Organizational Factors Affecting the ISMS Effectiveness in Sri Lankan IT Organizations: A Systematic Review

K.M.N. De Abrew and Dr. Ruwan Wickramarachchi
Department of Industrial Management
University of Kelaniya
Sri Lanka
deabrewk_im16100@stu.kln.ac.lk, ruwan@kln.ac.lk

Abstract

The world now considers information security to be a critical concern while most Sri Lankan public and commercial enterprises also have it as a legal requirement. Businesses must utilize an Information Security Management System (ISMS) as it improves resilience to cyber-attacks and decreases information-security expenses. Organizational factors are vital because no system or technology will be properly applied if the human aspect of the setting is neglected. As no prior study has been undertaken to focus on Sri Lankan organizations and the IT sector is an advancing sector, this research is aimed at identifying the organizational factors that influence the efficacy of ISMS in Sri Lankan IT organizations. A qualitative approach with a systematic literature review was done following the PRISMA method. Identified Success Factors were analyzed, and a conceptual model is developed from the top 7 constructs (Implementer IT competency, Information Security Training, Employee acceptance and readiness, Information Security Policy, Employee Security Awareness, Top Management Commitment, Information security standard compliance). Understanding the impact of organizational factors will aid businesses in developing more effective information security strategic planning and deployment suited for all employees. The suggested constructs will offer a base for future research on this study area.

Keywords
ISMS, Sri Lanka, Organizational factors, IT sector, Information Security Management

1 Introduction

As data plays the crucial factor in the present firm context, Information can be mentioned as the blood of an organization especially as access to high-quality, complete, accurate, and up-to-date information is vital in supporting the managerial decision-making process that leads to sound decisions (Burns 2018) (Susanto et al. 2011). Information security, shortened to infosec, is the practice of protecting information by mitigating information risks. ICT, being a fast-developing sector in Sri Lanka, offers a wide range of applications. Currently, Sri Lanka's fourth-largest export earner is the ICT industry. It is stated in Jothirathne and Pushpakumara (2017) that ICT investment should comprise funds for the development of ICT infrastructure, the training of human resources in ICT skills, and the creation of a favorable policy framework. Moreover, it describes that out of many opportunities available for the ICT industry of Sri Lanka an important benefit is its high level of information security stating that Sri Lanka, has one of the most stringent intellectual property protection regimes in the region. So, with these factors, it is evident that the IT industry has a growing future and with technological advancements the need for information security management is high. But still, there is a gap in this research area as not many studies have been done in the Information Security Management related to Sri Lankan organization context. It is clearly stated in Ibrahim and Ali (2018) that understanding the significance of organizational factors will aid businesses in developing a more successful information security strategic plan and creating the deployment of information security awareness customized to all employees, from top management to subordinates. Since ISMS is a management system that is used to safeguard an organization's information environment according to that enhancing the ISMS quality has a beneficial impact on administrative performance. Indeed, the fact that the ISMS is dependable and completes its operations on time is beneficial to the company's main business, and it should thus be carried out on time. Similarly, the more adaptable the ISMS, the more adaptable the global management system (Al-Rashdi et al. 2017) (Tewamba et al. 2019). Hence it is evident that a properly established and operated ISMS will be vital in ensuring information security in a firm. So, this research will be interesting and useful because there is no previous research focused on the effectiveness of Information Security

Management Systems in IT organizations in Sri Lanka. According to Ibrahim and Ali (2018), out of all the critical success factors which have an impact on ISMS implementation, organizational factors have the most significant effect. Organizational factors can be regarded as the characteristics of an organization that might have a significant impact on their decision such as top management support, organizational size, and technology readiness (Alkhater et al. 2014). Therefore, according to the fact that any system will not be a success if it forgets the human aspects, conducting research focusing on how organizational factors affect the Information Security Management Systems efficiency is important. Although there are studies done on how the ISMS implementation is affected by internal and external factors there is less focus on out of all success factors how the organizational factors matter for ISMS success. Moreover, there is a gap in research done since no previous study has been undertaken in terms of organizations operating in Sri Lanka. Additionally, the IT sector plays a key role when it comes to information security aspects.

1.1 Objectives

This research has several aims. Firstly, to conduct a systematic literature review on organizational factors that affect Information Security Management Systems. Secondly to identify the organizational factors on the effectiveness of ISMS in IT sector organizations in Sri Lanka.

2 Literature Review

This chapter elaborates the concepts of Information security standards, Information Security Management systems, organization factors, IT sector in Sri Lanka and is concerned with carefully reviewing and presenting current research on important success factors affecting Information security systems.

2.1 Information Security Standards

With the complexity of IT systems, to gain their stakeholders' trust, companies must achieve an acceptable security level. Information security standards can be mentioned as a set of rules, policies, or guidelines to be followed to achieve the security aspects of a product or a system. According to Arora (2010), the frameworks of standards on information systems management may conveniently be broken down into Information Security standards and IS Governance standards. Information Security standards such as ISO 27000 series (earlier known as ISO/IEC 17799), NIST 800 series, SOX, ISF SOGP, Risk IT, etc. solely focus on security by providing businesses with a risk-based approach to secure the information in a business context. There it has indicated COBIT, COSO, ITIL, etc. as examples for IT governance/service quality standards. Furthermore, this paper has stated that these two sets of standards are not mutually incompatible and some prominent IT governance and management frameworks, such as COBIT, have attempted to include features of security but have not gone into detail. It also has suggested that no one standards framework is a comprehensive choice. Hence it is better to examine if the collection of standards a firm selects is sufficiently focused on information security, or whether there is a need to go beyond and extend this framework to a hybrid of more standards (Arora, 2010). Out of many security standards and IT governance/quality standards, some are providing a focus on ISMS implementation. Each standard has its role and position in implementing ISMS, with ISO and BS7799 focusing on ISMS as their main domain and focus, while PCI-DSS focuses on information security relating to business transactions and smart cards, and ITIL and COBIT focusing on information security and its relationship with project management and IT governance. Susanto et al. (2011) have introduced five standards as a concept 'big five ISMS Standards': ISO27001, BS7799, PCI-DSS, ITIL, and COBIT as widely used security standards-based for ISMS in organizations.

