Exploring the factors influencing the adoption of ISMS standards or frameworks

Kai Song

A dissertation submitted to the University of Dublin

in partial fulfilment of the requirements for the degree of

MSc in Management of Information Systems

1st September 2017

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: ________________________________

Kai Song

1st September 2017

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: ____

Kai Song

1st September 2017

Acknowledgements

I would like to thank my supervisor, Brian O'Kane, for his invaluable advice, encouragement and guidance throughout this research.

I would like to thank my best friend, Dr. Bryan Duggan for his constant advice and guidance at all stages of this research without whom I could not have completed this research.

I would like to acknowledge my colleagues for their support and encouragement over the past two years.

I would also like to thank all the participants who responded to my online survey and took time to complete it without whom this research is impossible.

Finally, I must thank my parents and sister for their love and support. They have been very caring throughout the duration of this course.

Abstract

In the world of new technologies, information, as a key corporate resource, is often regarded as the lifeblood of business. It is imperative for organisations to protect information assets through a system of information security to ensure organisational competencies. As a result of the continued escalation of cyber-attacks and the increasingly regulated data protection landscape, organisations tend to comply with Information Security Management System (ISMS) best practices. This research attempts to unveil the reasons for the low adoption of ISMS standards or frameworks. In addition, this research draws a clear picture of currently popular ISMS standards and frameworks, adoption status, benefits, drivers, and challenges of adoption. These findings provide a greater understanding and a comprehensive analysis of factors influencing the adoption of ISMS standards or frameworks.

This research is based on an extensive literature review and findings resulting from quantitative data collected from 92 IT or information security professionals through an online survey. Findings indicate that human factors and external influences are the two main factors influencing adoption. Human factors include defining the scope, change resistance, obtaining employee buy-in, conducting risks assessments, and creating and managing ISMS documents. External influences include the cost of implementation and the complexity of ISMS standards and frameworks.

Table of Contents

List of Figures

List of tables

Abbreviations

BSI	British Standard Institute
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
COO	Chief Operating Officer
DTI	Department of Trade and Industry
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
IS	Information Security
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ITIL	Information Technology Infrastructure Library
PCAOB	Public Company Accounting Oversight Board
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan Do Check Act
SOX	Sarbanes-Oxley Act

Chapter 1 – Introduction

1.1 Context and Background

Over the past decades, information has been increasingly recognised as an important raw material and product for most service-oriented organisations. From an economic point of view, information and the ability to process information may have more impact on a firm's productivity than operational effectiveness or product innovation (Barlette & Fomin, 2009). In the world of new technologies, information is often regarded as the lifeblood of business, without which business cannot function (Peppard, 2007; Barlette & Fomin, 2009; Sharma & Dash, 2012). Given the immense value to organisations, it is important to secure information assets through a system of information security to ensure organisational competencies.

In recent years, the rapid development of technology has dramatically increased online business opportunities, but this has led to growing information security challenges (Soomro et al., 2015). In the world of e-commerce, information security regarding data breaches, consumer privacy issues, identity thefts, and other online threats is a major concern (Udo, 2001). Unfortunately, no single formula guarantees absolute information security. In the last decade, information security risks have become a top priority on senior management agendas because of the increased incidence of security breaches and the direct and potential cost (IT Governance, 2016). The recent UK Government Information Security Breaches report indicates that security breaches are becoming more common for every type of business, regardless of its size. Klahr et al. (2016) reported that the most costly breach identified was £3 million. In 2013, 93% of large organisations and 87% of small businesses in the UK were breached (Ring, 2013). According to a benchmarking report from the Ponemon Institute in 2015, the average total cost of a data breaches in the UK has risen to £2.37 million (Ponemon Institute, 2015). Furthermore, the introduction of EU General Data Protection Regulation (GDPR) laws, which will be enforced across EU countries in May, 2018, will increase the potential cost of noncompliance (European Commission, 2016). Apart from monetary penalties, inadequate security of information systems may result in regulatory non-compliance. According to the Sarbanes-Oxley Act (2002), organisations are legally responsible for the validity of reported financial data and the status of information systems where such financial data is stored and processed. Therefore, the importance of protecting information from being compromised has become vital for a company's daily operations and survival (Fomin et al., 2008). As a result of the continued escalation of cyber-attacks and the increasingly regulated data protection landscape, it is imperative for organisations to establish, implement, and maintain an effective Information Security Management System (ISMS) to manage critical information assets (IT Governance, 2016).

Without information security, organisations face various security issues including service disruption, data leakage, financial misstatements, successful internal and external attacks caused by ineffective information security management resulting in reputation damage, loss of market share, and regulatory censure (Humphreys, 2006). According to Aalders & Hind (2002), when a company experiences computer outage lasting longer than 10 days, they never fully recover—50% will be out of business within five years. The chance of going out of business is increasing as contemporary companies rely more on information systems. As a result, organisations without strong data loss prevention (DLP) are seeking to increase their capabilities (Advanced Network Systems, 2008). According to The Economic Times (2017), global spending on information security products and services will increase to $84.6 billion in 2017, which is an increase of 7% on last year. This number is expected to grow up to $93 billion in 2018. The increasing spending on information security addresses the importance of informational processes. Organisations should take an active role to protect their critical information assets (Barlette & Fomin, 2009). In the process of achieving this task, senior management faces various issues. Key questions should be addressed: How to secure an organisation's information? How to improve an organisation's current information security position? How to establish information security management? Would the investment be cost effective? How to identify the current information security level of an organisation? Which information security level would be appropriate for an organisation? What are the best practices for information security management?

Many studies have examined and addressed the importance of adopting ISMS standards or frameworks (Humphreys, 2011; Susanto et al., 2011; Sharma & Dash, 2012; IT Governance, 2016) to answer many of the above questions, if not all of them. However, implementation of ISMS standards or frameworks is a complex process. Simply ensuring organisational compliance with one of these standards or frameworks can be challenging.

Recent research indicates that some of these standards and frameworks are not well adopted (IT Governance, 2016; AXELOS, 2014). A recent survey from 319 IT security decision makers at companies with more than 100 employees, indicates that only less than half (44%) have been compliant with ISMS standards or frameworks for more than 12 months (Dimensional Research, 2016). Although many studies (Fomin et al., 2008; Werlinger et al., 2009) have questioned the complexity of ISMS standards or frameworks, other factors could be affecting adoption. However, there is a paucity of literature examining the factors that influence the adoption of ISMS standards or frameworks. While the existing literature has come to a conclusion about some factors influencing information security management within organisations, it is unknown if these identified factors have the same influence on the adoption of ISMS standards or frameworks.

This research draws a clear picture of currently popular ISMS standards or frameworks, current adoption status, drivers and challenges of adoption, and benefits with a quantitative research method. In addition, this research addresses senior management concerns on the adoption of ISMS standards or frameworks.

1.2 Objectives

As outlined above, adopting ISMS standards or frameworks is imperative for organisations to protect critical information assets and ensure regulatory compliance. However, recent research indicates that some of these standards and frameworks are not well adopted (IT Governance, 2016; AXELOS, 2014). In addition, there is a paucity of literature providing reasons why the adoption level is low. As such, the primary objective here is to obtain a realistic picture of the situation to understand the reasons why the adoption level of ISMS standards or frameworks is low.

In attempting to respond the primary research objective, the following sub-objectives are raised:

- To examine factors influencing the adoption of ISMS standards or frameworks
- To identify challenges of adopting ISMS standards or frameworks
- To summarise the concerns of senior management when adopting ISMS standards or frameworks

1.3 Research Questions

The goal of this research is to explore factors influencing the adoption of ISMS standards or frameworks and identify reasons why the adoption level is low. Additionally, this research will present the benefits, challenges, and barriers to adoption processes. Lastly, senior management concerns will be discussed.

The fundamental research question is:

What are the factors influencing the adoption of ISMS standards or frameworks?

Two sub-questions are:

SQ1: What are the challenges and barriers to adopting ISMS standards or frameworks?

SQ2: What are the concerns of senior management when adopting ISMS standards or frameworks?

1.4 Beneficiaries of Research

This research will be of interest to any organisations that are planning to implement, are implementing, or that have already implemented ISMS standards or frameworks. These organisations include those using information systems for information processing or storage, regardless of business type, size, and location.

In particular, this research presents and compares several currently popular ISMS standards and frameworks. It would be of great benefit to organisations to choose ISMS standards or frameworks appropriate to their operation. To a certain level, this research increases the awareness of such standards and frameworks.

This research is based on an extensive literature review and findings from quantitative data collected via an online survey distributed via LinkedIn® and information security related forums from participants who are IT or information security professionals. Thus, participants were not restricted to geographic locations. As such, this research will be of benefit to researchers for further studies on ISMS standards or frameworks.

1.5 Scope of Research

This research primarily focuses on exploring what factors influence the adoption of ISMS standards or frameworks. It focuses on unveiling and summarising the reasons why the adoption level of ISMS standards or frameworks is low.

1.6 Chapter Structure

The structure of this dissertation is as follows:

Chapter 1 – Introduction

This chapter introduces the context and background of the research topic, explains why the research is important, and outlines the research objectives, questions, beneficiaries, and scope.

Chapter 2 – Literature Review

This chapter provides a critical review of existing literature on information security management including a definition of ISMS, a review of currently popular ISMS standards or frameworks, and a review of key factors affecting information security management.

Chapter 3 – Methodology and Fieldwork

This chapter provides a brief overview of the research philosophies, methodologies, and strategies used by the lead researcher. Rationales for the chosen research philosophies and approaches are presented. It also includes ethical issues, problems encountered, and lessons learned.

Chapter 4 – Findings and Analysis

This chapter comprises data analysis and an interpretation of the findings resulting from the primary data collected from an online survey. The results of data analysis will address the proposed research questions.

Chapter 5 – Conclusions and Future Work

This chapter presents the conclusions from data analysis carried out as part of this research and demonstrates how the generated findings have answered the research questions. Key findings of this research are listed. Additionally, a discussion on the generalisability of findings is presented. Lastly, the limitations of the research and future research directions are outlined.

Chapter 2 – Literature Review

In order to present an overview of the key factors influencing the adoption of ISMS standards or frameworks, a systematic review of existing literature on challenges and barriers of implementing ISMS has been conducted. To obtain a basic understanding of what ISMS is, why it is important, and how it can be achieved in organisations, a general theory of ISMS is first described. Then, a summary of most popular ISMS standards and frameworks is presented. Further, a critical review of the key factors affecting information security management and the limitations of existing research on the adoption of ISMS standards or frameworks are provided. The aim of the literature review is to build a foundation for the research questions through the identified key factors affecting information security management. Each step within the literature review is supported by searching existing literature and using the findings to aid logical reasoning.

2.1 Background

In the world of new technologies, information is often regarded as the lifeblood of business: it is a key corporate resource and it must be managed effectively, in a proactive manner, to ensure organisational competencies (Peppard, 2007). In recent years, the rapid development of technology has dramatically increased online business opportunities; however, this has led to growing information security challenges (Soomro et al., 2015). In the world of e-commerce, information security, in relation to data breaches, consumer privacy issues, identity thefts and other online threats, is a major concern (Udo, 2001). Unfortunately, no single formula guarantees absolute information security. In the last decade, information security risks have become a top priority on senior management agendas because of the increased reporting of security breaches and the direct and potential cost (IT Governance, 2016). The recent UK Government Information Security Breaches report indicates that security breaches are becoming more common for every type of business, regardless of its size. Klahr et al. (2016) reported that the most costly breach identified was £3 million. In 2013, 93% of large organisations and 87% of small businesses in the UK were breached (Ring, 2013). According to a benchmarking report of Ponemon Institute in 2015, the average total cost of a data breach in the UK has risen to £2.37 million (Ponemon Institute, 2015). Also with the introduction of EU General Data Protection Regulation (GDPR) laws, which will be enforced across EU countries in the May of 2018 the potential cost of noncompliance will increase (European Commission, 2016). Therefore, the importance of protecting information from being compromised has become vital for a company's daily operations and survival (Fomin et al., 2008). As a result of the continued escalation of cyber-attacks and the increasingly regulated data protection landscape, it is imperative for organisations to establish, implement and maintain an effective ISMS to manage their information assets (IT Governance, 2016).

"Without information security, the business is faced with various negative impacts including financial consequences, weakened protection of the organisation's intellectual capital and IPR, loss of market share, poor productivity and performance ratings, ineffective operations, inability to comply with laws and regulations, or loss of image and reputation"(Humphreys, 2006)

2.2 Definition of ISMS

"An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process" (ISO, 2016).

An Information Security Management System (ISMS) is a set of policies and procedures defined by an organisation for systematically managing sensitive information to ensure that the principle of confidentiality, integrity and availability is adhered to (Susanto et al., 2011; Cherdantseva & Hilton, 2013). The ISMS concept was first described by Pro. Edward Humphreys in his successful quest to develop the first ISMS standard –BS 7799 issued in 1995 by the British Standard Institute (BSI) as a code of practice of information security management (Humphreys, 2011). Following on from this the UK launched the BS 7799 ISMS certification scheme to increase the awareness of this ISMS standard. As a result, by the end of 1999 more than 20 countries had adopted this standard and the number of certified organisations had been significantly increased (Humphreys, 2011).

Beginning with the BS 7799 standard many ISMS standards and frameworks are also published. Some examples include ISO 27001, PCI DSS, ITIL and COBIT (Susanto et al., 2011). For each standard, there are many implementation guidelines for organisations to choose depending on the nature of business, information security maturity level, company size and budget. However, ensuring organisational compliance with one of these standards or frameworks is challenging. Recent research indicates that some of these standards and frameworks are not well adopted (IT Governance, 2016; AXELOS, 2014). It is noted that, in a recent survey from 319 IT security decision makers at companies with more than 100 employees, only less than half (44%) have been compliant with ISMS standards or frameworks for more than 12 months (Dimensional research, 2016). In order to help organisations effectively establish, implement and maintain ISMS, many studies (Dojkovski, 2006; Rocha Flores et al., 2014; Barton et al., 2016; Chmura, 2016) have analysed the key factors that may affect ISMS within organisations, such as information security awareness, effective risk analysis, positive management, knowledge sharing, and organisational culture. Meanwhile, barriers to ISMS implementation have been argued, such as limited knowledge of applicable standards and frameworks, poor management commitment, wrong perceptions on cyber-attack targeting SMEs, limited budget, standard complexity, resistance to change, and inadequate academic publications (European Union Agency for Network and Information Security, 2015; Fomin et al., 2008; Khyavi & Rahimi, 2015).

2.3 ISMS Standards and Frameworks

In this section, an overview of most popular ISMS standards and frameworks is presented: ISO 27001, PCI DSS, COBIT, and ITIL. The overview includes profile, purpose and function for each standard in implementing ISMS for organisations.

2.3.1 ISO 27001

As mentioned above, ISMS was first introduced within the standard of BS 7799-1 written by the Department of Trade and Industry (DTI) in the late 80's and then issued by the BSI in 1995. The BS 7799-2 was published in 1999, titled "Information Security Management Systems – Specification with guidance for use". After approved for publication as ISO/IEC 17799 in October 2000, BS 7799-1 joined the ISO/IEC as a code of practice for information security management. It was then renumbered as ISO/IEC 27002 in 2006. This was after the introduction of BS 7799-2, which was then published as ISO/IEC 27001 in November 2005 (Humphreys, 2011). The main difference between ISO/IEC 27001 and ISO/IEC 27002 is that ISO/IEC 27001 only provides a prescription of the features of an effective ISMS, while ISO/IEC 27002 gives instructions and guidance on how to conduct the standard (IT Governance, 2013).

This standard is applicable to all types of organisations, all sizes, all industries and markets (ISO, 2013). It introduces a series of security process based on the well-known "Plan-Do-Check-Act" (PDCA) model (Figure 2. 1), which is a continuous improvement process that requires organisations to review their ISMS regularly to ensure the effectiveness (Humphreys, 2011; Susanto et al., 2011).

The purpose of the standard of ISO/IEC 27001 is to provide an approach that "*based on a business risk approach, to establish, implement, operate, monitor, review, maintain and* *improve information security*” (Calder, 2011). The effectiveness of complying with ISO/IEC 27001 for organisations is preventing or minimising the exposure to information security threats.

The core of this standard is information security risks assessment and management (IT Governance, 2017). A quantitative study identifies that companies compliant with ISO /IEC 27001 gain an improved risk based approach to information security management (Sharma & Dash, 2012). Similar research on the cost-benefit analysis of an ISMS based on ISO/IEC 27001 through a comparison of the KPI of effectiveness and efficiency argues that an ISMS based on ISO/IEC 27001 is equivalent to risk management (BOEHMER∗, 2009).

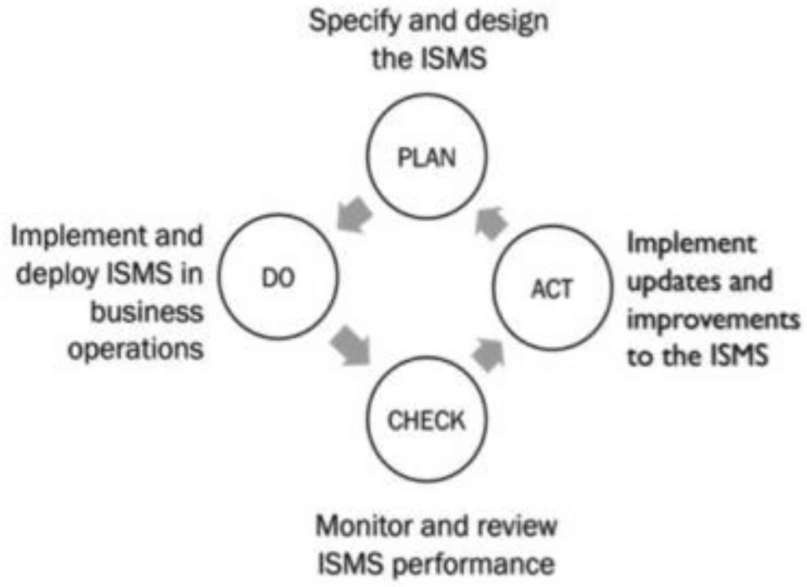


Figure 2. 1 PDCA Model (Humphreys, 2011)

2.3.2 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted proprietary information security standard defined by the Payment Card Industry Security Standards Council that is managed by major credit card brands (American Express, Discover, JCB, Visa, and MasterCard). PCI DSS is regarded as a key benchmark determining if a company has adequate security countermeasure to protect the cardholder data. Extensive industry rules are included in PCI DSS, which are updated regularly to reflect the latest best practices (Ramsey, 2016). These industry rules are related to the following main areas: Network and Systems; Protection of Cardholder Data, Vulnerability Management Program, Access Control, Monitoring and Testing of Networks, and Information Security Policy (Ukidve et al., 2017).

