implementer competency are the success factors for ISMS self- implementation. The management commitment was seen to be a factor to ensure active participation and effective implementation. The strategic values of IT have impacted every phase of ISMS implementation and increased the implementer motivation. The significant implementer commitment could ensure a smooth implementation of ISMS with the help of specific team members. The ISMS implementer is required to be competent in understanding the standard requirement and executing the ISMS procedure effectively.

The results obtained from this study can be used to conceptualize a better model for information security management. The overall finding of this study is beneficial in providing guidance towards the self-implementation and maneuver of ISMS at the Plan Phase in government sector.

Acknowledgment

We would like to thank the Ministry of Education, Universiti Teknologi Malaysia & Vote No. (01K11) for supporting this research.

References

[1] Ismail, Z., Masrom, M., Sidek, Z., & Hamzah, D. (2010). Framework to Manage Information Security for Malaysian Academic Environment. *Journal of Information Assurance & Cybersecurity*, *2010*, 1–16.

[2] Shoraka, B. (2011). An Empirical Investigation of the Economic Value of Information Security Management System Standards.

[3] British Standards Institution. (1995). BS7799-1: Information Security Management Systems – Code of Practice for Information Security Management Systems.

[4] Dash, P. K. (2012). Effectiveness of ISO 27001, as an Information Security Management System: An Analytical Study of Financial, *9*(3), 42–55.

[5] MAMPU. (2010). Surat Arahan Pelaksanaan Pensijilan MS ISO / IEC 27001: 2007 Dalam Sektor Awam

[6] MAMPU. (2010). MS ISO/IEC 27001 Information Security Management System (ISMS).

[7] Ku, C.-Y., Chang, Y.-W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*, *33*(7), 371–384.

[8] Ramli, N. A., & Aziz, N. A. (2012). Risk Identification for an Information Security Management System Implementation, pp. 57–61.

[9] Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255.

[10] Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221–232. 11. (Pelnekar, 2008).

[11] Pelnekar, C. (2008). Feature Planning for and Implementing ISO 27001, (70).

[12] Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), pp. 195–201.

[13] Ramli, N. A., & Aziz, N. A. (2012). Risk Identification for an Information Security Management System Implementation, pp. 57–61.

[14] Chang, A.J.-T. & Yeh, Q.-J. (2006) On security preparations against possible IS threats across industries, Information Management & Computer Security, vol. 14, no. 4, pp. 343-60

[15] Abusaad, B., Saeed, F. A., Alghathbar, K., Khan, B., & Arabia, S. (2011). Implementation Of ISO 27001 In Saudi Arabia – Obstacles, Motivation, Outcomes and lessons Learned, 1–9.

[16] Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255

[17] Lane, T. (2007). Information Security Management in a Australian Universities – An Exploratory,

[18] ISACA. (2006). *Information Security Governance*.

[19] British Standards Institution. (1999). BS7799-2: Information Security Management Systems – Specification with guidance for use.

[20] Boyatzis, R. (1998). "Transforming qualitative information: Thematic analysis and code development", Thousand Oaks, CA, Sage.

[21] Al-awadi, M., & Renaud, K. (2007). Success Factor in information security implementation in organizations.

[22] Jalil, S. A., & Hamid, R. A. (2003). ISMS Pilot Program Experiences : Benefits, Challenges & Recommendations

[23] Bjorck, F. (2001). Implementing Information Security Management Systems–An Empirical Study of Critical Success Factors. *Lic Thesis. Stockholm University*.

[24] Watts, C. (2003). Implementing Gov Secure Information Security Management System (ISMS) Methodology – A Case Study of Critical Success Factors, (November), 1–9.

[25] Bellone, J., Basquiat, S. De, & Rodriguez, J. (2008). Reaching escape velocity: A practiced approach to information security management system implementation. *Information Management & Computer Security*, *16*(1), 49–57.

[26] Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. *European Journal of Information Systems*, *17*(3), 236–263.