2.2 Information Security Management Systems (ISMS)

A properly equipped and managed ISMS will assist in gaining new clients and entering new markets, improving the relationship with the firm's current consumers while developing the company's brand and reputation. The information security management system (ISMS) is a component of the entire management system that is based on a risk-based business approach and is responsible for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security (Tewamba et al. 2019). ISMS can be defined as is a set of processes for systematically establishing, documenting, and continuously managing procedures to improve the safety and reliability of an enterprise's assets, as well as for achieving information confidentiality, integrity, and availability, which are the goals of information security. Being a set of policies dealing with Information Technology (IT) related risks or Information Security Management (ISM), it also ensures the continuous enhancement of information security (Amarachi et al. 2013) (Park et al. 2013). As discussed in Park, et al. (2013), implementing and maintaining a well-managed ISMS may provide significant benefits to a firm like the potential loss from a prospective threat to the present

operation of the information system may be statistically anticipated and tracked where the administrative can understand risk level and reduce the risk possibility, The assets of the organization may be enhanced in terms of stability, effectiveness, efficiency, and dependability. The visual depiction of risk levels derived from risk analysis and evaluation can raise administrators' and users' security awareness. ISMS aids decision-making in establishing security measures that consider the priority and cost/effectiveness elements of high-risk locations. Government certification indicates that the company is appropriately managing information security, increasing public trust, and competitiveness. To boost its corporate image, the company might tell its users or trade partners that they follow the legislation, policy, or standards. It has the potential to significantly contribute to the business aim. According to the research paper Ibrahim and Ali (2018, p. 545), ISMS is defined as "managing an organization's sensitive information through systematic policies and procedures to minimize risk and to ensure business continuity.". So, for this research also the above definition will be followed.

2.3 Organizational Factors

There is much past research done relevant to organizational factors affecting the system improvements/ concepts etc. but it is less focus is given to providing a clear definition of what are organizational factors? In general, companies focus their efforts on external threats while turning a blind eye to the reality that severe vulnerabilities may exist within the company and its processes, such as employee unawareness of the policies and the consequences of violations, poor information security legislation, and policies (Alsaif et al. 2015) (Al-Harethi and Al-Amoodi 2019). According to Zidane et al. (2016), Internal organizational influences may be seen in a variety of ways, including shared values, norms, and beliefs, as well as structure, competency, rules, and procedures. ISMS should consider non-technical elements, besides technical elements, to be inclusive, cooperative, and communicative whilst inviting exploration and promoting security satisfaction. Consideration of Human factors enables this but human factors at the same time are the most vulnerable part of the system (Alavi et al. 2014). Organizational factors are features of an organization that can have a major influence on their decision such as top management support, organizational size, and technology readiness (Alkhater et al. 2014). Therefore, within this research, the 'organizational factors' will be defined as behavioral attributes, conditions, and processes of internal parties/environment of an organization.

2.4 Information Technology Sector in Sri Lanka

In a state where ICT services are the country's fourth-largest export earner, with approximately 300 firms, the Sri Lankan ICT sector currently services a variety of Industry verticals. Sri Lanka Export Development Board (EDB) states that with a workforce of approximately 85,000, this sector's export income increased from US$ 166 million in 2006 to US$ 968 million in 2017. With over 90% value addition and high-paying jobs, has had a significant impact on the growth of the Sri Lankan economy. Moreover, EDB states that Sri Lanka is one of the emerging countries in the IT industry has a highly trained workforce and a cost-competitive business setting, focusing primarily on business process outsourcing (BPO) and knowledge services outsourcing (KPO). According to EDB, the IT sector is enthusiastic about adhering to global labor and environmental norms. Obtaining benefits such as being the first country in the region to install a 3G/4G network and being regarded as the region's most cost-effective real estate, comparatively Lower Operating Cost, talent pool, and high retention rate, etc. Sri Lankan ICT industry has been heading for a technology-enhanced future emerging ICT exports trends namely IoT /Embedded Products and services, Emotion-based analytics, Robotics (Automation), Open source, Cloud, Artificial Intelligence (AI), Advanced Simulation and behavioral control, Augmented reality and Virtual Reality and Big Data.

2.5 Factors affecting when implementing Information Security Management Systems (ISMS)

In Ibrahim and Ali (2018) it is mentioned that Information security necessitates the accountability of all employees, including top management, all management levels, and regular employees. When focusing on implementing an ISMS within an organizational context, the major elements to be highlighted for ISMS effectiveness are a lack of understanding of the success criteria and a lack of awareness about information security. Oversight of critical elements may impede the organization's attempts to fully comprehend the benefits of ISMS. As a result, it is necessary to determine the factors influencing the effectiveness of ISMS deployment (Ibrahim and Ali 2018) (Tu and Yuan 2014). When considering the factors affecting ISMS, there is a set of research focused on Critical Success Factors while some other research focuses on Key Success Factors (KSF) and some focuses on general term factors. CSF or KSF refers to the element which is essential for an organization/system/process to achieve its ultimate mission and goals. It is noted that the critical success factors can be further classified and from that, we can outstand what are the organizational factors out of CSFs. Through the literature review, it is identified since all these factor types have a magnificent impact on ISMS effectiveness all these factors should be considered to identify the organizational factors.

On the other hand, Information Security Management (ISM) is a component of the entire organization management system that serves as the basis for managing security risks, to establish, implement, operate, monitoring, reviewing, maintaining, and improving information security in the company (Ključnikov et al. 2019) (Rajnoha et al. 2017). Therefore, for this research, the literature based on ISM implementation success factors also has been considered as a domain. For the implementation and operation of any technology/system or a process, internal and external factors can be common. Still, there may be specific factors that are especially affecting a particular system or a technology, but for this research, it is considered that looking into all the possible similar systems and technologies will be more effective to identify a wide range of common factors. Another research that has focused on cloud computing adaption Alkhater et al. (2014) has developed an integrated model consisting of three fundamental factors: technological, organizational, and environmental factors. Looking at this set of factors and comparing these with research done on ISMS systems effectiveness it is clear that those factors are commonly mentioned and hence these can be considered for this research as well. The research Chander et al. (2012) has focused on various factors affecting IS environment in an organization and the ISM-based model has been proposed to demonstrate the factors and their interrelationships. According to the literature, regardless of security measures, all types of human factors can have a significant impact on security management in an organizational setting, ISMS implementation is highly impacted by organizational factors, and this must be investigated more. Table: 1 shows the summary of identified organizational factors from selected literature and the frequency of each actor mentioned is also presented.