The purpose of this standard is to help entities process, store or transmit cardholder information in a secure environment, reduce the risk of compromised credit card data, protect the confidentiality of cardholder data, and to prevent credit card fraud (Ramsey, 2016; Ukidve et al., 2017; Coburn, 2010).

It should be noted that PCI DSS standard is not a law. Although it must be implemented by all entities that process, store or transmit cardholder information, formal validation of the compliance is not mandatory. But it should not be regarded as a reason for non-compliance (Bonner et al., 2011). A report indicates that nearly half of the reported security breaches were non PCI DSS compliant (Coyler & Clement, 2005). In the event of a security breach, entities are subject to penalties if there were noncompliance (European Union Agency for Network and Information Security, 2015). Considering the high cost of data breach, organisations should comply with this standard to protect the information asset effectively. A compliance should be a continuous process rather than just meet the audit requirement annually. To ensure the compliance, validation can be carried out internally or externally annually, depending on the classified compliance tiers (one to four) relating to the volume of transitions in the past 12 months (Ukidve et al., 2017). Organisations with an annual number of transaction volume of 6 million or more are subject to the compliance validation conducted by an independent assessor, Qualified Security Assessor. Other organisations handling a smaller volume of transactions annually can carry out self-assessment scanning quarterly (Susanto et al., 2011).

2.3.3 COBIT

Control Objectives for Information and Information related Technologies (COBIT) is a good practice IT governance framework created by international professional association ISACA and the IT Governance Institute in 1996 (IT Governance Institute, 2007). It was created as an IT audit framework at the beginning. As such, it focuses more on internal IT controls within an organisation (Devos & Van de Ginste, 2015).

The purpose of COBIT framework is to provide business owners and management with an information technology framework that delivers business value, meets business requirements, and that aligns IT strategy with business strategy to support organisations in achieving business goals (IT Governance Institute, 2007; ISACA, 2017).

COBIT has 5 key principles: Strategic alignment; Value delivery; Resource management; Risk management; Performance measurement (Susanto et al., 2011; Devos & Van de Ginste, 2015). It also consists of 34 IT processes to contribute to effective internal controls over the reliability of financial reporting. An international survey of professionals indicated that some of these IT processes were critical for effectively governing internal IT environment via internal IT controls (Kerr & Murthy, 2007).

In 2012, the new version of COBIT was released by ISACA, called by COBIT 5. It helps organisations meet performance and compliance requirements. COBIT 5 is aligned with some well-known frameworks, such as ITIL, ISO/IEC 20000 and ISO/IEC 27001 (Radhakrishnan, 2015). It provides a comprehensive IT governance framework that "*assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT*" (Nugroho, 2014). It also has 5 key principles to improve the performance of IT to ensure that IT delivers business value (Radhakrishnan, 2015) (Figure 2. 2).

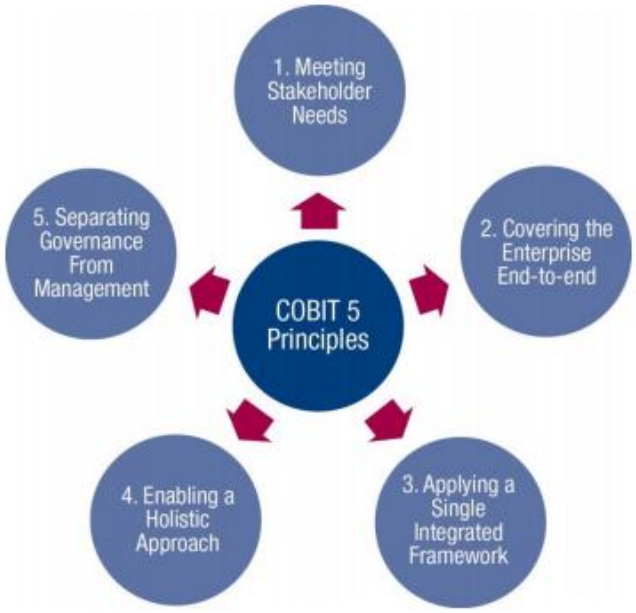

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Figure 2. 2 COBIT 5 Principles Source: ISACA, COBIT 5, USA, 2012

2.3.4 ITIL

The Information Technology Infrastructure Library (ITIL), which was introduced by the Office of Government Commerce (OGC) in the UK in the late 1980s, is a set of concepts and practices for IT service management (ITSM) that focus on aligning IT services with the needs of the business. At present, it is the most widely accepted approach to IT service management in the world (Sahibudin et al., 2008; AXELOS, 2017).

The initial purpose of ITIL was to reduce the IT costs and to better manage the IT delivery when the British government were not satisfied with the quality of IT service (Sallé, 2004). It provides a framework for the governance of IT and focuses on continual measurement and improvement of the quality of IT service. It builds a bridge between IT and business to enable IT to deliver business value via effectively aligning IT strategy with business strategy.

The ITIL framework consists of five service delivery processes, five service support processes and one service support function (service desk). The five service delivery processes are Service Level Management (SLM), Financial Management, Capacity Management, IT Service Continuity Management, and Availability Management. The five service support processes are Incident Management, Problem Management, Change Management, Release Management, and Configuration Management (Cater-Steel, 2006).

A research paper on ITIL adoption through case studies at five large organisations in Australia indicated that implementing ITIL within organisations can transform IT service management to ensure that IT service is effectively managed, IT strategy is aligned with business strategy, and that IT supports organisations in achieving business goals (Cater-Steel, 2006).

2.4 Key factors affecting information security management and limitations of existing research

This section will synthesise existing literature on the key factors affecting information security, such as senior management commitment, external influences, and human factors (Figure 2. 3). Relevant literature has been identified through a rigorous systematic search process. And for each identified factor, an analysis of the selected literature is presented.

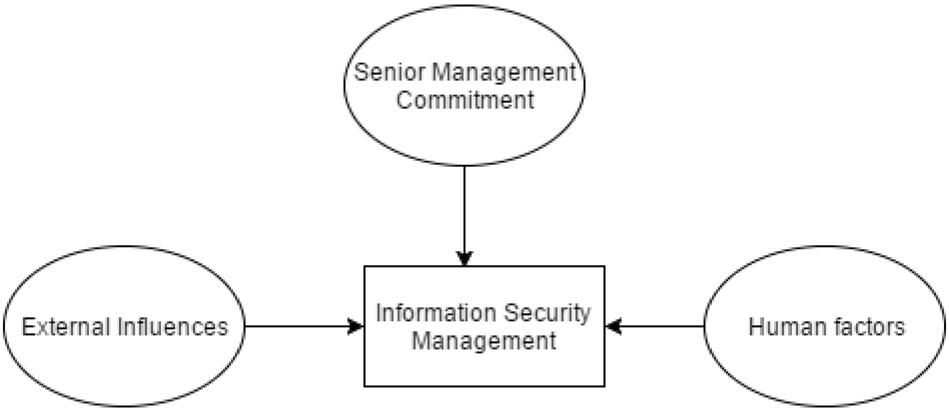


Figure 2. 3 Key factors affecting information security management

2.4.1 Senior Management Commitment

Although now in the technology world, many cutting edge technologies have emerged in recent years and they are utilised to protect organisations' data and information, information security risks are still the greatest challenges to most organisations (Ring, 2013; Ponemon Institute, 2015). Research (McFadzean et al., 2006) indicates that technology alone does not guarantee the success of information security. Information security should be considered and managed from a managerial perspective (Soomro et al., 2015; Barton et al., 2016; Van Kessel, 2012). Many studies on information security have identified that senior management commitment is critical to successful information security management. Further, information security governance should be deemed as one of board level responsibilities (Barton et al., 2016; McFadzean et al., 2006; Knapp et al., 2006; Van Kessel, 2012; Alberts & Dorofee, 2002; Ma et al., 2009). It is imperative for the board of directors to take the responsibility of an organisation's success, including protecting the "lifeblood" of business- information (McFadzean et al., 2006). By their commitment, senior management help paves the way towards information security management within organisations.

The definition of "senior management" can vary from organisation depending on its size and structure. But in general, senior management refers to members of the top management who make key strategic decisions within organisations, including the Chief Executive Officer (CEO), the Chief Information Officer (CIO), the Chief Financial Officer (CFO), the Chief Operating Officer (COO), and other members of top management. Given the fact that senior management is the prime sponsor and motivator of information security projects, information security researchers believe that senior management commitment is necessary and critical to successful information security management within organisations (Barton et al., 2016; Alavi et al., 2014; Sharma & Dash, 2012; Van Kessel, 2012; McFadzean et al., 2006). For instance, with senior management support, an adequate budget for information security projects, such as an implementation of ISMS, can be allocated. On the other hand, senior management commitment can drive organisational changes and improve employees' compliance. Although senior management commitment alone does not guarantee effective information security management, senior management commitment and support is a prerequisite for effective development, implementation, and maintenance of ISMS within organisations (Barton et al., 2016).

The intent of involving senior management within information security management is to ensure information security objectives and activities are aligned with business objectives. And this alignment can only be achieved through senior management commitment and their support. As such, raising information security awareness of senior management has been found necessary to gain their commitment and support in information security management within organisations. For each information security project, despite being well-motivated, senior management is also required to have a better understanding of information security and clear expectations of what benefits can be expected from the information security project (Imszennik, 2017; Kajava et al., 2006). As such, senior management's IT knowledge is critical and can influence the degree of their involvement in information security management. Li et al. (2007) indicate that organisations with senior management members who have IT background or IT knowledge are less likely to have material weaknesses in IT internal controls over financial reporting.

By summarising the existing literature, reasons why senior management commitment is critical to successful information security management are listed as follows:

Leadership

Senior management has a core responsibility for business activities to ensure all parts of business are delivering business value as expected (Soomro et al., 2015). As information security issues are on senior management agenda, decisions made from the managerial perspective can drive organisational changes to information security management, which can potentially reduce or mitigate risks to information systems and organisations (Barton et al., 2016). All of these information security decisions are made through assessment strategies or strategic decision-making processes, such as risk assessment, cost benefits analysis, balanced scorecard usage and SWOT analysis, should be made from a managerial level considering all factors that may affect the delivery of business value (Papadakis et al., 1998). As such, effective senior management decision-makings can drive an organisation in achieving business goals and reduce risks to information systems.

Governance responsibilities

Senior management also takes governance responsibilities within organisations, which include information security governance. Key responsibilities include policy-making, controls development and compliance monitoring, communication, and security training (McFadzean et al., 2006). Within these senior management activities information security awareness training, information security policy development & implementation are the most important components of security programs (Soomro et al., 2015; Ma et al., 2009). They have a significant role in protecting organisational data from being breached (Bulgurcu et al., 2010). This is accepted by Whitman (2004) who argues that the effectiveness of information security relies on three key factors: information security policies, security mechanisms (controls), and information security awareness. And they are all managed by senior management. Without senior management support, information security cannot be established, implemented and maintained.

Vision and Plan

Senior management has a holistic view of an entire organisation, including a view of the trend in the near future (McFadzean et al., 2006). They also have access to various organisational resources and assets, which pave the way to effective information security management within organisations. With a visibility to each part of business functions, including IT activities, directors of boards are able to make better decisions on information security management to ensure there are no disagreements within the units of an organisation. They also have a better control of information security investments to ensure each investment on information security complies with business requirements. And this relies on the financial backing from senior management within organisations (Ghonaimy et al., 2002).

2.4.2 External influences

Barton et al. (2016) show that external influences motivate senior management commitment to information security management through two phases: firstly, senior management belief increases senior management participation; secondly, greater senior management participation leads to greater information security assimilation. Information security assimilation refers to the ability of an organisation to assimilate technology, security awareness and may extend to the ability to respond various external influences (Barton et al., 2016).

External influences, such as increased reporting of security breaches, high cost of security breaches (both directly and potential cost), technology changes, and regulatory forces have a significant impact on information security management through affecting IT controls quality that is regarded as a critical role in business (Li et al., 2007). As a key driver of senior management commitment, external influences also provide senior management with the awareness of information security situation and landscape (Franke & Brynielsson, 2014; Holgate et al., 2012). In 2013, 93% of large organisations and 87% of small businesses in the UK were breached (Ring, 2013). According to a benchmarking report of Ponemon Institute in 2015, the average total cost of a data breach in the UK has risen to £2.37 million (Ponemon Institute, 2015). The increasing reported security breaches and high cost on average for each breach are driving organisations to allocate more resources and efforts on information security management.

Among these external influences, regulatory compliance is the most concern within organisations. While information security concerns had been on the backburner of senior management, they have certainly been the top priority on the agenda of senior management as the result of mandatory rules enforced by regulators or industry groups (Hu et al., 2007). Studies (such as Hu et al., 2007; Ghose & Rajan, 2006) show that regulatory forces are powerful drivers for information security management within organisations. For example, the upcoming law, General Data Protection Regulation (GDPR), will drive information security changes within organisations. Data-processing companies need to be prepared, as they will otherwise be liable for fines of up to 4% of annual global turnover or €20M (Ashford, 2016). Regulatory changes require senior management prompt consideration to ensure that amended business practices, supported by IT systems and operational processes are compliant with this new regulation (Grant Thornton, 2017). Another example would be the landmark Sarbanes-Oxley Act (2002). In section 404 of this act, it requires that public companies should document and assess internal control systems to identify the effectiveness of internal controls, including information technology controls. As most critical information stored and processed digitally within ICT systems, internal information technology controls are an integral part of the overall internal control systems (Li et al., 2007). As such, it is important for auditors to provide evidence that financial applications and supporting sub-systems and networks, where financial data is processed or stored, are adequately secured to ensure the integrity of financial data (Ghose & Rajan, 2006). Except for mandatory rules, such as GDPR and SOX section 404, industry groups also have an influence on senior management regarding information security management within organisations. The Public Company Accounting Oversight Board (PCAOB) specifically states that the effectiveness of controls, including information technology general controls, on which other controls are dependent, should be assessed in management's assessment process (PCAOB, Standard No.2, 2004).

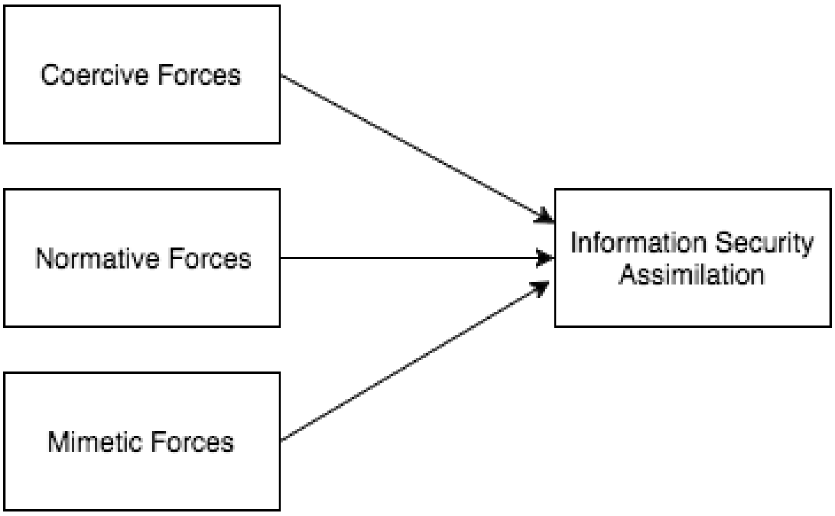


Figure 2. 4 External Influences –Conceptual Framework

Internal and external influences on information security management are often analysed from three institutional isomorphic processes – coercive, normative, and mimetic processes presented from the perspective of neo-institutional theory (Hu et al., 2007; Barton et al., 2016; Bulgurcu et al., 2010). The neo-institutional theory is one of the main theoretical perspectives used to understand factors affecting organisational behaviour. These factors can be categorised as coercive isomorphic mechanisms, mimetic isomorphic mechanisms, and normative isomorphic mechanisms (Björck, 2004). This theory is adopted for research within disciplines as diverse as economics, political science, sociology, and business studies (Barton et al., 2016; Björck, 2004). Figure 2. 4 shows the conceptual framework.