3 Methods

A systematic literature review (SLR) was done to select the past research that contributes to identifying factors affecting when implementing Information Security Management Systems. Preferred Reporting Items for Systematic Reviews and Meta-Analyses, (PRISMA) was used for the systematic literature review done for this study. PRISMA is a widely accepted methodology which already being used in research done in different fields such as technology, medicine, tourism, etc. (Liberati et al. 2009) (Sharif et al. 2019) (Kalhoro et al. 2021). The PRISMA checklist was referred to for providing an analyzed review.

Search strategy - Electronic databases were used and a keyword-based search was done. Inclusion and exclusion criteria were defined for retrieving the most related publications.

- Search string keywords - Pre-defined keywords were used with Boolean operators “AND” and “OR” to identify research papers from a broader perspective. The keywords used were “factors”, “Information Security Management”, “Information Security Management system”, “Sri Lanka”, “Information security”, “critical success factors”, “key factors”, “ISMS”. Some of these terms were selected considering the probability of being interchangeable with research keywords. Using a keyword-based search will prevent us from being biased on well-known authors or well-cited papers (Abraham et al. 2019).

- Data sources - To identify relevant material for this systematic review, some of the popular scientific databases were considered. The advanced search was done in selected electronic databases. ResearchGate, ScienceDirect, Emerald Insight, SpringerLink, and IEEE Xplore are used as databases while google scholar is also used as a search engine. A complete list of the number of papers retrieved from databases will be further presented in Figure: 1. For a literature search, electronic databases were used with predefined inclusion and exclusion criteria. ResearchGate, ScienceDirect, Emerald Insight, SpringerLink, and IEEE Xplore are used as databases while google scholar is also used as a search engine. To improve research quality the retrieved articles were further reviewed.

- Study Selection - Research screening was followed according to the PRISMA method as mentioned in Figure:1 while the research papers were selected according to a few specified rules. The selected papers from databases were checked and duplications were removed. Also, since this research was carried in the English language all the papers written in some other were eliminated. Before the comprehensive evaluation of the text, an abstract and topic-based screening was performed. Following that, out of the selected papers, some could not be obtained due to access restrictions. Then research was evaluated based on the inclusion and exclusion criteria. Following a full-text review, a total of 42 suitable publications were identified. The PRISMA flowchart shows the number of studies investigated at each step of the study.

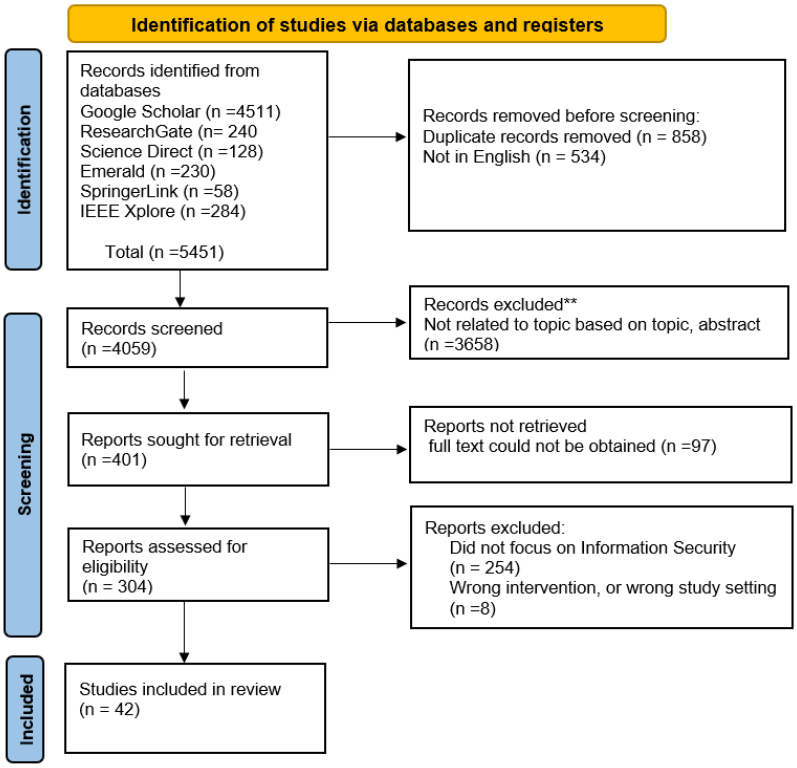

Figure 1. Flow chart of the study selection process

Inclusion Criteria:
IC1- Studies must be published between 2011 and 2021.
IC2- Studies must be published in a journal or a conference proceeding.

Exclusion Criteria:
EC1- Newspaper articles, online blogs, book chapters, short paper summaries, and abstracts.
EC2- Irrelevant and out-of-scope studies.

The records were excluded by manually using Microsoft Excel. There are research papers that specially focused on Information Security Practices or ISMS and there are papers that broadly focused on technology implementations. As discussed previously, in this research the focus is to analyze papers broadly and identify all related organizational factors that can affect the effectiveness of ISMS. Hence, below mentioned Table: 1 will provide a better overview of selected research studies and the factors identified in them.

4 Data Collection

The major literature consists of forty-two (42) papers selected through the qualitative method mentioned above. All the papers are published in recent years(2011-2021).

Table 1. Summary of the organizational factors

Factor group	Cited papers	No
User characteristics	(Dunkerley and Tejay 2011), (Nguyen et al. 2015), (Waly et al. 2012), (Din et al. 2021), (Ferreira et al. 2018)	5
Information technology competency	(Ibrahim and Ali 2018), (Tu and Yuan 2014), (Tatiara et al. 2018), (Alavi et al. 2015), (Weerasinghe and Wijayanayake 2017), (Dunkerley and Tejay 2011), (Elattresh et al. 2019),	13

	(Khana et al. 2021), (Parsons et al. 2015), (Arbanas and Hrustek 2019), (Chander et al. 2012), (Ismail et al. 2014), (Hasbini et al. 2018)	
Employee acceptance and readiness	(AlKalbani et al. 2014), (Assefa and Tensaye 2021), (AlGhamdi et al. 2020), (Zammani et al. 2019), (Ismail et al. 2014), (Zammani and Razali 2016), (Alavi et al. 2015), (Alavi et al. 2014), (Sarmoen et al. 2019), (Nesren et al. 2012), (Parsons et al. 2015), (Waly 2013), (Weerasinghe and Wijayanayake 2017), (Glaspie and Karwowski 2017), (Ferreira et al. 2018), (Sadeghi 2016), (Kazemi et al. 2012), (Tatiara et al. 2018), (Kiilu and Nzuki 2016)	19
Top management commitment	(Norman and Yasin 2012), (Arbanas and Hrustek 2019), (Zammani et al. 2019), (Ključnikov et al. 2019), (Maarop et al. 2015), (Chander et al. 2012), (Alkhater et al. 2014), (Singh et al. 2014), (Tu and Yuan 2014), (Obeidat and Mughaid 2019), (Kazemi et al. 2012), (Hashim and Razali 2019), (Tu et al. 2018), (Alavi et al. 2015), (Zammani and Razali 2016), (Khana et al. 2021), (Din et al. 2021), (Sari et al. 2016), (Glaspie and Karwowski 2017), (Singh et al. 2013), (Sadeghi 2016), (Alavi et al. 2014), (Sarmoen et al. 2019), (Tatiara et al. 2018), (Ibrahim and Ali 2018), (AlKalbani et al. 2014), (Kiilu and Nzuki 2016), (Assefa and Tensaye 2021)	24
Information security policy	(Arbanas and Hrustek 2019), (Ibrahim and Ali 2018), (Zammani et al. 2019), (Ključnikov et al. 2019), (Al-Harethi and Al-Amoodi 2019), (Sarmoen et al. 2019), (Chander et al. 2012), (Singh et al. 2014), (Tu and Yuan 2014), (Kazemi et al. 2012), (Elattresh et al. 2019), (Ismail et al. 2014), (Hashim and Razali 2019), (Tu et al. 2018), (Zammani and Razali 2016), (Tatiara et al. 2018), (Khana et al. 2021), Din et al. 2021), (Sari et al. 2016), (Yildirima et al. 2011), (Glaspie and Karwowski 2017), (Singh et al. 2013), (Sadeghi 2016), (AlGhamdi et al. 2020)	24
Information security training	(Arbanas and Hrustek 2019), (Chander et al. 2012), (Singh et al. 2014), (Tu and Yuan 2014), (AlKalbani et al. 2014), (Obeidat and Mughaid 2019), (Kazemi et al. 2012), (Waly et al. 2012), (Hashim and Razali 2019), (Tatiara et al. 2018), (Khana et al. 2021), (Assefa and Tensaye 2021), (Glaspie and Karwowski 2017), (Singh et al. 2013), (Sadeghi 2016), (AlGhamdi et al. 2020), (Alavi et al. 2014), (Kiilu and Nzuki 2016)	19
Legal/social pressure	(AlKalbani et al. 2014)	1
Funding	(Khana et al. 2021), (Alavi et al. 2015), (Sari et al. 2016)	3
Safety skills	(Elattresh et al. 2019)	1
Access control	(Al-Harethi and Al-Amoodi 2019), (Ismail et al. 2014), (Yildirima et al. 2011), (Elattresh et al. 2019)	4
User satisfaction	(Nguyen et al. 2015), (Waly 2013)	2
Incident management	(Singh et al. 2014), (Nesren et al. 2012), (Ismail et al. 2014), (Waly 2013), (Tatiara et al. 2018), (Singh et al. 2013)	6
Process integration	(AlKalbani et al. 2014), (Tatiara et al. 2018), (Din et al. 2021)	3
Security awareness	(Arbanas and Hrustek 2019), (Ibrahim and Ali 2018), (Ključnikov et al. 2019), (Sarmoen et al. 2019), (Chander et al. 2012), (Tu and Yuan 2014), (AlKalbani et al. 2014), (Kazemi et al. 2012), (Ismail et al. 2014), (Waly 2013), (Tu et al. 2018), (Alavi et al. 2015), (Zammani and Razali 2016), (Tatiara et al. 2018), (Khana et al. 2021), (Assefa and Tensaye 2021), (Glaspie and Karwowski 2017), (Singh et al. 2013), (Sadeghi 2016), (Dunkerley and Tejay 2011), (Obeidat and Mughaid 2019), (Nesren et al. 2012), (Sari et al. 2016), (Ferreira et al. 2018), (Maarop et al. 2015), (Alavi et al. 2014)	26
Information security standard compliance	(Ibrahim and Ali 2018), (Ključnikov et al. 2019), (Chander et al. 2012), (Singh et al. 2014), (Tu and Yuan 2014), (Kazemi et al. 2012), (Ismail et al. 2014), (Hashim and Razali 2019), (Singh et al. 2013), (AlGhamdi et al. 2020), (Sadeghi 2016), (Hasbini et al. 2018), (Diescha et al. 2020)	11
Resource planning	(Zammani et al. 2019), (Chander et al. 2012), (Tu and Yuan 2014), (Hashim and Razali 2019), (Zammani and Razali 2016), (AlGhamdi et al. 2020), (Diescha et al. 2020)	6
Risk management	(Zammani et al. 2019), (Tu and Yuan 2014), (Elattresh et al. 2019), (Waly et al. 2012), (Hashim and Razali 2019), (Zammani and Razali 2016), (Tatiara et al. 2018), (Din et al. 2021), (AlGhamdi et al. 2020), (Diescha et al. 2020)	10
Business continuity management	(Zammani et al. 2019) ,(Al-Harethi and Al-Amoodi 2019), (Ismail et al. 2014), (Hashim and Razali 2019), (Zammani and Razali 2016), (Yildirima et al. 2011), (Diescha et al. 2020)	6