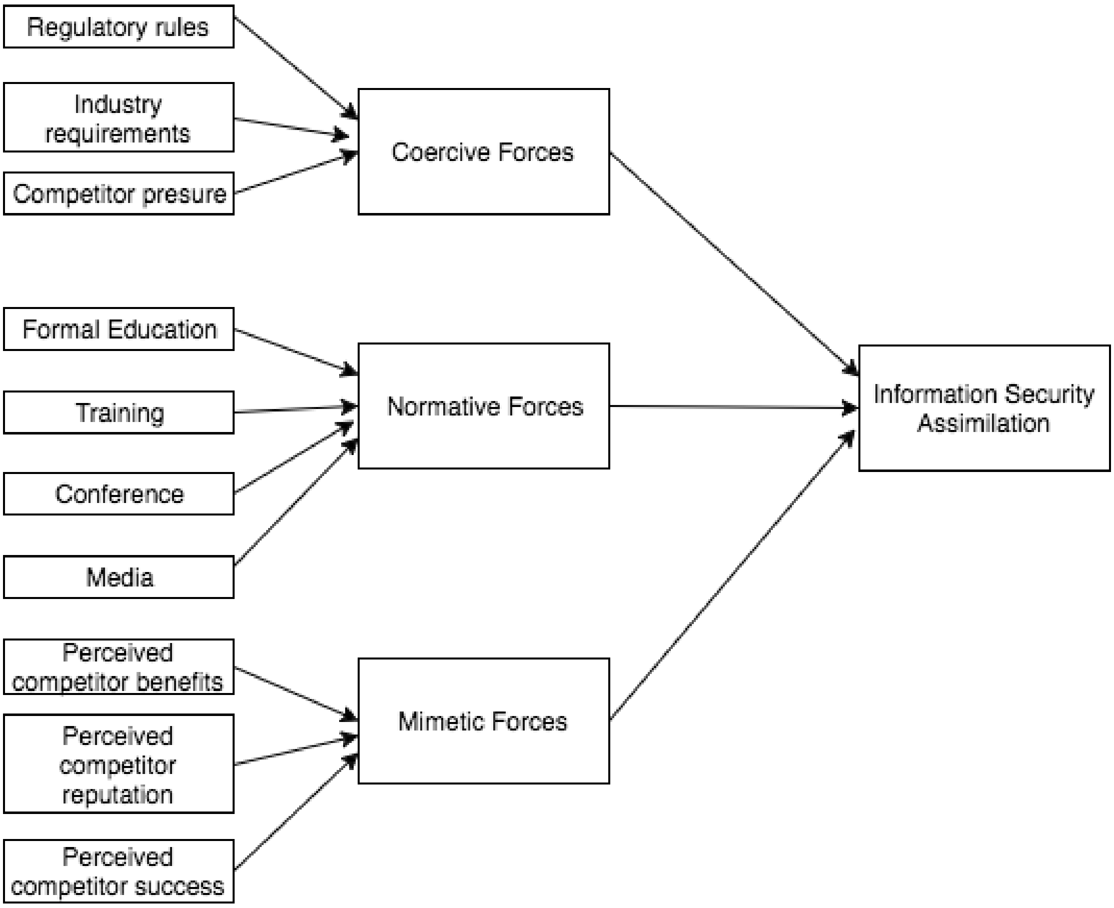


Figure 2. 5 External Influences in detail

More specifically, the coercive institutional isomorphic process has an impact on information security management within an organisation influenced by rules and regulatory requirements of agencies that oversee the organisation. For example, some regulatory rules, such as PCI DSS or GDPR, are enforced within some data processing organisations. This force has a direct influence on senior management in relation to information security management. The normative institutional isomorphic process has an impact on information security management within an organisation influenced by their sense of professionalism. It has two main sources: formal education and professional networks (Palthe, 2014). This process emphasises the role of social obligation and is likely to focus on informal structures rather than formal structures within organisations. It is manifested through education and training, which have influences on beliefs (Barton et al., 2016). The mimetic institutional isomorphic process has an impact on information security management within an organisation influenced by other peer competitors perceived to be successful. It is important in uncertainty or when technologies are not well adopted in decision-making processes. In such situations, organisations tend to mimic other peer organisations that are perceived as legitimate and successful (Barton et al., 2016; Liang et al., 2007). Liang et al. (2007) suggest that mimetic pressures positively affect top management beliefs in the need for information security. As discussed above, top management beliefs increase senior management participation, which will lead to information security assimilation (Barton et al., 2016; Liang et al., 2007). Figure 2. 5 shows external influences from the three perspectives in detail.

Hu et al. (2007) indicate that all the three institutional isomorphic processes play significant but different roles in information security management. More specifically, Barton (2016) argues that only mimetic mechanism has a strong influence on senior management belief, which increases senior management participation in information security management. Hu et al. (2007) agree that coercive influences, such as regulatory forces have a different effect than the normative influence, which will motivate senior management to mandate top-down information security management and reduce security risks to information systems and the organisation.

2.4.3 Human factors

Although technical controls are in place within most organisations to mitigate the risk of human mistakes or insider attack (such as controls on data encryption, logical access, segregation of duties, activity monitoring, compliance monitoring, and auditing), human factors are still the Achilles' heel in achieving information security (Colwill, 2010; IBM, 2015). No matter to what extent automatic processes might be within any computer-based system, information security is still determined by human actions (Björck, 2004). Alavi et al. (2014) suggest that all kinds of human factors can deeply affect information security management within organisations. This is based on the fact that information security systems are designed, implemented and maintained by people and that human factors are the most vulnerable part of information security systems. Therefore, to improve the robustness of information security systems, information security management should consider human factors as key elements.

As mentioned above technology alone does not guarantee effective information security management (McFadzean et al., 2006; Alavi et al., 2014). To effectively manage information security, organisations should achieve a balanced approach of technical, human and organisational factors (Werlinger et al., 2009). Within the three key factors, human factors play a critical role in the majority of security breaches, as most of security breaches are partially due to employees' mistakes (Gonzalez & Sawicka, 2002; IBM, 2015). For instance, most organisations have password policies that require complex passwords. As lacking security awareness, employees write down their passwords and leave them on their desks. This behaviour increases the risk of unauthorised access resulting in data theft and reputation damage. Research indicates that human factor is the weakest link in effectively maintaining information security within organisations (Chmura, 2016).

Given the fact that a well-designed ISMS still has to rely on people (Gonzalez & Sawicka, 2002), many studies conclude that maintaining the effectiveness of ISMS is deeply affected by human factors, such as information security awareness, senior management support, security knowledge and skillsets, and communication (Alavi et al., 2014; Soomro et al., 2015; Rocha Flores et al., 2014). Without effective management of those human factors, organisation will be facing with insider threats that pose security risks due to their knowledge of information assets and privilege access to information systems. For instance, with the use of firewalls and intrusion detection/prevention systems, cyber-attacks can be identified and/or prevented from outside of an organisation in a timely manner. But residual risks of malicious activities or ignorance from inside still remain (Colwill, 2010). According to Van Zadelhoff (2016), insiders are today's biggest security threat. IBM research (2015) indicates that 55% of cyber-attacks are carried out by insiders. With many advantages over an outside attacker, insider security threats can cause more damage to organisations, as they have more privileges and know how to achieve the greatest benefit without being noticed (Colwill, 2010). However, insider security threats are often ignored by organisations (Colwill, 2010; Parker, 2017).

Although potential insider security threats always exist within organisations and most organisations fail in addressing them, risks of insider security threats can be assessed and controlled through risk assessment, security training, knowledge sharing, activity and compliance monitoring (Pfleeger & Stolfo, 2009; Rocha Flores et al., 2014). For instance, to prevent employees from writing down their passwords, organisations should have periodic security awareness training advising all employees about information security policies and systems. Key elements of security awareness include motivation (to ensure all stakeholders' requirements are met), involvement (to ensure all stakeholders are involved), individual roles and responsibilities (to ensure all stakeholders' roles and responsibilities are clearly presented), and training (to ensure all necessary security topics, knowledge and skills are included) (Alavi et al., 2014). With regard to risk assessments, human factors should be taken into consideration as a key element. For example, risk assessments should be conducted on privileged access accounts that have a potential to change security settings or alter security logs; suspicious activities should be identified and monitored within key financial systems and databases (Colwill, 2010).

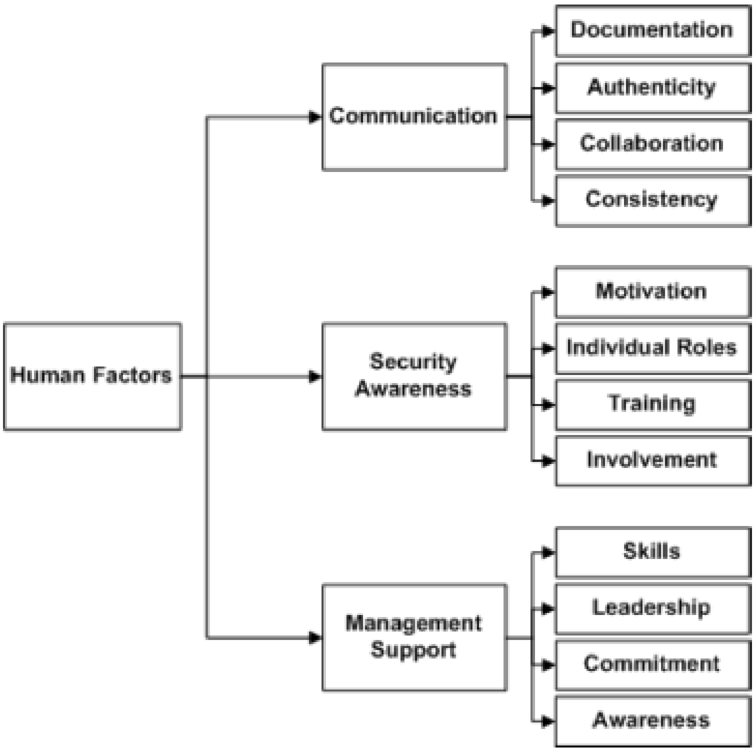


Figure 2. 6 Human Factors (Alavi et al., 2014)

Human factors are often categorised into three main areas: Communication, Security Awareness and Management Support (Alavi et al., 2014; Bulgurcu et al., 2010; McFadzean et al., 2006). Figure 2. 6 provides an overview of the three main areas. Kraemer et al. (2009) argue that human factors and organisational factors, such as communication, security awareness and management support, play a critical role in computer and information security management. **Communication** within organisations refers to messages and ideas exchange. Although human factors are often neglected, organisations are aware of the risks resulted by insufficient communication between information technology, management and end users (Ashenden, 2008). Bulgurcu et al. (2010) argue that effective communication is a prerequisite for information security compliance within organisations. It should include the following attributes: documentation, authenticity, collaboration and consistency (Alavi et al., 2014). Documentation provides the way to present information security policies and procedures. In information security management, it also requires that key activities and events within information systems should be logged. Authenticity ensures communication among stakeholders is necessary and reliable. Collaboration and consistency give steady and coherent communication among stakeholders (Alavi et al., 2014).

Given the fact that security awareness is influencing and shaping the attitudes and behaviour of individuals, Bulgurcu et al. (2010) indicate that providing organisational **security awareness** is the most critical factor in convincing employees to comply with information security policies and procedures. Security awareness not only makes employees aware of information security policies and procedures, but also teaches employees how to keep information assets safe from malicious attacks and other vulnerabilities (Soomro et al., 2015). Within the three defined main areas, security awareness is necessary for all employees including senior management, which should ensure that security-related policies and procedures should be compliant with stakeholders' willingness; individual's roles and responsibilities are identified; periodic security training for all employees are in place; and that all stakeholders are involved in the process (Alavi et al., 2014). The purpose of raising security awareness among employees is to develop essential competencies to deal with security-related issues. The most popular way to raise security awareness among employees is security awareness training. The main objective of security awareness training is to educate users on their responsibilities to protect business information to ensure its availability, integrity and confidentiality.

Lastly, **management support** is essential for information security management. Research (McFadzean et al., 2006) indicates that technology alone does not guarantee the success of information security. Information security should be considered and managed from a managerial perspective (Soomro et al., 2015; Barton et al., 2016; Van Kessel, 2012). Many studies on information security have identified that senior management commitment is critical to successful information security management. Further, information security governance should be deemed as one of board level responsibilities (Barton et al., 2016; McFadzean et al., 2006; Knapp et al., 2006; Van Kessel, 2012; Alberts & Dorofee, 2002; Ma et al., 2009). Management support includes the following key attributes: Skills: senior management's IT knowledge is critical and can influence the degree of their involvement in information security management; Leadership: effective senior management decision-makings can drive an organisation in achieving business goals and reduce risks to information systems. Senior management has the responsibility for information security visions and plans; Commitment: senior management commitment can help pave the way towards information security management within organisations through their support and involvement; Awareness: Senior management should have appropriate security awareness to ensure the importance of information security can be addressed within organisations (Alavi et al., 2014).

2.5 Summary of the literature

Without information security organisations are faced with various risks resulting in financial loss, reputation damage, and regulatory noncompliance caused by ineffective information security management. As a result of external influences, such as the increasingly reported security breaches and the regulatory landscape, organisations have started seeking cost effective ways to protect the “lifeblood” of business. To obtain systematic and comprehensive information security management, more and more organisations are establishing ISMS aligned with best practices. In this literature review a summary of most popular ISMS standards and frameworks, such as ISO 27001, PCI DSS, COBIT and ITIL, is presented. Although all of them are information security related standards or frameworks aiming at protecting critical informational processes within organisations, functions and purposes of them are different: ISO 27001 is an information security framework based on business risks; PCI DSS is an information security standard released by the Payment Card Industry Security Standards Council to protect cardholders’ data; COBIT is an IT governance framework which is created to map IT processes; ITIL is a good practice for IT service level management.

To in line with the main objective of the study, a systematic review of existing literature was conducted to explore key factors affecting information security management within organisations. Three key factors have been identified and analysed, including senior management commitment, external influences, and human factors. Within the three identified factors, human factors are taking the most challenging role in information security management. But this factor can be addressed through risk management, information security training and awareness, which helps organisations foster healthy information security culture. Further, positive security culture can effectively improve the operating effectiveness of information security controls within organisations. Moreover, senior management commitment is needed to gain management support for the development and enforcement of information security controls. Considering the privilege of leadership and governance responsibility, senior management commitment generates fundamental value to information security management within organisations. It is also noted that senior management commitment is affected by external pressures, such as increased reporting of information security breaches and the regulatory landscape. These external influences have critical impacts in all of coercive, normative, and mimetic processes.

Since it has not been proved by existing literature whether these identified factors would affect the adoption of ISMS standards or frameworks, this study will cover the gap to explore the reasons of the low adoption.

Chapter 3 – Methodology and Fieldwork

This chapter describes the research methodology and fieldwork for this study. Firstly, research philosophies and approaches considered will be introduced and analysed. Rationales for the adopted philosophies and approaches will be presented and discussed in detail. Secondly, research methodology and strategy will be presented in order to answer the questions how the research is designed, how to conduct this research, how to choose prospective participants, how to collect data, and what tools will be utilised to collect data. Thirdly, ethical issues will be discussed and relevant solutions will be presented. Lastly, problems encountered and lessons learned from this research will be concluded at the end of the chapter.

3.1 Research Philosophies

Philosophy is concerned with views of the world and how the world works. It tells people what knowledge itself should be, what questions people can ask about the world, which academic research approaches (inductive, deductive or adductive) should be adopted to ask those questions, and which research methods or strategies are appropriate to collect data to answer those questions (Lee & Lings, 2008). Those questions include the ones about **ontology** (*what are we studying?*), **epistemology** (*how can we have warranted knowledge about chosen domains?*), and **axiology** (*why do we study them?*) (Johnson & Clark, 2006). In an academic research process, it is important to think about the way in which researchers perceive reality, knowledge, and existence, as their perception of reality, knowledge, and existence will affect the way in which they conduct the research. Lee and Lings (2008) demonstrate philosophy as a process linking together the theoretical world and the 'real' world (Figure 3. 1). The theoretical world comprises our ideas, theories, and concepts existing in the real world. The real world is the world where we live and observe. Philosophy is concerned with exactly how to relate theoretical ideas and our perceptions to the real world, and how to transfer knowledge of real world back to theory. And this is the way in which we understand the nature of the reality (Lee & Lings, 2008).

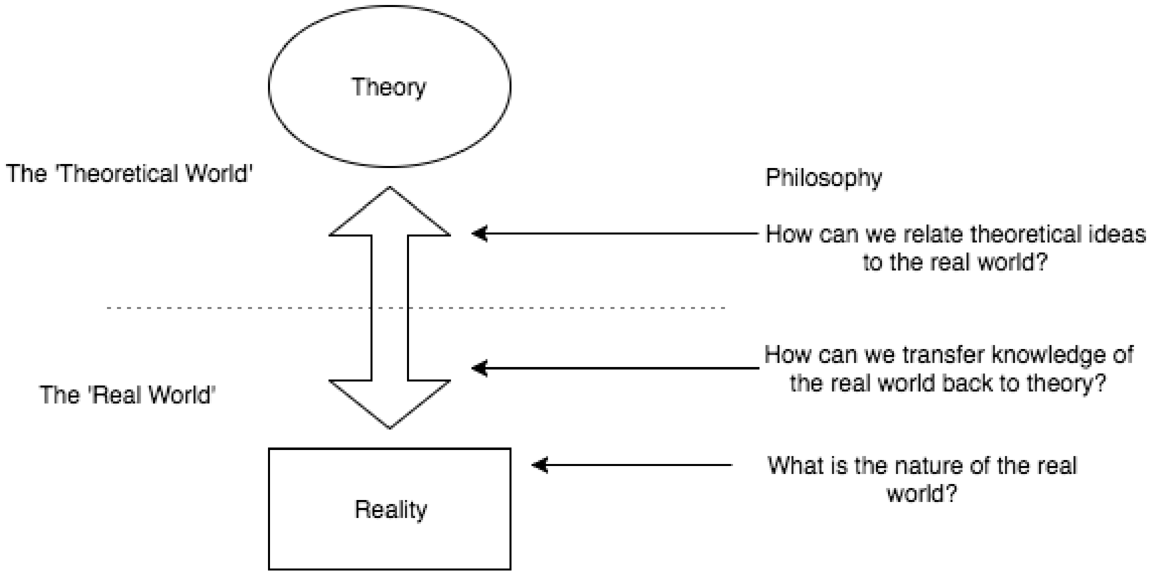

Theory
The 'Theoretical World'
Philosophy
How can we relate theoretical ideas to the real world?
The 'Real World'
How can we transfer knowledge of the real world back to theory?
What is the nature of the real world?
Reality

Figure 3. 1 Philosophy's place in research model (Lee & Lings, 2008)

A research philosophy is a system of philosophical stances, beliefs or assumptions adopted by researchers to develop acceptable knowledge and explore the nature of that knowledge. It is a belief about the way in which data about a phenomenon should be gathered, analysed, and presented. It includes important assumptions about the way in which researchers view the world and perceive reality (Saunders et al., 2016). These assumptions are usually categorised into three different types: ontological assumptions (*the nature of realities*), epistemological assumptions (*human knowledge*), and ontological assumptions (*values in research*) (Saunders et al., 2016; Crotty, 1998).

To obtain a better understanding of the adopted research philosophies and the reasons, three different types of assumptions (ontology, epistemology, and axiology) are discussed in detail, which is used to distinguish the adopted research philosophies. **Ontology** refers to assumptions about the nature of reality and every essence of the phenomena under investigation. For example, ontology might be regarded as a set of beliefs about what the world actually is. **Epistemology** concerns assumptions about the grounds of knowledge, how one might begin to communicate this as knowledge to others, what constitutes acceptable, valid and legitimate knowledge (Burrell & Morgan, 1979). It should be noted that epistemology should follow from ontology (Lee & Lings, 2008). **Axiology** refers to the role of values and ethics within research processes (Saunders et al., 2016). It incorporates questions about how researchers deal with both their own values and those of research participants. It is in essence about the 'aim' of the research and it follows again from ontology. Figure 3. 2 shows the relationship among the three different types of assumptions.