IS audit	(Zammani et al. 2019, (Chander et al. 2012), (Singh et al. 2014), (AlKalbani et al. 2014), (Zammani and Razali 2016), (Tatiara et al. 2018), (Assefa and Tensaye 2021), (Singh et al. 2013), (AlGhamdi et al. 2020)	9
Asset Classification and control	(Al-Harethi and Al-Amoodi 2019), (Chander et al. 2012), (Singh et al. 2014), (Ismail et al. 2014), (Yildirima et al. 2011), (Singh et al. 2013)	6
Physical and Environmental Security	(Al-Harethi and Al-Amoodi 2019), (Chander et al. 2012), (Yildirima et al. 2011)	3
System Development and Maintenance	(Al-Harethi and Al-Amoodi 2019), (Ismail et al. 2014), (Yildirima et al. 2011)	3
Communication	(Waly et al. 2012), (Alavi et al. 2015), (Kiilu and Nzuki 2016), (AlGhamdi et al. 2020), (Al-Harethi and Al-Amoodi 2019), (Hashim and Razali 2019), (Alavi et al. 2014), (Hasbini et al. 2018), (Elattresh et al. 2019), (Tatiara et al. 2018)	10
IS culture	(Tu and Yuan 2014), (Singh et al. 2014), (Waly et al. 2012), (Singh et al. 2013), (Nesren et al. 2012), (Chander et al. 2012), (Parsons et al. 2015), (Alavi et al. 2015), (Sadeghi 2016), (AlGhamdi et al. 2020)	10
Technology acceptance and readiness	(Obeidat and Mughaid 2019), (Hashim and Razali 2019), (Khana et al. 2021), (AlKalbani et al. 2014), (Weerasinghe and Wijayanayake 2017), (Alkhater et al. 2014), (Din et al. 2021), (Zammani et al. 2019)	8
Organization structure	(Zammani et al. 2019), (Hashim and Razali 2019), (Zammani and Razali 2016), (Kiilu and Nzuki 2016), (AlGhamdi et al. 2020), (Tu and Yuan 2014), (Norman and Yasin 2012)	7
Organization culture	(Sari et al. 2016), (Sadeghi 2016), (Alkhater et al. 2014), (Tu and Yuan 2014), (AlGhamdi et al. 2020), (Chander et al. 2012), (Nesren et al. 2012), (Waly 2013), (Obeidat and Mughaid 2019), (Tu et al. 2018)	8

Based on Table:1 result, the frequency was calculated to categorize highly mentioned constructs, and which were mentioned more than in 10 papers were selected as variables for the conceptual model as shown in Table: 2.

Table 2. Construct of organizational factors

Construct	**Cited number out of 42**
Implementer IT Competency	13
Employee Acceptance and Readiness	19
Top Management commitment	24
Information Security Policy	24
Information Security Training	19
Employee Security Awareness	26
Information Security Standard Compliance	11

4.1 Conceptual Model

Based on the literature studies, the conceptual model with seven (7) constructs shown in Figure: 2 was developed. This model was created, and hypotheses were developed to examine the major influence of organizational factors on the effectiveness of the ISMS.

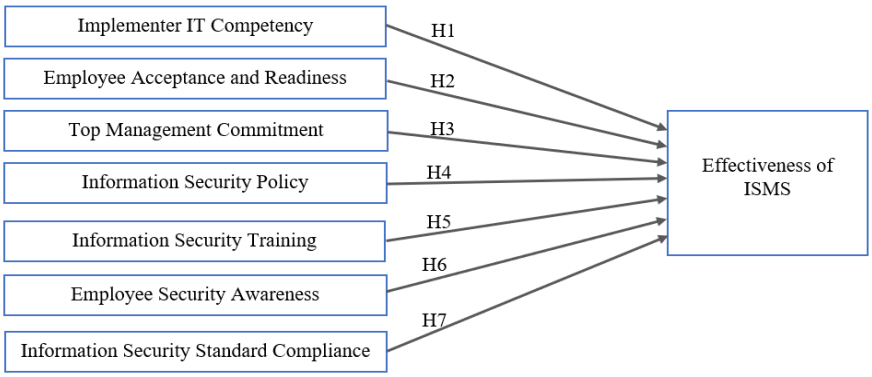

Figure 2. Conceptual model

Implementer IT competency - Success of any system or technology relies on how well the implementer has knowledge, skills, and experience to implement and continue the process. Competency is a crucial factor when it comes to dealing with all aspects of ISMS since it is a whole process with phases like planning, executing, monitoring, and improving and properly managed ISMS effect on the organization's stakeholder (Ibrahim and Ali 2018), (Tu and Yuan 2014), (Tatiara et al. 2018), (Alavi et al. 2015). Also, it's important not to overestimate or underestimate people's skills and provide opportunities to update the skills and knowledge while encouraging them to experience the processes of learning from past mistakes (Weerasinghe and Wijayanayake 2017).
H1: Implementer IT Competency has a relationship with the effectiveness of the ISMS.

Employee acceptance and readiness - ISMS is consisting of people, processes, and technologies so the people who are ultimately the end-users are a major factor when it comes to ISMS effectiveness. No matter how well the information Security team implements the ISmS if the employees of the firm are not ready to use it, follow the processes the ISMS will fail. So, if the employees are accountable, have motivation towards adapting, have trust in the ISMS it will create a positive effect on ISMS effectiveness (AlKalbani et al. 2014), (Assefa and Tensaye 2021), (AlGhamdi et al. 2020), (Zammani et al. 2019), (Ismail et al. 2014), (Alavi et al. 2015), (Alavi et al. 2014).
H2: Employee acceptance and readiness have a relationship with the effectiveness of the ISMS.

Top management commitment- Previous studies have given attention to management support as a special factor because it is evident that without the management involvement not only ISMS, but even a firm's Information security strategy won't take in right place. In this study we have considered the management commitment is the combination of Management support (Norman and yasin 2012), (Arbanas and Hrustek 2019), (Zammani et al. 2019), (Ključnikov et al. 2019), (Maarop et al. 2015), (Chander et al. 2012), (Alkhater et al. 2014), (Singh, et al. 2014), (Tu and Yuan 2014), (Obeidat and Mughaid 2019), (Kazemi et al. 2012), (Hashim and Razali 2019), (Tu et al. 2018), (Alavi et al. 2015), (Zammani and Razali 2016), (Khana et al. 2021), (Din et al. 2021), (Sari et al. 2016), (Glaspie and Karwowski 2017), (Singh et al. 2013), (Sadeghi 2016), management commitment (Alavi, et al., 2014), (Zammani et al. 2019), (AlKalbani et al. 2014), (Tatiara et al. 2018), (Kiilu and Nzuki 2016), (Assefa and Tensaye 2021), (Ibrahim and Ali 2018), management leadership (Din et al. 2021), (Alavi et al. 2014),(Sarmoen et al. 2019),(Hashim and Razali 2019), (Tatiara et al. 2018),(Hasbini et al. 2018), management skills (Alavi et al. 2014), management reviews (Tatiara et al. 2018) and management awareness (Alavi et al. 2014).
H3: Top management commitment has a relationship with the effectiveness of the ISMS.

Information security policy - Security policies are defined as a collection of directives, regulations, rules, and practices that specify how an organization maintains, secures, and distributes information. A good information security policy should be simple and concise, easy to comprehend, and free of legal and technical jargon. Furthermore, it must be practical, effective, widely communicated to employees, and enforced, as information security rules and procedures frequently change as the work develops continuously (Ibrahim and Ali 2018), (Diesch et al. 2020), (Din et al. 2021).
H4: Information security policy has a relationship with the effectiveness of the ISMS.
Information security training -Training provides advanced knowledge, skills to people while giving practical experiences sometimes. Many research studies have stated that since stakeholders of an ISMS like employees, IS team, management, etc. may have lack competence, providing comprehensive training periodically will aid businesses to develop their confidence and competence on Information security (Arbanas and Hrustek 2019), (Chander et al.

2012), (Singh et al. 2014), (Tu and Yuan 2014), (AlKalbani et al. 2014), (Obeidat and Mughaid 2019), (Kazemi et al. 2012), (Waly et al. 2012), (Hashim and Razali 2019), (Tatiara et al. 2018), (Khana et al. 2021), (Assefa and Tensaye 2021), (Glaspie and Karwowski 2017), (Singh et al. 2013). Also as stated in AlKalbani et al. (2014) it's important for those training to be understandable, useful to the participant, and conducted at a satisfactory level.
H5: Information security training has a relationship with the effectiveness of the ISMS.

Employee security awareness - While the IT competency of the implementers is essential for the ISMS effectiveness, the same or more responsibility comes for the users. No matter what system/guidelines are established the employee behavior, user activities, user engagement, user reaction, user mistakes, and defects are affecting the success of it. So all the above elements are examples of awareness. Moreover, all aspects of knowledge, such as skills, education, training, and competency, of employees are included in the awareness component. Literature on awareness addresses not only people's conduct but also their personal requirements, privacy concerns, trust difficulties, cultural beliefs, and the social context (Diesch et al. 2020), (Kazemi et al. 2012), (Ismail et al. 2014), (Waly 2013), (Tu et al. 2018), (Alavi et al. 2015), (Zammani and Razali 2016). Whatever the policies, procedures introduced with ISMS if the general staff/ employees have a clear understanding of them, what is their role in the information security aspect, if they know how to act in any situation matters a lot. Moreover, from the firm side, proper awareness materials should be provided and they should be properly communicated to the employees.
H6: Employee security awareness has a relationship with the effectiveness of the ISMS.

Information security standard compliance - Compliance with approved and accepted standards of information security will be an advantage for firms it increases user confidence, stakeholder confidence, and client trust while meeting any regulatory requirements applicable to public-sector companies (Ibrahim and Ali 2018), (Ključnikov et al. 2019), (Chander et al. 2012), (Singh et al. 2014). Also, periodic audits also essential to maintain security standard compliance o a firm (Hashim and Razali 2019). While many firms employ related information security governance standards such as BS 7799, ISO 27001, PCI-DSS, ITIL, and COBIT, the most extensively utilized standard in the ISMS domain is ISO 27001. But sometimes if any organization plans to achieve additional standards while currently having an ISMS based on one standard, they can do a gap analysis and add additional features required. Especially security standard compliance ISMS will be a requirement when the firms have international clients from different counties.
H7: Information security standard compliance has a relationship with the effectiveness of the ISMS.

5 Results and Discussion

Using the critical success factors method, this study investigated the variables that led to the success of ISMS and found organizational factors linked to the efficacy of information security. By analyzing the literature in the field of information security, seven (7) organizational factors are identified, and a link between these elements and the efficacy of the ISMS is presented with seven hypotheses. These seven elements were chosen because they reflect most of the organizational factors identified in prior studies. As a result, a conceptual model has been created and will be evaluated in IT sector firms in Sri Lanka to explore the substantial influence of organizational factors on ISMS efficacy. This research has only followed the qualitative approach to build a conceptual model to identify Organizational factors affecting the effectiveness of Information Security Management Systems in IT sector organizations operating in Sri Lanka. But further studies should be carried on with a quantitative approach with some survey results which may be able to support or evaluate the validity of the results of this research.

6 Conclusions

The function of organizational factors must be investigated in order to guarantee that workers follow the information security policy, standards, procedures, rules, and regulations to decrease security breaches and improve corporate performance. Previous research has clearly indicated that organizational factors may impact the efficacy of the ISMS. Sri Lanka's IT industry is rapidly growing and at the same time related as a core to many other parallel industries. So, aligning to security standards and ensuring the security of organizations' data will be a competitive advantage for IT organizations. Hence the organizational factors identified through this research will be useful to be considered for the effectiveness of ISMS and develop a framework to support managing Information Security Management Systems of IT sector organizations in Sri Lanka. This research's aims have been achieved by completing a systematic literature review and identifying the organizational factors on the effectiveness of ISMS in IT sector organizations in Sri Lanka. The findings of this research will help the IT sector organizations recommendations to improve the effectiveness of the Information Security Management Systems and adding to that, this study results can be useful for some other countries as well creating a more academic value for this study. Understanding the major impact of organizational

factors will aid businesses in developing more effective information security strategic planning and creating information security awareness deployment suited for all employees, from the top down to the bottom up.