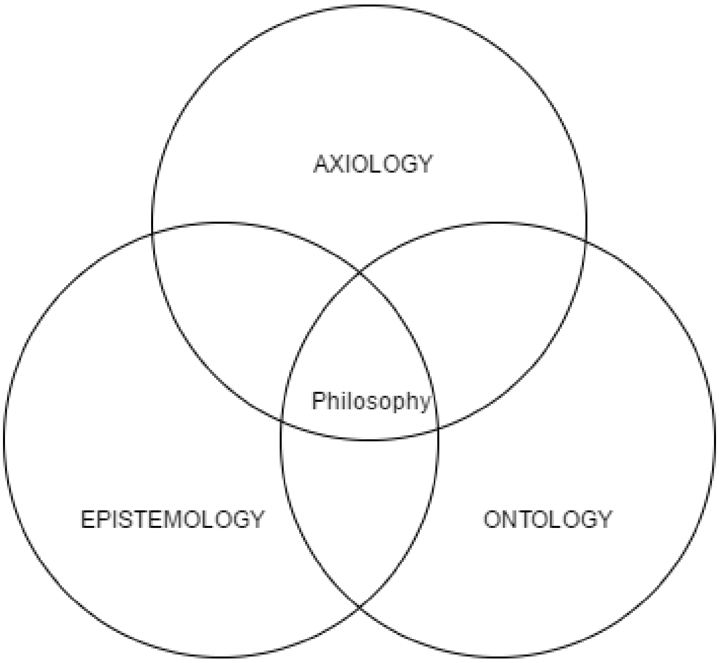


Figure 3. 2 Philosophy Assumptions

Apart from the three different types of assumptions that research philosophies make, in order to distinguish research philosophies, a multidimensional set of continua between two opposing extremes or positions (objectivism and subjectivism) are often analysed and discussed to illustrate the two different philosophical stances (Saunders et al., 2016). **Objectivism** is concerned with assumptions about natural science. Objectivist approach advocates the beliefs that the reality is external and independent from social entities' perceptions; the experiences of social entities would not affect the existence of reality. **Subjectivism** is concerned with assumptions about the arts and humanities, arguing that social reality consists of social entities' perceptions and there is no underlying and true reality that exists independent of perceptions. Table 3. 1 shows the three different types of philosophical assumptions in relation to the two continua extremes. It also summaries key questions with which the three different types of philosophical assumptions are concerned.

Table 3. 1 Philosophical assumptions (Saunders et al., 2016)

Assumption Type	**Questions**	**Two positions**	
		Objectivism	Subjectivism
Ontology	• What is the nature of reality? • What is the world like?	• Reality exists independently. • Reality is external. • There is only one true reality.	• Reality is decided by perceptions of social entities • Reality is

			socially constructed. • There are multiple realities.
Epistemology	• How can we know what we know? • What is acceptable knowledge in a particular field of study? • What constitutes good-quality data? • What kinds of contribution to knowledge can be made?	• Adopt assumptions of the natural scientist. • Focus on facts. • Conclusions are supported by numbers. • Law-like generalisations.	• Adopt assumptions of the arts and humanities. • Focus on opinions. • Conclusions are supported by narratives. • Individuals and contexts, specifics.
Axiology	• What roles do values play in research choices? • How should we deal with the values of research participants?	• Value-free	• Value-bound

Saunders et al. (2016) summarised five major research philosophies. Two of them were excluded from consideration: interpretivism and postmodernism. Three of them were considered for this research, which are positivism, critical realism, and pragmatism. Rationales are provided for each identified research philosophy in the following.

Positivism refers to the philosophical stance of natural science that emphasises empirical data and scientific methods. It generates 'law-like' generalisations through an observation of the social reality by researchers. It also embraces the belief that acceptable knowledge is based on experiences of senses that are observable and measurable (Saunders et al., 2016; Crotty, 1998; Orlikowski & Baroudi, 1990). From the epistemological perspective, positivist researchers conduct their research through observations or measurements of empirical events based on large-scale sample surveys that contribute to the production of credible and meaningful data. The data will then be analysed to explain and predict behaviour and events of the nature of reality. Most positivist researchers tend to use existing theory to develop research hypotheses. These hypotheses are subject to testing by using collected quantitative data. It is noted that during the research most positivist researchers would maintain an objective stance and try to avoid elements that would have influences to findings. In other words, positivist researchers would conduct their research in a value-free way (Saunders et al., 2016). Typically, most positivist researchers adopt a highly structured research methodology in a deductive approach and they are likely to use statistical analysis to collect quantifiable data. While quantitative method is usually associated with deductive approach, within this study in order to explore and examine observable and measurable facts, quantitative data was collected through highly structured survey followed with an inductive approach. From this perspective, positivism was considered for this research.

Critical realism is a philosophy of scientific enquiry. It shows the relationship between human sensations and the truth. It also focuses on explaining what we see and experience. Sayer (2010) summarises 8 key assumptions of critical assumptions:

1. *The world exists independently of our knowledge of it.*
2. *Our knowledge of that world is fallible and theory-laden.*
3. *Knowledge develops neither wholly continuously, as the steady accumulation of facts within a stable conceptual framework, nor wholly discontinuously, through simultaneous and universal changes in concepts.*
4. *There is necessity in the world; objects – whether natural or social – necessarily have particular casual powers or ways of acting and particular susceptibilities.*
5. *The world is differentiated and stratified, consisting not only of events, but objects, including structures, which have powers and liabilities capable of generating events. These structures may be present even where, as in the social world and much of the natural world, they do not generate regular patterns of events.*
6. *Social phenomena such as actions, texts and institutions are concept dependent.*
7. *Science or the production of any kind of knowledge is a social practice.*

8. *Social science must be critical of its object.*

Critical realists consider reality as the most significant element in philosophical assumptions (Saunders et al., 2016). Ontologically, critical realists adopt the assumption that reality is external and it exists independently from human mind. And this assumption is supported by points 1, 4, 5, and 8. Epistemologically, critical realists accept that the reality is socially constructed and represented through sensations, which are some of the manifestations of things in the real world. These sensations form or develop an understanding of the real world (Easton, 2009). And this assumption is supported by points 2, 3, 6 and 7.

Critical realism embraces the stance that people understand the world through two steps. First, there are sensations and events that we experience. Second, these sensations and events are subject to mental processing (Saunders et al., 2016). By contrast, there is another type of realism that is in an extreme form, direct realism. It claims that what you see is what you get and reality can be readily accessed. And there is no second step for direct realism. As a result, direct realism is often embraced within some areas of natural science that needs to be accurately measured. In this research, direct realism is not in consideration, since the step of mental processing is critical for identifying and extracting perceptions from participants.

Pragmatism refers to the philosophical stance that adopts both objectivism and subjectivism and underlies mixed methods approach. Epistemologically, it focuses on problems, solutions, practices and relevance in a practical form without unified rules (Saunders et al., 2016; Pansiri, 2005). Pragmatist researchers recognise that reality is complex and it cannot be interpreted by a single view (Saunders et al., 2016). Most pragmatist researchers are likely to use multiple methods to conduct their research to ensure credible and reliable data. In order to meet the need for considering practical concepts and actions rather than abstract distinctions in some research, pragmatism provides a set of new philosophical assumptions and moves to a new position on the continuum. It contributes to practical solutions and embraces the two extremes supported by positivism and interpretivism. Table 3. 2 compares positivism, interpretivism and pragmatism from three key assumptions, research approach, and research strategy. As pragmatism underlies mixed methods and adopts both objectivism and subjectivism, this research philosophy was considered for this research.

Table 3. 2 Positivism, interpretivism and pragmatism

	Ontology	Epistemology	Axiology	Research Approach	Research Strategy
Positivism	Objective	Focus on observable and measurable facts	Value-free	Deductive	Quantitative
Interpretivism	Subjective	Focus on narratives, stories, perceptions and interpretations	Value-bound	Inductive	Qualitative
Pragmatism	Objective or subjective	Focus on practical solutions to ensure credible and reliable data	Value-free/ value-bound	Deductive/ Inductive	Quantitative and/or qualitative

Interpretivism refers to the philosophical stance that takes the opposite approach to positivism. From the axiological perspective, positivist researchers maintain an objective stance and follow the methods of the natural science; however, interpretivism emphasises the importance of subjective meanings and interpretations of the social world (Gray, 2009; Crotty, 1998). Interpretivist researchers adopt the assumption that the knowledge of reality is social constructed (Walsham, 2001). Orlikowski & Baroudi (1990) argue that the social world is not 'given'. Rather, it is produced and reinforced by humans through their interactions. However, humans are different with physical phenomena as humans generate meanings that are studied by interpretivist researchers. As such, interpretivism, which regards humans and their social worlds as the core components, cannot be studied in the same way as physical phenomena (Saunders et al., 2016). From the axiological perspective, value-free data cannot be obtained since perceptions of humans are an integral part of interpretivist research. Instead, value-bound is adopted by interpretivist researchers. As such, interpretivism leans towards the collection of qualitative data through the method of interviews.

The aim of interpretivist research is to understand interpretations of social worlds and context, and discover how people construct meaning in social worlds (Saunders et al., 2016; Neuman, 2011; Crotty, 1998). In terms of epistemology, interpretivism focuses on meaningful social actions that attach subjective meanings, such as narratives, stories, perceptions, and interpretations. However, as a result of the complexity of social worlds, different people who have different backgrounds, under different circumstances create different perceptions and meanings. And this drives interpretivist researchers to discover universal ‘laws’ that are applicable for all specific social entities. From this view, interpretivism is the same as positivism except that they adopt different approaches.

In this research, quantitative data was collected through a highly structured questionnaire. However, the data collected was not subjective meanings, such as narratives, stories, perceptions, and interpretations. For this reason, interpretivism was not considered for this research.

Postmodernism refers to a philosophical stance that is a rejection of modernism. Modernism refers to basic assumptions, beliefs, and values that arose in the enlightenment movements (Saunders et al., 2016; Neuman, 2011; Crotty, 1998). Postmodernists go even further than researchers who are supporting interpretivism or critical realism. They reject objectivism and question the power of relations that sustain realities. Instead, they embrace the role of language and power relations. Postmodernists support the assumption that the nature of social reality is chaotic and fluid without real patterns. Furthermore, extreme postmodernism even rejects the possibility of a science in the social world and distrusts all systematic empirical observations and measurements. From this view postmodernist researchers would undertake their research in a detached and neutral way.

In terms of academic research, postmodernist researchers tend to deconstruct realities, such as texts, to expose how values and interests are embedded within them. They would not focus on the meaning that the texts are describing. Rather, they emphasise how the social world is represented. Questioning and investigation processes are important for postmodernist research. For instance, postmodernist researchers would not focus on social entities, such as ‘management’, ‘organisation’ and ‘performance’. Instead, they emphasise ongoing processes, such as managing, organising and performing (Saunders et al., 2016).

The output of postmodernist research is similar to a work of art, which is used to stimulate others, and ‘to give pleasure’ (Neuman, 2011). Hence postmodern analysis often focuses on areas in advertising, lifestyle, fashion and arts (Gray, 2009). While subjective methodologies are adopted for this research, rejecting or questioning truth or reality is unnecessary for this research. For this reason, postmodernism philosophy was not considered in this research.

3.2 Inductive Research Approach

Both Saunders et al. (2016) and Gray (2009) have outlined the two main scientific approaches: inductive approach and deductive approach. Inductive approach starts from data collection. The collected data, usually qualitative data, are subject to analysis for exploring a phenomenon and developing a theory. The aim of inductive approach is to generate themes, patterns or conclusions from the specific to create a conceptual framework. In an inductive approach, known premises are used to generate untested conclusions. By contrast, deductive approach moves towards hypothesis testing. In a deductive approach, data collection, usually collecting quantitative data, is used to evaluate propositions or hypotheses related to an existing theory. Generally speaking, inductive approach is from data to theory; deductive approach is from theory to data. Figure 3. 3 illustrates the two research approaches. Table 3. 3 compares the two approaches from three perspectives.

Table 3. 3 Comparison of Inductive and deductive approach

	Inductive	**Deductive**
Generalisability	From the specific to the general	From the general to the specific
Usage of data	Data collection is used to explore a phenomenon and develop a theory	Data collection is used to evaluate propositions or hypotheses related to an existing theory
Aim	To generate themes, patterns or conclusions	To test a theory

In this research, **inductive approach** was adopted. The primary purpose of this research was to examine factors influencing the adoption of ISMS standards and frameworks. The first task after data collection was to make sense of the collected data through the data analysis process. The result of the data analysis process would be the formulation of a theory. This theory expressed as a conceptual framework would identify the factors influencing the adoption of ISMS standards and frameworks.

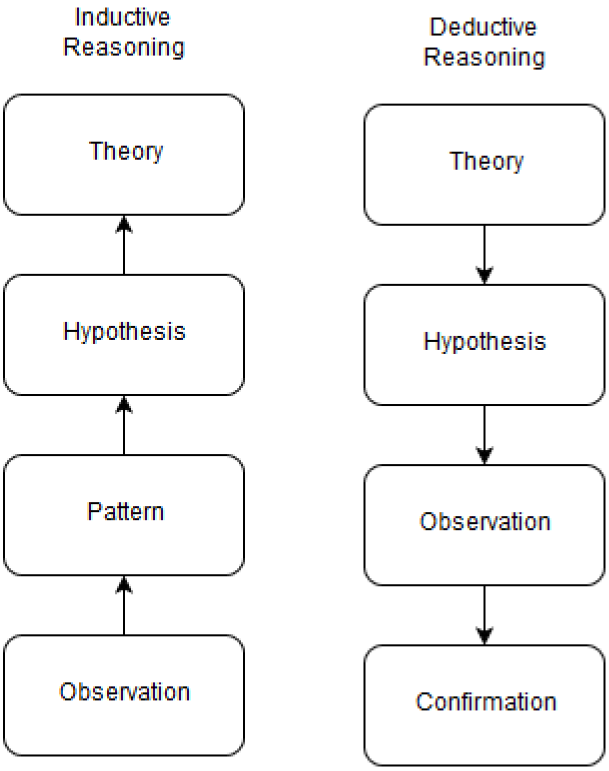


Figure 3. 3 Inductive and deductive approach

3.3 Research Design

This research follows quantitative method research design and is carried out through a combination of exploratory and explanatory study. Online survey is selected as the research strategy to collect quantitative data in order to develop a conceptual framework to answer the research question. There are two main stages in this study: theoretical review stage and confirmatory stage. Figure 3. 4 illustrates the research process.

The reason for employing theoretical review in this research is that the factors influencing the adoption of ISMS standards and frameworks are unknown. It is noted that there is a gap in the existing literature in relation to identifying the factors influencing the adoption of ISMS standards and frameworks. However, existing literature has analysed factors influencing information security management. While this is helpful to answer the research question, a confirmatory stage is still necessary to confirm the accuracy of the assumptions. In the first stage, a richer understanding of factors influencing information security management is obtained. This is achieved by reviewing existing literature on information security management. Three main factors are identified in this stage, which will potentially affect information security management within organisations. And they are senior management commitment, external influences, and human factors.

The confirmatory stage including data collection and data analysis (Chapter 4 – Findings and Analysis) was established after the theoretical review stage with the purpose to validate the assumptions generated in the first stage. In the data collection process, an online survey was selected to collect primary quantitative data. The design for this structured online survey evolved from the literature review in the first stage. The survey comprised 23 questions and would take participants 10 – 15 minutes to complete. The prospective participants were information security or ICT professionals. A LinkedIn profile was created for advertising this research and showing the lead researcher's academic background. A list of prospective participants was generated through LinkedIn, which included 100 prospective participants who have information security or ICT background. Probe messages stating research purposes followed up with a link to the online survey questionnaire were sent to all of the prospective participants on the list. The response rate in this research was restricted to the following two facts:

- The research is related to a critical domain of information security. Participants do not want to discuss any sensitive topics.
- Participants are not willing to accept online surveys through LinkedIn from a person they don't know.

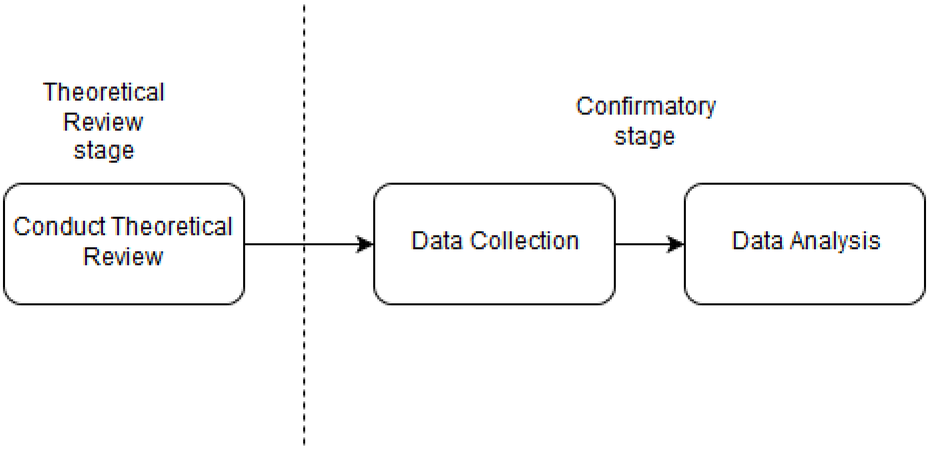


Figure 3. 4 Main stages of the research

3.4 Quantitative Research Method

Research methodical choices can be broadly divided into three categories: quantitative method, qualitative method, and mixed methods (Saunders et al., 2016; Neuman, 2011; Gray, 2009). **Quantitative research** is empirical research followed with structured data collection where data is in the form of numbers. It is generally associated with positivism philosophy and followed with a deductive research approach that is aimed at testing a theory or hypothesis. **Qualitative research** is empirical research where data is not in the form of numbers. Rather, data collected in qualitative research are open to many types of data, such as interview transcripts, diary entries, observation notes, videos and photographs. Qualitative research is usually associated with interpretive philosophy and followed with an inductive research to develop a theory. Qualitative research is aimed at making sense of subjective meanings expressed about a phenomenon. It also focuses on understanding the ways in which people act and account for their actions. **Mixed methods research** is empirical research and usually associated with multiple methods that combine quantitative and qualitative data collection methods. Mixed methods research adopts an inductive, deductive or abductive approach.

This research focuses on explaining a phenomenon or fact that the adoption of ISMS standards and frameworks is low and exploring the factors influencing the adoption of ISMS standards and frameworks. Quantitative method was chosen for this research followed with a highly structured data collection strategy to answer the research questions. **Mono method quantitative study** was adopted in this research, which means that a single data collection technique was used. In this research quantitative data was collected through an online survey. The purpose of this research was to generate a theory from the collected quantitative data followed with an inductive approach. This quantitative research focused on collecting participants' perceptions represented in the online survey to answer the research question. The results of this research develop a conceptual framework to explore and examine the factors influencing the adoption of ISMS standards and frameworks. It also contributes to the existing literature on information security management.

It should be noted that inductive approaches are generally associated with qualitative methods, whilst deductive approaches are commonly associated with quantitative methods. This research used an inductive approach, but it followed a quantitative method through a structured online survey. For the majority questions, an 'Other' option followed by an open text box is provided for each question, when the provided options do not include participants' ideal choices. As such, qualitative data was enabled during data collection. The combination of quantitative and qualitative data collection generates the research theory.

3.5 Research Purpose

Saunders et al. (2016) suggest that research is usually designed to fulfil either an exploratory, descriptive, explanatory, evaluative purpose or some combination thereof. This research was designed to fulfil a combination of exploratory and explanatory purpose. An exploratory study asks open questions beginning with ‘what’ or ‘how’ to discover what is happening and investigate the reason why. An explanatory study is for seeking answers to a phenomenon or problem. It asks open questions beginning with ‘why’ or ‘how’.

A combination of **exploratory study** and **explanatory study** was adopted for this research. The primary purpose of this study was to explore and examine factors influencing the adoption of ISMS standards and frameworks. This research also identifies challenges and barriers to adopting ISMS standards and frameworks within organisations.

In order to obtain the foundation of the exploratory and explanatory study, a theoretical review was conducted. Not only did the comprehensive theoretical review provide an up-to-date understanding of information security management and factors influencing information security management but also it guided the development of research topics and questions. Through demonstrating essential theories and understandings in the field of information security, the theoretical review presents the gap between existing literature and the research topic. Databases used for searching literature include Stella Search (Trinity College Library), ACM Digital Library, IEEE Xplore Digital Library and Google Scholar. Literature materials include academic papers, government publications, journal articles, books, and conference papers. All literature materials were evaluated to ensure the knowledge obtained is up-to-date and trustworthy.

3.6 Research Strategy

An online survey was selected for the main research strategy. It is a common and popular strategy in business and management research. Most researchers are likely to use the survey strategy for exploratory research (Saunders et al., 2016). It provides an efficient and cost effective way of generating a large number of responses in a short period of time. Primary data was collected through the online survey to answer the research question, identify relationships between variables, and develop a conceptual framework for this research.

The online survey was designed based on the knowledge obtained through the theoretical review process (Chapter 2 – Literature Review). It comprises 23 questions and 6 topics including company profile; interviewee profile; information security environment; challenges and barriers; benefits; plans for the future. The online survey took participants 10 – 15 minutes to complete. Each question was optional. Participants were able to quit the online survey without submitting answers at any time without penalty. This online survey was anonymised. No individual and organisation names were required. All participants were advised not to input personal details or organisation names on the online survey.

The online survey tool chosen for this research was SurveyMonkey®. Reasons for choosing SurveyMonkey® are

- It includes over 100 templates and 1,600 pre-made questions
- It has user-friendly interface
- It creates reports in PDF
- It provides data analysis function

After the creation of the online survey, 5 information experts were invited for pilot testing. The aim of pilot testing was to refine the questionnaire to ensure participants have no problems in answering those questions. Suggestions and opinions were collected. Necessary amendments were made to the online survey. All information collected through the online survey was treated confidentially. Online survey data was stored and encrypted on the server managed by SurveyMonkey®. Sufficient data protection controls were deployed within SurveyMonkey® to protect data stored and processed on SurveyMonkey® products. SurveyMonkey® (2016) has an appropriate privacy policy in place, which explains how SurveyMonkey® handles data protection issues. Additionally, a strong password was deployed on the account with the access to the survey data. This password was subject to periodic change every 60 days. All survey data would be destroyed from both SurveyMonkey® and the lead researcher's laptop after September 30th, 2017.

3.7 Samples

A self-selection sampling technique was chosen for selecting samples in this research. By choosing self-selection sampling rights was given to individuals to identify their desire to take part in the research. As the research explores a phenomenon on information security, the prospective participants have to be information security or ICT professionals. A LinkedIn profile was created advertising this research and showing the lead researcher's academic background. A list of prospective participants was generated through LinkedIn, including 100 prospective participants who have information security or ICT background. Probe messages introducing research purposes followed up with the online survey link were sent to all of the prospective participants on the list through LinkedIn.

3.8 Time Horizon

The research started in January 2017 and ended in August 2017. Considering the timeframe of this research, cross-sectional study was adopted, which only involves the phenomenon at a particular time. This research at a ‘snapshot’ of the time horizon provides knowledge and perceptions during the research time.

3.9 Ethics of the research

Human participation was involved in this research for collecting research data. Ethical issues were considered at each stage of this research, especially at the stage of data collection, to ensure that all prospective participants were fully informed about this research and its implications for them as participants. A research ethics application (Appendix A: Ethics Approval) was submitted to the Research Ethics Committee in the School of Computer Science and Statistics of Trinity College Dublin on April 24th, 2017. Approval was received on May 2nd, 2017 before the survey was distributed to participants.

In order to ensure all prospective participants were informed about this research, a Participant Information Form (Appendix B: Information Sheet for Participants) and an Informed Consent Form (Appendix C: Informed Consent Form) were sent to all prospective participants along with a link to the online survey. Background and procedures of this research were addressed in both of the two forms. Key elements, such as conflict of interest, publication and declaration were clearly defined in the consent form.

Participants cannot proceed to the online survey until they have read and accepted all the terms and conditions in the consent form.

3.10 Limitations

While online surveys saved effort for the lead researcher to distribute questionnaires and collect responses, it has limitations. Firstly, as this research is related to information security management, which is usually regarded as confidential information within organisations, some participants did not want to provide any information about this topic. And this resulted in negative responses. Secondly, some participants did not have sufficient information security or ICT management knowledge, which resulted in inaccurate answers. Thirdly, open questions were not added to the questionnaire, which resulted in missing critical perceptions of participants. Fourthly, this questionnaire was highly structured and some of expected answers might not be included in the structured questionnaire. And this might result in that the provided options did not represent participants’ perception accurately.

Lastly, the sample size was too small, which might not represent the whole population.

3.11 Lessons Learned

LinkedIn was the tool used for distributing the online survey. However, based on the fact that most people on LinkedIn do not want to respond any messages from people they do not know, the response rate was very low. From this view, LinkedIn is not an effective way to distribute the survey.

The online survey was distributed in May. Many prospective participants were busy and had no time to complete the online survey. It was noted that only a few of participants completed the questionnaire in full without skipping any questions.

After the completion of the survey design, five information security experts were chosen for pilot testing to ensure participants have no problems in understanding and answering the questions. High-quality recommendations were collected during the pilot testing. The survey was revised and retested afterwards. The pilot testing provided the lead researcher with ideas, approaches, and clues that have not foreseen before conducting the pilot testing.

3.12 Summary

Three key philosophical assumptions, two opposing philosophical extremes, and five main research philosophies are discussed at the beginning of this chapter. Rationales for selecting appropriate research philosophies are provided. This research adopted an inductive research approach to build a theory answering the question what factors are affecting the adoption of ISMS standards or frameworks.

This research followed quantitative method research design and was conducted through exploratory and explanatory study. An online survey was selected as the research strategy to collect primary data in order to develop a conceptual framework and make a theoretical contribution. There were two main stages in this study: theoretical review stage and confirmatory stage. A literature review was carried out in the first stage to provide a theoretical foundation of this research and present an up-to-date knowledge of the research topic. Quantitative data was collected in the second stage through a highly structured online survey.

The main limitation of the research was the small sample size, which might affect the accuracy of the data analysis results.

Chapter 4 – Findings and Analysis

4.1 Introduction

This chapter comprises data analysis and an interpretation of the findings resulting from the primary data collected from an online survey. The results of data analysis illustrate how the proposed research questions were answered. Firstly, the research strategy will be presented in order to outline the research design. Following an overview of the number of responses and the means of data analysis, the results from both quantitative and qualitative data analysis will be discussed. Lastly, key findings will be summarised.

The primary objective of this research is to examine factors influencing the adoption of ISMS standards or frameworks. As outlined in the literature review, information security management within organisations tends to be affected by senior management commitment, external influences, and human factors. Since there is a gap in existing literature knowledge, quantitative research was designed to answer the following research questions:

1. What are the challenges and barriers to adopting ISMS standards or frameworks?
2. What are the concerns of senior management when adopting ISMS standards or frameworks?

4.2 Research Strategy

As outlined in the previous chapter, quantitative research was used in this study in the form of an online survey. Considering that online surveys are one of the most efficient and cost effective strategies to gather a large number of responses in a short period of time, it was selected as the only data collection technique for this research.

An online survey was designed based on knowledge obtained through the literature review. It comprised 23 questions and 6 topics, including organisation profile, participant profile, information security environment, challenges and barriers, benefits, and plans for the future (Appendix D: Online Survey Questions). The online survey took participants around 10-15 minutes to complete. Each question was optional. Participants were able to quit the online survey without submitting answers at any time without penalty. This online survey was anonymised. No individual or organisation names were required. All participants were advised to avoid inputting any identifiable personal or organisational information during the online survey.

Whilst a quantitative research method was chosen, some qualitative data was also collected. An ‘Other’ option followed by an open text box was provided for most survey questions to ensure that participants could input accurate answers when provided options did not include or represent their ideal response. Because the size of qualitative data collected from the online survey was minimal and did not increase the complexity of data analysis, qualitative data analysis methods were not considered in this research.

A self-selection sampling technique was chosen for this research. Rights were given to individuals to identify their desire to take part in the research. As the research explores a phenomenon on information security, the prospective participants were required to be information security or ICT professionals. A LinkedIn profile was created to advertise this research and included the lead researcher's academic background. A list of prospective participants was generated through LinkedIn, including 100 individuals with information security or ICT backgrounds. Probe messages introducing the research purposes followed up with an online survey link were sent to all prospective participants on the list via LinkedIn.

However, after the first two weeks of data collection, response rates were extremely low—only 11 responses were collected during the first two weeks. As a result, other methods to increase the awareness of this research were taken into consideration rather than sending the same online survey to 100 prospective participants. In order to obtain more responses, the lead researcher became a member of information security or ISMS standards and frameworks related groups on LinkedIn and posted a research introduction followed by a survey link. Table 4.1 lists all the LinkedIn groups where the lead researcher advertised this research.

Table 4.1 Information Security Groups on LinkedIn

Group Name	Group Description	Members	Joined Date
Information Security Community	This Information Security Community on LinkedIn is the largest community of cyber security professionals in the industry. The main objective is to build a network that connects people, opportunities, and ideas. This group is created for people who are involved in purchasing, selling, designing, developing, and using information security solutions. Covered topics include compliance, encryption, anti-virus, malware, cloud security, data protection, hacking, network security, virtualisation, and more.	375,135	15/05/2017

Information Security Careers Network	The largest group on LinkedIn dedicated to careers in IT and Information Security. This group provides a way of connecting InfoSec professionals to each other and to recruiters in order to help them find their next career move. Topics covered include (but aren’t limited to) PCI DSS, ISO 27001, CISA, CISM, Intrusion Detection and Prevention, Identity and Access Management, Network Security, ITIL, and more.	57,725	20/05/2017
ISO 27001: Information Security Management Systems – Implementation and Audit	This group connects information security professionals, standard bodies, managers, consultants, auditors, analyst, students, and all those who are interested, and wish to discuss information security management systems, practices, experiences, and knowledge. Related topics include data security, ISMS, information security threats, legal compliance, cloud security, network security, information security awareness, education, and training.	3,981	20/05/2017
Information Technology Audit and Governance Group	This LinkedIn group focuses on all things related to IT audits, compliance, quality assurance, business continuity, disaster recovery, IT governance, fraud, risk, and forensics. This group maintains information, discussions, and resources for information technology auditors, internal auditors, application auditors, compliance, information security and forensics professionals.	68,008	01/06/2017

Apart from resources on LinkedIn, the online survey was distributed through information security related forums, such as the forum managed by Information Systems Audit and Control Association (ISACA). Focusing on IT governance, ISACA is an independent, nonprofit, global association engaging in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems.

Table *4.2* lists all the ISACA communities in which the lead researcher advertised this research.

Table 4.2 Information Security communities on ISACA

Community Name	Description	Members	Joined Date
Information Security Management	This ISACA community focuses on cloud computing, application security, vulnerability management, PCI DSS, and data protection.	1,375	20/05/2017
PCI DSS	This ISACA community focuses on PCI DSS, Europay, MasterCard and Visa (EMV), PCI Cloud, and other payment card areas.	1,242	25/05/2017
ISO/IEC 27000 Series	This ISACA community focuses on Information Security Risk Assessment, ISO/IEC 27000 guidance implementation, continuous improvement and feedback activities, guidance on Information Security topics and addressing changes utilising such guidance.	1,188	25/05/2017
COBIT - Implementation	This ISACA community focuses on COBIT implementation guidance.	1,614	02/06/2017
Security Trends	This ISACA community focuses on top security trends and issues.	667	02/06/2017
Strategic Planning/Alignment	This ISACA community focuses on ISMS planning/alignment.	763	03/06/2017

4.3 Data Analysis

As outlined in the previous chapter, quantitative analysis of a structured online survey was required in this research. The online survey tool, SurveyMonkey®, was used to collect data, which was then exported to Excel (XLS) and comma-separated values (CSV) files for further analysis. The two types of data files provided the potential for statistical, mathematical, or computational analysis. In general, quantitative data can be divided into two groups: categorical and numerical. In this research, only categorical data was collected, so that it could not be measured or calculated numerically, but can be either classified into sets or categories according to their characteristics or placed in rank order. In order to increase the probability of exploring correlations between two variables, coding of categorical data was required. According to the complex data in this research, the quantitative analysis process was divided into four stages.

Stage 1: Data formatting

Collected data was exported to XLS and CSV files from SurveyMonkey® for further analysis. Two types of XLS files were generated. One included presentation-ready survey results for each question with response counts, response percentages, and charts. Each question occupied one spreadsheet. The other presented all responses data in one spreadsheet and provided a summary of raw data collected from the survey. Each question comprised one column and each response occupied one row. The latter was used for further statistical analysis. Both types of files included open-ended answers.

Stage 2: Data cleaning

According to the American Association for Public Opinion Research (2016), four levels of non-response can be reported:

- Complete refusal: no questions answered;
- Break-off: less than 50 per cent of all questions answered other than by a refusal or no answer (this, therefore, includes complete refusal);
- Partial response: 50 per cent to 80 per cent of all questions answered other than by a refusal or no answer;
- Complete response: over 80 per cent of all questions answered other than by a refusal or no answer.

In this stage, complete refusal responses were discarded. The remaining non-response and full responses were retained for further analysis. It should be noted that the following two scenarios were regarded as complete refusal responses:

- Agreed to the Informed Consent Form (who answered Yes to the first question), but no questions answered after;
- Disagreed to the Informed Consent Form (who answered No to the first question).

Stage 3: Coding

The online survey resulted in categorical data, which cannot be measured or calculated numerically. In order to increase the likelihood of further statistical analysis, categorical data was coded using numerical codes. A set of rules was designed for coding.

The first position of the code represents how many options were selected followed by the number representing the selected option (A=1, B=2, C=3, D=4, etc.). For example, the code of ‘14’ means only 1 option was selected and this option is D; the code of ‘3123’ means 3 options were selected and they were A, B and C; the code of ‘110’ means 1 option was selected and this option was J. A skipped question was represented by 0.

Stage 4: Exploring findings

Whilst SurveyMonkey® provided data analysis for each question and the results clearly portrayed response counts, response percentages, and charts, further data analysis for identifying any possible correlations between questions was required. Two sub-processes were designed to obtain correlations between questions – one was via an Excel Pivot table; the other was via pre-designed and tested Python scripts.

It should be noted that only two variables with a likely correlation were subject to any of the two sub-processes to examine causation. When there was no logical reasoning between two independent variables/questions, no causation is implied even though statistical results show a potential correlation. Indeed, one important principle of statistical analysis is that correlation does not necessarily imply causation.

4.4 Analysis Results

An online survey was created on 27/04//2017, opened on 08/05/2017, and closed on 26/06/2017. Ninety-two responses were obtained during this period of time. As required by the Ethics Committee of Trinity College participants had to read and agree to an Informed Consent Form prior to the commencement of participation. As a result, two responses were disqualified. Table 4. 3 shows an overview of collected responses.

Table 4. 3 Overview of responses

Responses received	92
Valid responses	90
Completed responses	71

Partial responses	19
Disqualification responses/ Complete Refusal	2

Within 19 partial responses, 7 responses accepted the Informed Consent Form (by answering ‘Yes’ to the first question) but did not answer any questions after the first question. As such the 7 responses were discarded and were not subject to further data analysis. This resulted that 9 responses in total were deleted including 7 responses above and 2 disqualification responses (disagreed to the Informed Consent Form).

It should be noted that the last question asked participants if they want to submit their answers. If participants answered ‘No’, their answers would not be submitted. And such answers, therefore, were not shown in the data analysis process.

The survey consisted of 23 questions (2 of them are not shown below: 1 for Informed Consent Form and 1 for submitting answers) and was divided into six sections:

- Section 1 – Organisation profile (3 questions)
- Section 2 – Participant profile (2 questions)
- Section 3 – Information security environment (7 questions)
- Section 4 – Challenges and barriers (4 questions)
- Section 5 – Benefits (3 questions)
- Section 6 – Plans for the future (2 questions)

Survey findings of the individual analysis and cross tables are detailed in the subsequent sections.

Section 1 – Organisation Profile

The first section was to analyse information gathered about the background of respondents’ organisation. The purpose of this section was to build organisation profiles. Participants were asked demographic questions and three key factors were collected in this section: business sector (Question 2), the number of full-time employees (Question 3), and key stakeholders making ICT decisions (Question 4).