References

Abraham, R., Schneider, J. and Brocke, J. v., 2019. Data governance: A conceptual framework, structured review, and research agenda, *International Journal of Information Management*, Volume 49, pp. 424-438.

Alavi, R., Islam, S. and Mouratidis, H., A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations*, International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2014.

Alavi, R., Islam, S., Jahankhani H., and Al-Nemrat A., Analyzing Human Factors for an Effective Information Security Management System, *An International Journal of Secure Software Engineering*, 2015.

AlGhamdi, S., Win, K. T. and Vlahu-Gjorgievska, E., Information security governance challenges and critical success factors: Systematic review, *Computers, and Security*, vol. 99, 2020.

AlKalbani, A., Deng, H. and Kam, B., A Conceptual Framework for Information Security in Public Organizations for E-Government Development*.*, *25th Australasian Conference on Information Systems*. Auckland, New Zealand, 2014.

Alkhater, N., Wills, G. and Walters, R., Factors Influencing an Organisation's Intention to Adopt Cloud Computing in Saudi Arabia., *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, 2014.

Alsaif, M., Aljaafari, N. and Khan, A. R., Information Security Management in Saudi Arabian Organizations., *Procedia Computer Science*, vol. 56, 2015.

Alsaif, M., Aljaafari, N. and Khan, A. R., Information Security Management in Saudi Arabian Organizations., Procedia *Computer Science*, vol. 56, 2015.

Al-Harethi, A. A. M. and Al-Amoodi, A. H. A., Organizational Factors Affecting Information Security Management Practices in Private Sector Organizations., *International Journal of Psychology and Cognitive Science,* Volume 5(1), 2019.

Al-Rashdi, Z., Dick, M. and Storey, I., Literature-based analysis of the influences of the new forces on ISMS: A conceptual framework, *Australian Information Security Management Conference*, 2017.

Amarachi, A., Okolie, S. and Ajaegbu, C., Information Security Management System: Emerging Issues and Prospect. *IOSR Journal of Computer Engineering (IOSR-JCE),* vol.12, no. 3, 2013.

Arbanas, K. and Hrustek, N. Ž., Key Success Factors of Information Systems Security, *Journal of Information and Organizational Sciences,* vol. 43, no. 2, 2019.

Arora, V., Comparing Different Information Security: COBIT vs. ISO 27001. *Carnegie Mellon University, Qatar,* 2010.

Assefa, T. and Tensaye, A., Factors influencing information security compliance: an institutional perspective, *SINET: Ethiopian Journal of Science*, 2021.

Burns, A. J., Security Organizing: A Framework for Organizational Information Security Mindfulness, *The Data Base for Advances in Information Systems, 2018.*

Chander, M., Jain, S. K. and Shankar, R., Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. *Journal of Modelling in Management,* vol.8, no. 2. 2012.

Diescha, R., Pfaff, M., and Krcmar, H., A comprehensive model of information security factors for decision-makers, *Computers and Security*, 2020.

Din, Z., Jambari, D. I., Yusof, M. M. and Yahaya, J., critical success factors for managing information systems security in SMART city enabled by Internet of Things, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol.11, no.12, 2021.

Dunkerley, K. D., and Tejay, G., A Confirmatory Analysis of Information Systems Security Success Factors, *2011 44th Hawaii International Conference on System Sciences, 2011.*

Elattresh, J., Ramadan, K. and Tokeser, U., Factors Effecting Information Security Management, and their impacts on Organization performance in the work environment: Case study; Hatif Libya Company (HLC), *Australian Journal of Basic and Applied Sciences*, 2019.

Ferreira, R. d. S., Frogeri, R. F., Coelho, A. B. and Piurcosky, F. P., Information Security Management Practices: Study of The Influencing Factors in a Brazilian Air Force Institution, *Journal of Information Systems and Technology Management – Jistem USP*, vol. 15, 2018.

Glaspie, H. W., and Karwowski, W., Human Factors in Information Security Culture: A Literature Review, *International Conference on Applied Human Factors and Ergonomics*, 2017.

Hasbini, M. A., Eldabi, T., Aldallal, A., Investigating the information security management role in smart city

organizations, *World Journal of Entrepreneurship, Management and Sustainable Development*, vol. 14, no. 1, 2018.

Hashim, R., and Razali, R., Contributing Factors for Successful Information Security Management Implementation: A Conceptual Model*, International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 9, no. 2, 2021.

Ibrahim, N. and Ali, N., The Role of Organizational Factors to the Effectiveness of ISMS, *International Journal of Engineering and Technology, vol. 7, 2018.*

Ismail, W., Norwawi, N., and Saadan, K., The Challenges in Adopting Information Security Management System for University Hospitals in Malaysia, *Knowledge Management International Conference (KMICe)Malaysia*, 2014.

Jothirathne, P. and Pushpakumara, C., Review the Sri Lankan Information and Communication Technology Industry, *International Journal of Management, Accounting and Economics,* vol. 4, no. 2, 2017.

Kazemi, M., Khajouei, H. and Nasrabadi, . H., Evaluation of information security management system, *African Journal of Business Management,* vol. 6, *2012.*

Kalhoro, S., Rehman, M., Ponnusamy, V. A. and Shaikh, F. B., Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. s.l., *IEEE Access*, vol. 9, 2021.

Khan, A., A., Ibrahim, M. and Hussain, A., An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries, *International Journal of Information Management Data Insights*, vol 1, no. 2, 2021.

Kiilu, P. K. and Nzuki, D. M., Factors Affecting Adoption of Information Security Management Systems: A Theoretical Review, *International Journal of Science and Research (IJSR),* 2016.

Ključnikov, A., Mura, L. and Sklenár, D., Information Security Management In SMEs: Factors Of Success, *Entrepreneurship and Sustainability Issues,* vol 6, no. 4, 2019.