Figure 4. 1 shows participants’ business sector. 80 participants (89%) answered Question 2. Of that 63% were from the following five business sectors – information technology (19%), government (15%), financial services (11%), banking (10%), and education (8%). Within ‘Other’ sector 11 respondents were from agriculture, charity, digital marketing, food processing, gambling, healthcare/hospitals, mass media, manufacturing, professional services, real estate and utility.

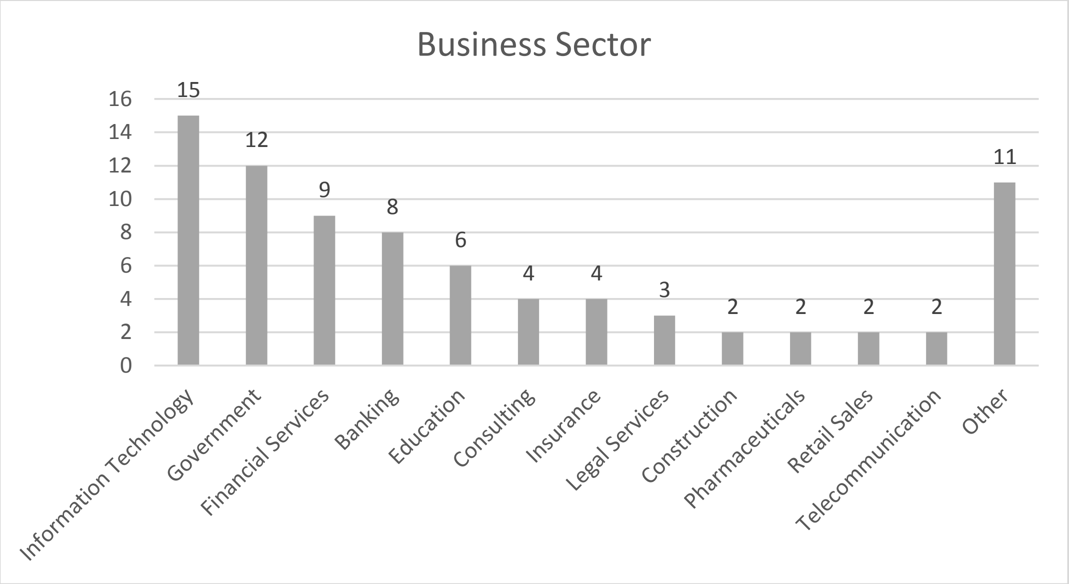


Figure 4. 1 Business Sector

In Question 3 participants were asked to indicate how many full-time employees in their companies. 82 participants answered this question. Results show that most participants (43.9%) were from big companies with more than 2,000 full-time employees. 16 participants (19.5%) were from small companies with less than 100 full-time employees. Only 4 participants (4.9%) indicated that they were from companies with more than 500 but less than 1,000 full-time employees. 13 participants (15.9%) were from companies with 101 – 500 full-time employees. And the same number of participants were from companies with 1001 – 2000 full-time employees. Figure 4. 2 indicates that most participants were from big companies with more than 2,000 full-time employees while companies with more than 500 and less than 1,000 full-time employees had the lowest response rate.

Considering that more than 80% of respondents were from companies with more than 100 full-time employees findings identified in the following questions were more accurate to medium or large companies compared with small companies with less than 100 full-time employees.

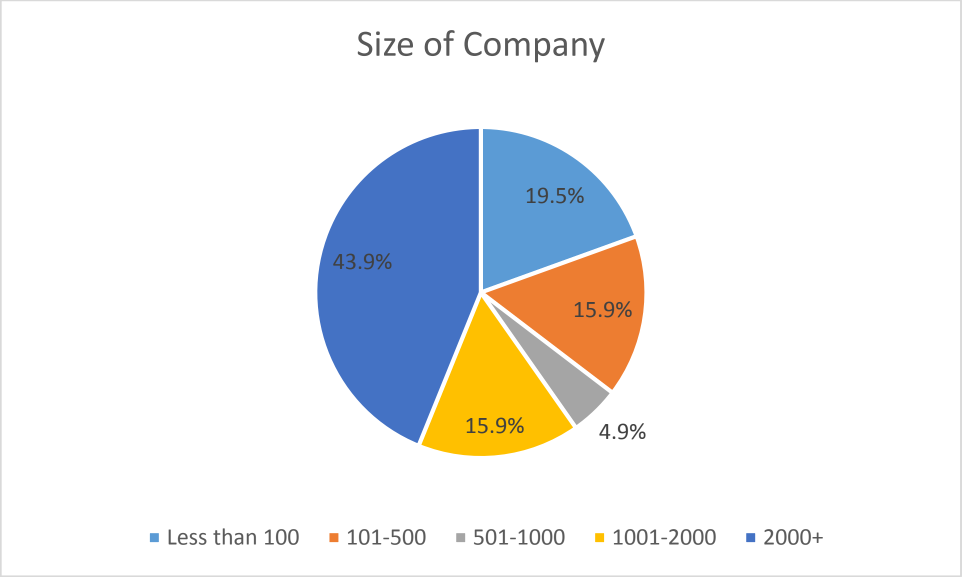


Figure 4. 2 Company Size

As outlined in the literature review, technology alone does not guarantee the success of information security management. As an increasingly important factor for companies in achieving business goals, information security should be considered and managed from a managerial perspective. Consequently, it is imperative that senior executives take the responsibility of making key ICT decisions and protecting the 'lifeblood' of business. Many researchers (McFadzean et al., 2006; Soomro et al., 2015; Ghonaimy et al., 2002) argue that information security should remain within the sight of senior directors because of their leaderships, governance responsibilities, visions and plans.

However, there are many organisations still recognise information security as a solely technical problem within IT department. Within these organisations, information security is haphazardly delegated (McFadzean et al., 2006). Therefore it is necessary to know if senior management commitment will contribute well-organised information security management to their organisations. Senior management commitment can be identified by asking the question who are the key stakeholders for making ICT decisions within companies (Question 4).

83 participants answered Question 4 and 48 of them (57.8 %) indicated that CIO or CTO (globally or locally) was the key stakeholder for making ICT decisions in their companies. 16 respondents (19.3%) informed that ICT Director took the responsibility for making ICT decisions. Only 13 respondents (15.7%) chose ICT manager. Results also noted that more than 70% of participants were working in the companies with senior executives making ICT decisions. Figure 4. 3 shows the results of Question 4.

There were only 6 respondents (7.2%) chose ‘Other’. Their answers included Executive management team, IS officer, Head of Information Security, project leader, Director of Finance, and ICT Assistant. Within the 6 positions, three of them were dedicated IT positions.

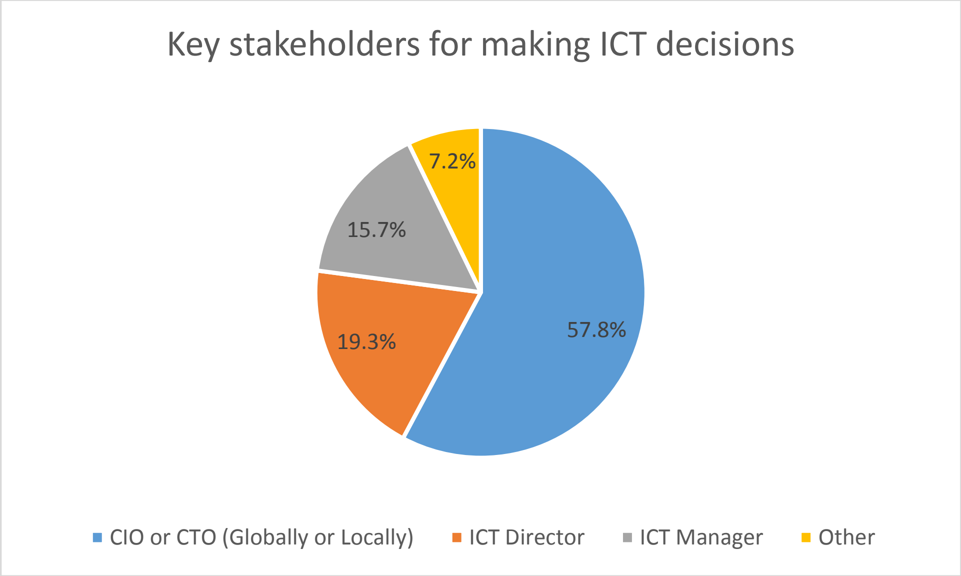


Figure 4. 3 Key Stakeholders for making ICT decisions

Section 2 Participant Profile

The purpose of the second section of the questionnaire was to build participant profiles by asking demographic questions related to their job titles (Question 5) and the number of years of experience in ICT management (Question 6). As this research was related to information security management participants selection was only focused on IT related professionals. Two methods were used for advertising and distributing the online survey – one was through LinkedIn messages, and the other one was through information security forums.

However, neither of the two methods was able to ensure that only IT related professionals were chosen to take part in the online survey. If most participants were non-IT related professionals, the results of the research would be inaccurate resulted by a large number of unqualified answers. Therefore it was necessary to identify demographic factors.

Question 5 asked participants their job titles. 79 responses were collected. 63 of them (79.7%) were IT related professionals. 7 of them were compliance managers who were aware of information security within their organisations. 16 of them (20.3%) chose the ‘Other’ option, which included IT Analyst, Compliance Director, System Administrator, Data Consultant, IS Officer, Stage 2 Compliance Analyst, Financial Controller, Project Leader, Head of Quality and Team Lead. It was noted that the majority of participants (79.7%) were IT related professionals. Table 4. 4 shows the results of Question 5.

Table 4. 4 Participant Position

Job Title	No. of responses
CIO or CTO (Globally or Locally)	3
ICT Director	12
ICT Manager	16
IT Consultant	17
Compliance Manager	7
IT Auditor	9
Other	16

Question 6 asked participants about their experience of ICT management. 79 participants answered this question. Whilst only 16 of them (20.3%) indicated that they had less than 5 years ICT management experience, more than half of them (55.7%) had more than 10 years of ICT management experience. Figure 4. 4 shows the results of Question 6.

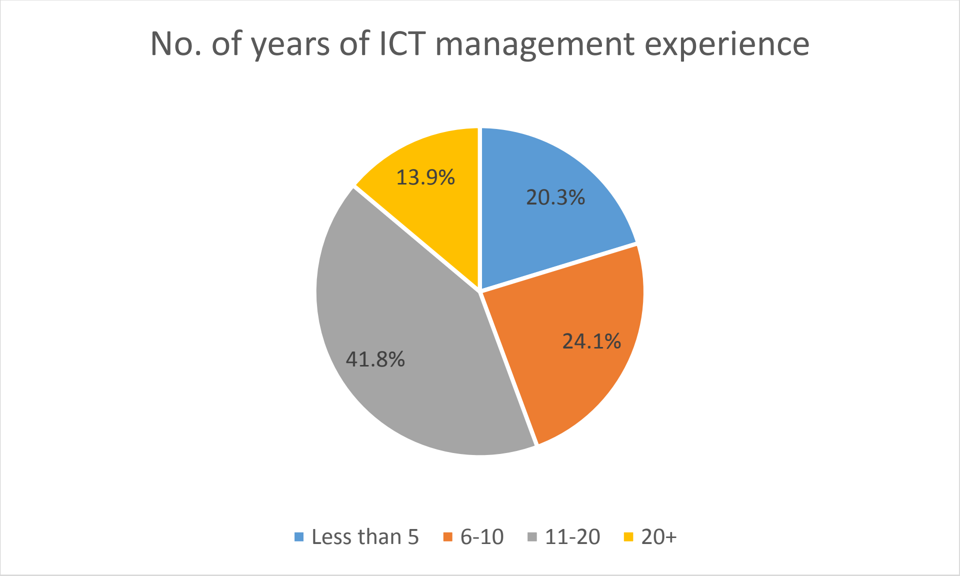


Figure 4. 4 No. of years of ICT management experience

Section 3 Information Security Environment

The third section was to analyse information gathered about information security management within participants’ companies. The purpose of this section was to identify and summarise the ways how ISMS was managed in participants’ companies. 7 questions were asked in this section, including questions about ISMS establishment (Question 7), who manages ISMS (Question 8), adopted ISMS standards and frameworks (Question 9 and 10), average cost (Question 11), main driver of the adoption (Question 12), and external help (Question 13).

ISMS Establishment

It should be noted that except direct data analysis for each question additional data analysis between questions was carried out in order to obtain more useful information from collected responses. All the data analysis details and findings were presented.

Question 7 asked participants if their companies had implemented a formalised ISMS. Within 80 respondents 58 of them (72.5%) indicated that ISMS had been implemented. And 22 of them (27.5%) answered 'No'. As all the following questions were related to ISMS, participants who answered 'No' were led to the final submission page of the questionnaire.

In order to identify the popularity of ISMS in different industries, Question 7 results were analysed in business sectors (Question 2). Through tracking Question 2 answers against Question 7 correlations were identified. As shown in Figure 4. 5 most companies in information technology, financial services, banking, insurance and consulting had formalised ISMS in place. Especially for information technology, financial services, banking and insurance companies, ISMS was implemented and maintained. Restricted by the sample size, a sufficient number of responses were not obtained from some industries, such as construction, legal services, pharmaceuticals, retail sales and telecommunication. This will be improved in the future research when the sample size is increased.

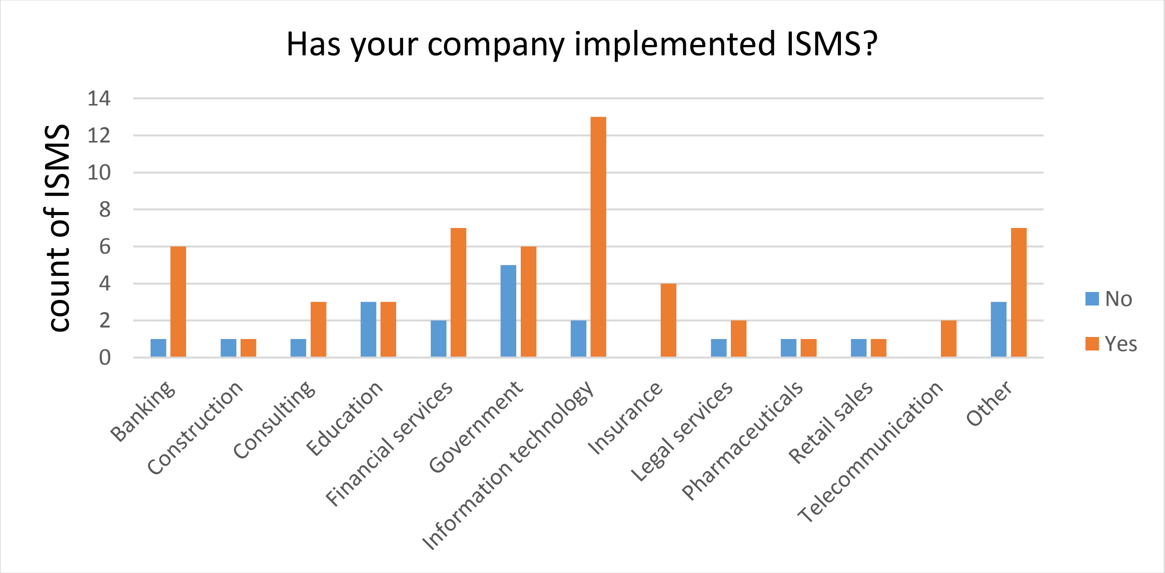


Figure 4. 5 ISMS in business sector

Because of the continued escalation of cyber-attacks and increasingly regulated data protection landscape it is important and necessary for companies, no matter in what business sectors, to establish, implement and maintain an effective ISMS to manage their information assets (IT Governance, 2016). As an increasingly important factor for companies in achieving business goals, information security should be considered and managed from a managerial perspective. Consequently, it is imperative that senior executives take the responsibility of making key ICT decisions and protecting the 'lifeblood' of business. As outlined in the literature review, senior management commitment is one of the key factors affecting information security management because of its leadership, governance responsibilities, visions and plans. Therefore it is necessary to know if senior management commitment will contribute well-organised information security management to companies.

Li et al. (2007) indicated that companies with senior management members who have IT background or IT related knowledge are less likely to have a material weakness in IT internal controls over financial reporting. From this perspective, the lead researcher analysed data gathered from Question 4 (key stakeholders for making ICT decisions) and Question 7 (the existence of formalised ISMS) with the purpose of identifying if there is a relationship between dedicated ICT senior executives and formalised ISMS.

Question 4 answers were tracked and analysed against Question 7. The purpose was to explore if dedicated ICT senior management contributes well – organised ISMS management to companies. Figure 4. 6 shows the results of Question 4 and Question 7. It was noted that most companies with a CIO, CTO or ICT director had implemented a formalised ISMS. Within 80 respondents 49 of them (61.3%) indicated that they had implemented a formalised ISMS. Those respondents also informed that dedicated ICT senior executives (CIO, CTO or ICT director) were the key stakeholders for making ICT decisions in their companies. With regard to companies delegating ICT manager as the key stakeholder for making ICT decisions, only 6 respondents (7.5%) indicated that their companies had implemented formalised ISMS.

The results above confirmed that companies with dedicated ICT senior executives were likely to have formalised ISMS in place. It also corroborated that information security matters should not be haphazardly delegated to IT department. Rather senior management executives should take the responsibility of information security management.

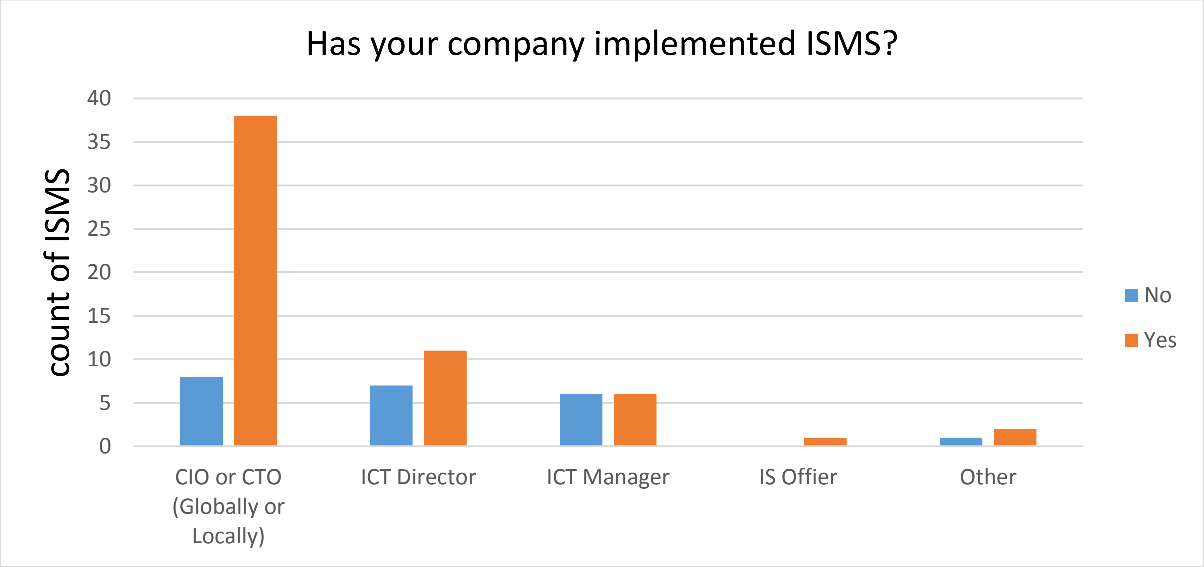


Figure 4. 6 ISMS and senior management

In order to explore the relationship between company size and formalised ISMS within companies, the following data analysis was carried out.

The lead researcher analysed data gathered from Question 3 (company size) and Question 7 (the existence of formalised ISMS) in order to confirm if company size positively correlates with ISMS establishment. Findings noted that except senior executives (CIO, CTO or ICT director), company size had an impact on ISMS establishment, but a fairly minor one. Large companies with more than 500 full-time employees were likely to have formalised ISMS established and maintained (Figure 4. 7). Data analysis results (Table 4. 5) show that within 79 respondents, 42 of them (53.2%) indicated that they had established and maintained formalised ISMS within their companies and they were all from companies with more than 500 employees. With regard to companies with less than 500 full-time employees, only 15 respondents (19.0%) indicated that they had established and maintained formalised ISMS within their companies.

Table 4. 5 ISMS and company size

Company Size	**With ISMS**	**Without ISMS**	**With ISMS / Without ISMS**
Less than 100	8	7	1.14
101 - 500	7	6	1.17
501 - 1000	3	1	3.00
1001 - 2000	9	3	3.00

2000 +	30	5	6.00
Total	57	22	N/A

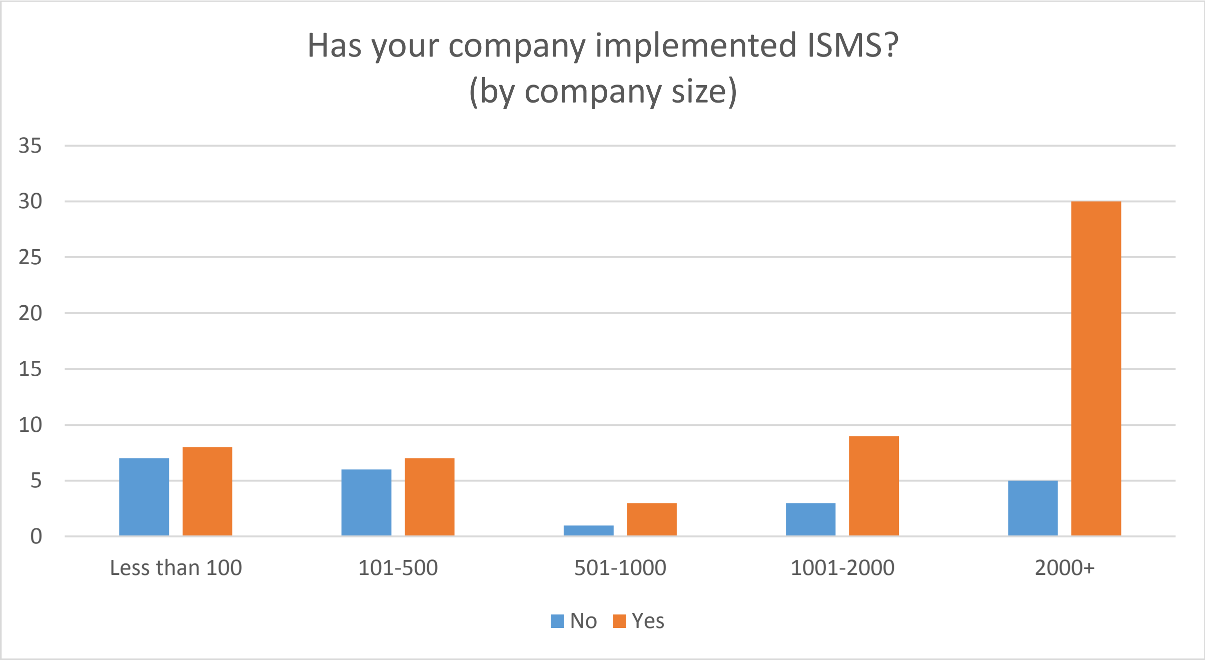


Figure 4. 7 ISMS and company size

ISMS management

Question 8 asked participants who manage implemented ISMS. The purpose of this question was to identify if a dedicated role was in place for managing and maintaining ISMS. Data analysis results show that 57 participants answered this question. 15 of them (26.3%) indicated that ICT directors managed ISMS; 13 of them (22.8%) indicated that ISMS manager managed ISMS; 12 of them (21.1%) indicated that ICT manager managed ISMS.

Figure 4. 8 shows the results of Question 8 indicating that the top three roles for managing and maintaining ISMS were ICT Director, ISMS Manager and ICT Manager. However, most respondents (26.3%) indicated that ICT Director managed ISMS. It should be noted that ICT Director, as one of the senior executives, should not be recognised as a dedicated role for managing and maintaining ISMS. The other two positions, ISMS Manager and ICT Manager, are more appropriate than ICT Director for managing and maintaining ISMS.

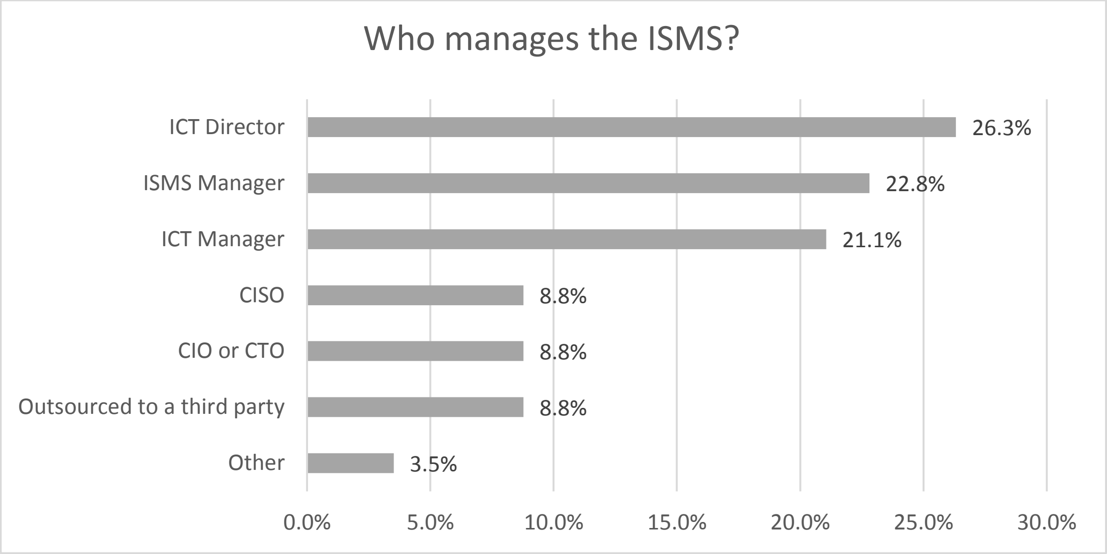


Figure 4. 8 ISMS owner

Adoption status of ISMS standards or frameworks

Question 9 asked participants if their companies had adopted any ISMS standards or frameworks. This question was one of core questions in the questionnaire. It divided participants into two groups. Each group of participants were asked different questions based on different scenarios after this question. The four prospective choices are listed below:

- Yes
- No, but we are in progress
- No, but we might in the near future
- No, and we are not planning to adopt any of ISMS standards or frameworks

56 respondents answered this question. 41 of them (73.2%) indicated that their companies had adopted at least one ISMS standard or framework. Only 2 of them (3.6%) informed that their companies had not adopted any ISMS standards or frameworks and they did not plan to adopt any. Figure 4. 9 shows that majority of respondents indicated that their companies had adopted at least one ISMS standard or framework.

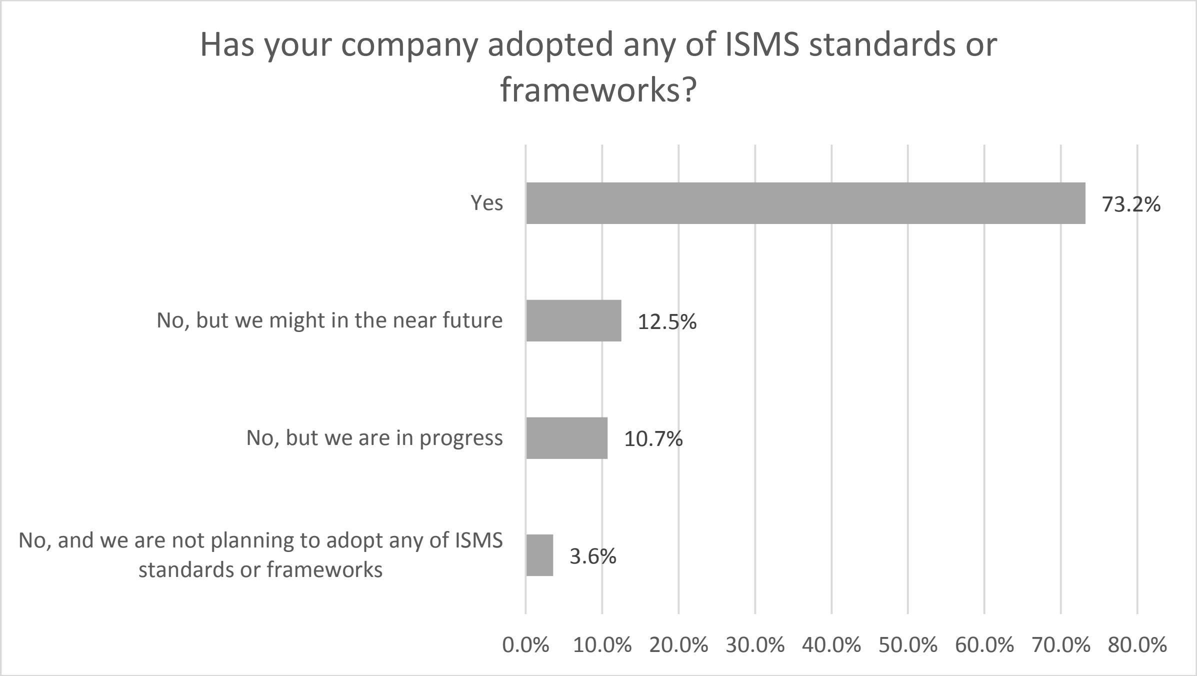


Figure 4. 9 The adoption status of ISMS standards or frameworks

Whilst an overview of the adoption of ISMS standards or frameworks presented positive results, there were still many companies (26.8%) that had not adopted any ISMS standards or frameworks to protect their information. This might be resulted by the lack of regulatory pressure in some industries. To the contrary, in some particular industries, companies are enforced to adopt some standards or frameworks. And the non-compliance will result in a penalty. For example, PCI DSS is widely accepted and it must be implemented by all companies dealing with cardholders' information. As such, most companies dealing with banking transactions have adopted PCI DSS standard. Another example is the upcoming EU GDPR law. The non-compliance companies will be liable for a fine of up to 4% of annual global turnover. However, in some other industries, there are no such mandatory standards or frameworks to follow. Without regulatory pressure, companies in these industries may not consider adopting any ISMS standards or frameworks.

For this reason, it was necessary to identify the ISMS adoption status in each business sector. Question 9 results were analysed in business sectors (Question 2). Through tracking Question 2 answers against Question 9 answers, correlations were identified. As shown in Figure 4. 10 ISMS standards or frameworks were widely adopted in the following industries – information technology, financial services, banking, insurance and consulting. Especially in banking, all respondents indicated that ISMS standards or frameworks had been adopted. In financial services, only 1 out of 7 respondents (14.3%) indicated that ISMS standards or frameworks had not been fully adopted but it was in progress. Restricted by the sample size, a sufficient number of responses were not obtained from some industries, such as education, telecommunication, legal services, pharmaceuticals, retail sales and construction. This will be improved in the future research when the sample size is increased.

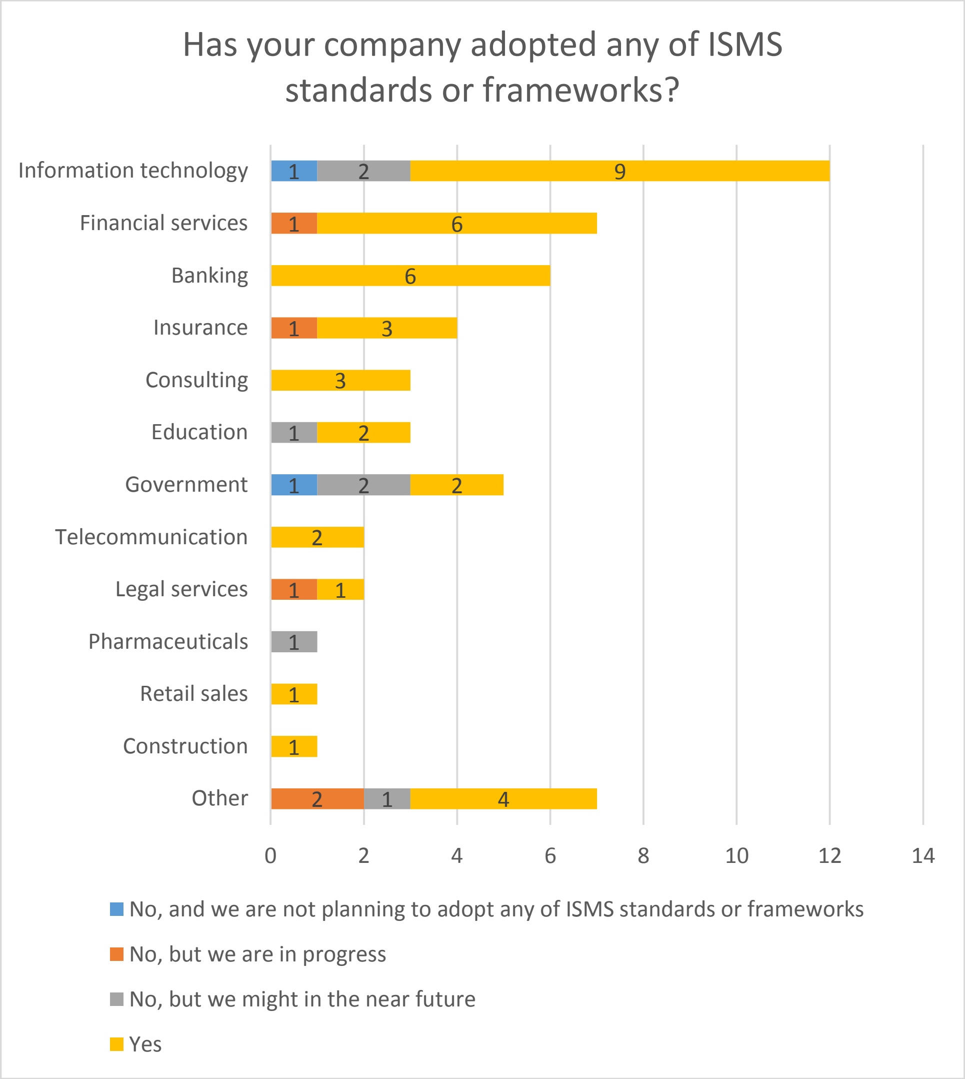


Figure 4. 10 ISMS status in each business sector

Apart from business sectors, the adoption of ISMS standards or frameworks is influenced by company size, structure and complexity as well. This is because securing more people, more information systems, more workstations, more processes, and more techniques will require more enhancement of the design of ISMS (Raggad, 2010). For example, if a company does not have a software development department and there is no need to setup such a department, this company then does not have to create a detailed plan for establishing security controls for software development life cycle or making effort to align with best practice standards or frameworks.

In order to identify ISMS standards or frameworks adoption status in different sizes of business, Question 9 results were analysed in different company sizes (Question 3). Through tracking Question 3 answers against Question 9 answers, correlations were identified. As shown in Figure 4. 11 most big companies (92.9%) with more than 2,000 full-time employees had adopted at least one ISMS standard or framework. Only 7.1% of them indicated that they had not fully adopted any ISMS standards or frameworks, but it was already in progress. With regard to small companies, with less than 100 full-time employees, only 50% of respondents indicated that they had adopted at least one ISMS standard or framework. And there were 12.5% of them indicating that they were not planning to adopt any of ISMS standards or frameworks.