Liberati, A. et al., 2009. The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. *PLoS Medicine*, 6(7), e1000100.

Maarop, N. et al., Understanding Success Factors of an Information Security Management System Plan Phase Self-Implementation. *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering,* vol. 9, no. 3, 2015.

Metalidoua, E., Marinagic, C., Trivellasc, P., Eberhagen, N., Skourlasd, C. and Giannakopoulos, G., The Human factor of Information Security: Unintentional Damage Perspective, *Procedia - Social and Behavioral Sciences 147 (2014) 424 – 428*, 2014.

Norman, A. A. and Yasin, N. b. M., Information Systems Security Management (ISSM) Success Factor: Retrospection from the Scholars, *11th European Conference on Information Warfare and Security 2012*, Laval, France, 2012.

Nguyen, T. D., Nguyen, T. and Cao, T. H., Information Systems Success: A Literature Review, *Lecture Notes in Computer Science., 2015.*

Obeidat, I. and Mughaid, A., Implementing Factors of Information Security in Governmental Organizations of Jordan., *The Thirteenth International Conference on Digital Society and eGovernments*, 2019.

Park, C.-S., Jang, S.-S. and Park, Y.-T., A Study of Effect of Information Security Management System(ISMS) Certification on Organization Performance, *IJCSNS International Journal of Computer Science and Network Security,* vol. 10, no.3, 2013.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., and Jerram, C., The Influence of Organizational Information Security Culture on Information Security Decision Making, *Journal of Cognitive Engineering and Decision Making*, vol. 5, no.2, 2019.

Rajnoha, R., Korauš, A. and Dobrovič, J., Information systems for sustainable performance of organizations, *Journal of Security and Sustainability Issues, vol. 7, no. 1, 2017.*

Rosmiati, Riadi, I. and Prayudi, Y., A Maturity Level Framework for Measurement of Information Security Performance, *International Journal of Computer Applications,* 2016.

Sadeghi, R. A., Identifying Key Success Factors in the Implementation of Information Security Systems on Service Businesses: A Case Study of the Private Banks of Tehran, *American Journal of Theoretical and Applied Business*, 2016.

Sari, P. K., Nurshabrina N. and Candiwan, Factor Analysis on Information Security Management in Higher Education Institutions, *4th International Conference on Cyber and IT Service Management*, 2016.

Sarmoen, N., Khalid, H., Rasid, S. Z. A., Baskaran, S. A/L and Basiruddin, R., Understanding Human Behaviour in Information Security Policy Compliance in a Malaysian Local Authority Organization. *Business Management and Strategy,* vol. 10, no. 2, 2019.

Sharif, S. P., Mura, P. and Wijesinghe, S. N. R., Systematic Reviews in Asia: Introducing the “PRISMA” Protocol to

Tourism and Hospitality Scholars, *Quantitative Tourism Research in Asia. Perspectives on Asian Tourism. Springer*, Singapore 2019.

Singh, A. N., Gupta, M. and Ojha, A., Identifying factors of "organizational information security management", *Journal of Enterprise Information Management, 2014.*

Singh, A. N., Picot, A., Kranz, J., Gupta, M. and Ojha, A., Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany, *Global Journal of Flexible Systems Management,* 2013.

Susanto, Almunawar and Tuan, Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical and Computer Sciences IJECS-IJENS, vol. 11, no. 05, 2011.

Tatiara, R., Fajar, A. N., Siregar, B., Gunawan W., Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001, *2nd International Conference on Computing and Applied Informatics*, 2018.

Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., Bahanag, N. N. M., Effects of Information Security Management Systems on Firm Performance, *American Journal of Operations Management and Information Systems,* vol. 4, no. 3, 2019.

Tu, Z. and Yuan, Y., Critical Success Factors Analysis on Effective Information Security Management: A Literature Review, *Information Systems Security, Assurance, and Privacy Track (SIGSEC)*, 2014.

Cindy Zhiling Tu, Yufei Yuan, Norm Archer, Catherine E. Connelly, Strategic Value Alignment for Information Security Management: A Critical Success Factor Analysis*, Information, and Computer Security*, 2018.

Waly, N., Tassabehji, R. and Kamala, M., Improving Organisational Information Security Management: The Impact of Training and Awareness*, Proceedings of the 2012 IEEE 14th International Conference on High Performance Computing and Communication and 2012 IEEE 9th International Conference on Embedded Software and Systems*, 2012.

Weerasinghe, S. and Wijayanayake, J., Analysis of Human Factors In Information Security in Public Licensed Commercial Banks in Sri Lanka: An Internal Stakeholder Perspective, 2017.

Yildirim, E. Y., Akalp G., Aytac, S. and Bayram, N., Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey, *International Journal of Information Management,* 2016.

Zidane, Y. J.-T., Hussein, B. A., Gudmundsson, J. Ø. and Ekambaram, A., Categorization of organizational factors and their impact on project performance, *Procedia - Social and Behavioral Sciences 226,* 2016.

Zammani, M., Razali, R. and Singh, D., Factors Contributing to the Success of Information Security Management Implementation, *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol 10, no. 11, 2019.

Zammani, M. and Razali, R., An Empirical Study of Information Security Management Success, *International Journal on Advanced Science Engineering and Information Technology, vol.6, 2016.*

Biographies

K.M.N. De Abrew is a final year undergraduate at the Department of Industrial Management of University of Kelaniya, Sri Lanka who is reading for her BSc (Hons) in Management and Information Technology degree. She is currently completing her final year undergraduate research in the area of Information Security.

Dr. Ruwan Wickramarachchi is a Senior lecturer at the Department of Industrial Management, University of Kelaniya. He holds BSc in Industrial Management from the University of Kelaniya and an MPhil in Management Studies (specialized in Information systems) from the University of Cambridge, United Kingdom. He received his Ph.D. in distributed simulation from Sheffield Hallam University, United Kingdom. His current research interest includes applications in distributed simulation, management of information technology, and project management. Currently, he is also servicing as Director of the Information and Communication Technology Centre, University of Kelaniya.