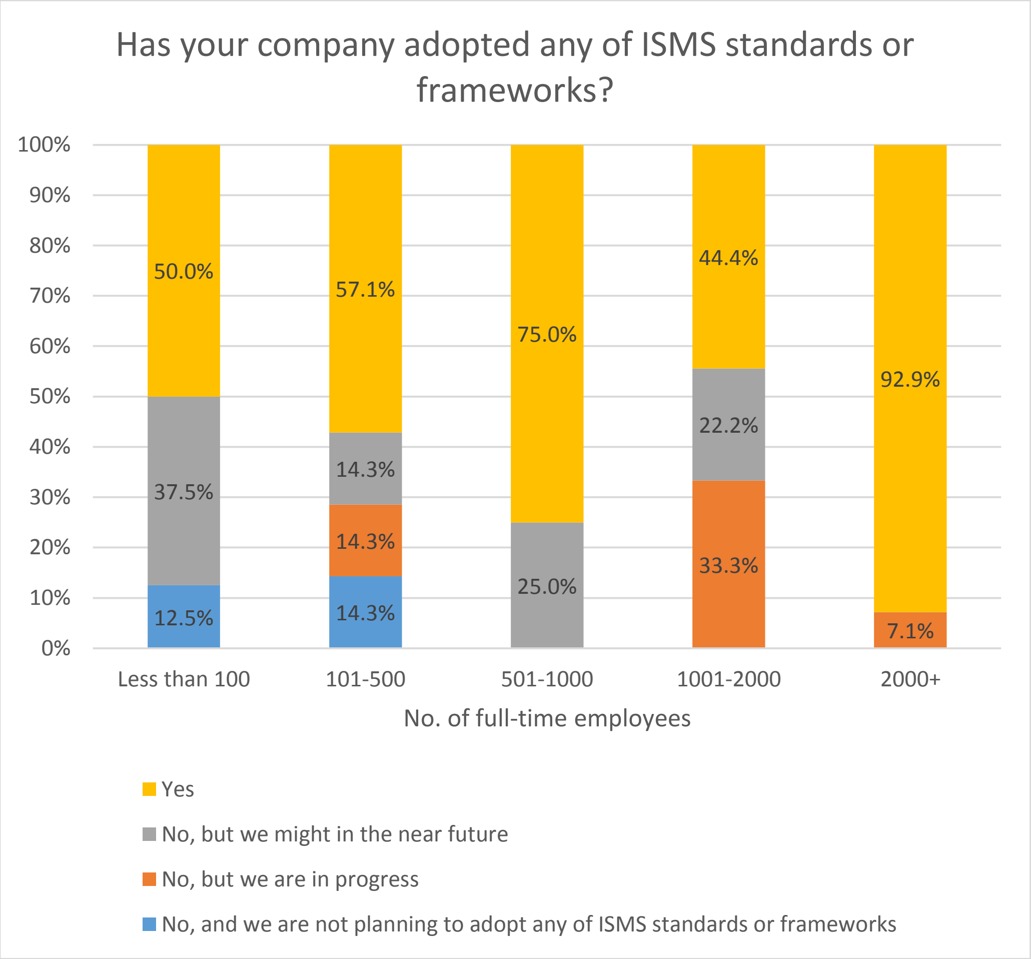


Figure 4. 11 ISMS status in different business sizes

Having been asked if their companies had adopted any of ISMS standards or frameworks, participants were divided into two groups (logic switch was deployed on this question). Participants who answered ‘Yes’ or ‘No, but we are in progress’ were required to continue answering the following questions. However, participants who answered ‘No, but we might in the near future’ or ‘No, and we are not planning to adopt any of ISMS standards or frameworks’ were required to jump to section 6 of the questionnaire.

Popularity of ISMS standards or frameworks

Question 10 (multiple choice) asked participants what ISMS standards or frameworks had been adopted. Figure 4. 12 shows the proportion of each ISMS standard or framework that had been adopted by participants' companies. The top three most popular ISMS standards or frameworks were ISO 27001 (79.5%), NIST Cyber Security Framework (36.4%) and PCI DSS (31.8%).

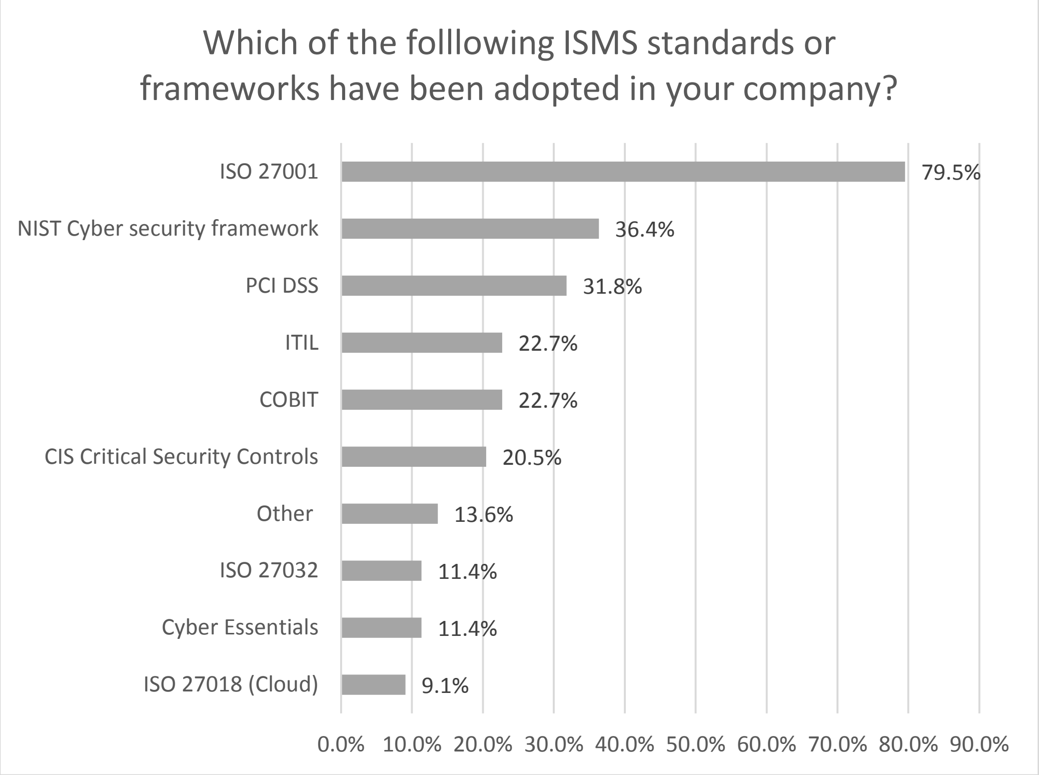


Figure 4. 12 Adopted ISMS standards or frameworks

In order to identify the adoption level of the top three most popular ISMS standards or frameworks in some particular business sectors, further data analysis was conducted. As shown above, ISO 27001, NIST Cyber Security Framework and PCI DSS received the most votes from respondents. However, the rank of the three ISMS standards or frameworks might change in different business sectors because of different business needs and requirements.

Findings (Question 7) noted that formalised ISMS had been established and maintained in the majority of companies in information technology, banking, financial services and insurance. Question 2 answers regarding the four identified particular business sectors above were tracked against Question 10 answers regarding the three most popular ISMS standards or frameworks. This was to identify if the rank of the three most popular ISMS standards or frameworks changes in particular business sectors, such as information technology, banking, financial services and insurance.

Figure 4. 13 shows the adoption level of the top three most popular ISMS standards or frameworks in information technology, banking, financial services and insurance. Results indicate that ISO 27001 was still the most popular ISMS standard in each of the four business sectors. Especially in financial services, 63.6% of respondents from financial companies had adopted ISO 27001. This was followed by information technology, half of the respondents from information technology companies indicated that they had adopted ISO 27001. It should be noted that the rank of PCI DSS increased to the second place in information security, banking and financial services.

Overall findings noted that ISO 27001 was widely adopted in the majority of industries. Other ISMS standards or frameworks were adopted based on different business needs and requirements in different business sectors.

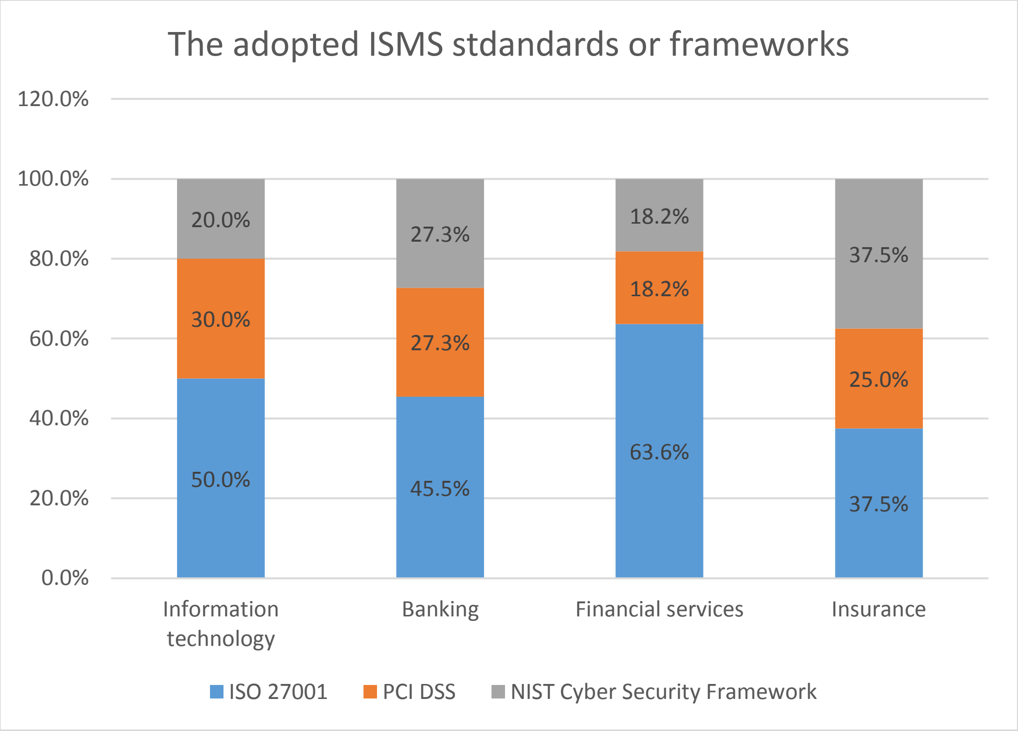


Figure 4. 13 Adopted ISMS standards or frameworks in four business sectors

Costs

Question 11 asked participants opinions on the average cost of the whole ISMS standards or frameworks adoption process. 45 participants answered this question. Findings noted that more than half (55.6%) indicated the total cost of the whole adoption process was high, 31.1% of them found that the total cost was neutral, and only 2.2% of them thought the total cost was low.

It should be noted that the cost of adoption of ISMS standards or frameworks varies influenced by the following factors:

- The size of company
- The physical and logical scope of the ISMS standards or frameworks
- The complexity of ISMS standards or frameworks
- The current maturity level of the ISMS
- The current ISMS Gap
- The capability of in-house development of ISMS
- Internal and external resources
- Certification 'Deadline' (Project Schedule)
- Cross certification

Among these factors, business size is the most significant factor determining the overall cost of the adoption process. Companies with a big number of employees and systems will cost more because it needs more resources. As such, it was necessary to identify opinions in different sizes of business. Figure 4. 14 shows the results of participants' opinions grouped by company size. Findings noted that only 1 respondent (3.8%) from big companies with more than 2,000 full-time employees indicated that the total cost was low. Regarding other sizes of companies, more than half of participants thought the total cost was high. Rest of respondents found the total cost was neutral.

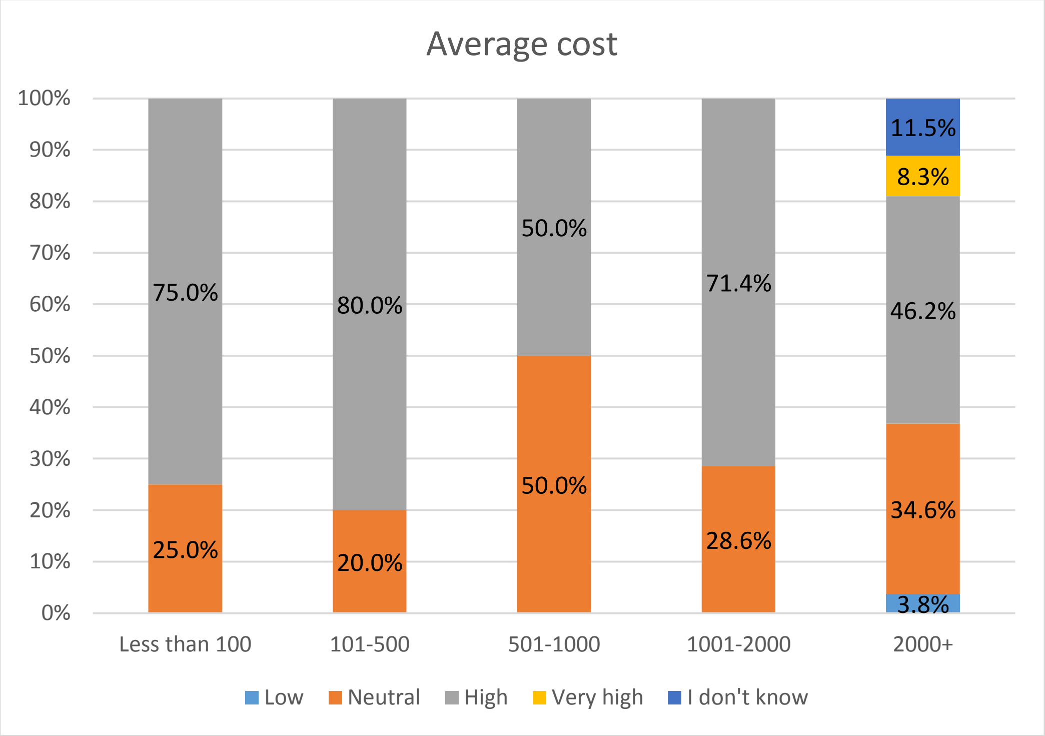


Figure 4. 14 The average cost of ISMS standards or frameworks adoption

Main drivers of adopting ISMS standards or frameworks

Question 12 (multiple choice) asked participants why their companies had adopted ISMS standards or frameworks. 45 responses were collected. As shown in Figure 4. 15, 73.3% of the respondents indicated that adopting ISMS standards or frameworks was for improving information security posture within their companies. This was followed by the second main driver – regulatory compliance. 62.2% of respondents reported that the main reason for adopting ISMS standards or frameworks was to ensure legal and regulatory compliance. Findings also noted that 48.9% of respondents indicated that the main driver of adopting ISMS standards or frameworks was to gain competitive advantage, especially in a tender.

Except the top three drivers identified above, results show that more than 40% of respondents also chose the following three aspects as main drivers of adopting ISMS standards or frameworks:

- To improve stakeholders' confidence when running business;
- To meet business needs;
- To meet contractual requirements.

Under the category of 'Other', only one respondent indicated that adopting ISMS standards or frameworks was used as a means of protecting customers' best interests.

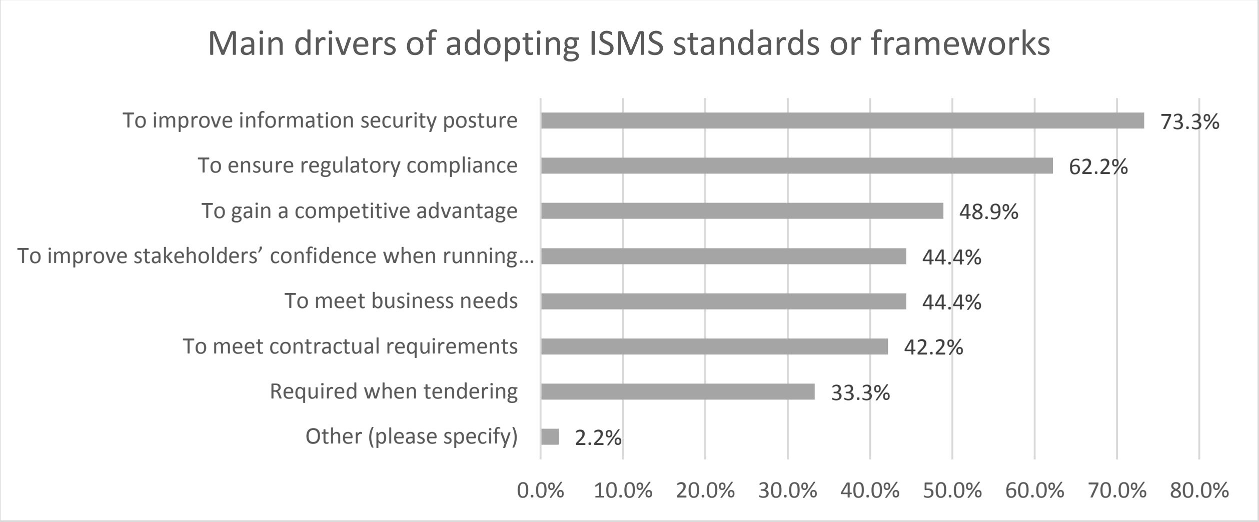


Figure 4. 15 Main drivers of adopting ISMS standards or frameworks

External resources

Question 13 asked participants if they had used any external consultant services for adopting ISMS standards or frameworks. 45 respondents answered this question. Findings reveal that 82.2% of them indicated that they had used external consultant services to help with the implementation process. This comprises 64.4% of respondents indicating that they used mixed resources (internal and external) and 17.8% of respondents indicating that they mostly relied on external resources.

Only 11.1% of them indicated that they had never used any external consultant services to help with the implementation process.

Table 4. *6* shows an overview of the results indicating that most companies had used external consultant services for adopting ISMS standards or frameworks.

Table 4. 6 External resources

Have you used any services of external consultants for adopting ISMS standards or frameworks including obtaining certifications?	**Responses**
Yes, mostly external	17.8%
Yes, mixed resources	64.4%
No	11.1%
I don’t know	6.7%

Section 4 Challenges and Barriers

The challenges and barriers to adopting ISMS standards or frameworks can be overwhelming. With so many areas need to be addressed prior to the commencement of implementation organisations need to know what challenges and barriers they are facing. The purpose of this section was to analyse the information gathered about challenges and barriers to adopting ISMS standards or frameworks. Information was analysed from the perspectives of challenges of choosing ISMS standards or frameworks (Question 14), challenges in adoption processes (Question 15), challenges of obtaining senior management support (Question 16) and challenges of implementing specific controls (Question 17). These questions were designed to elicit opinions regarding the main challenges and barriers to the entire processes of adopting ISMS standards or frameworks.

As outlined in the literature review, many ISMS standards and frameworks were released to help organisations keep information assets secure. The choice to adopt a particular ISMS standard or framework can be driven by multiple factors, such as regulatory compliance, business requirements, and organisation structure and complexity. As a result, choosing a suitable ISMS standard or framework is a prerequisite for managing information security programs effectively within organisations.

Question 14 asked participants if they had any challenges in choosing suitable ISMS standards or frameworks. 39 responses were collected from this question. Results show that 76.9% of respondents had no difficulties in choosing ISMS standards or frameworks. Only 18.0% of respondents indicated they had difficulties in choosing ISMS standards or frameworks because there were too many options.

As outlined in the literature review, adoption processes of ISMS standards or frameworks are not only affected by internal factors. External factors, such as education, media, training, perceived competitor benefits and external resources have influences on such processes in the meantime. With regard to companies having difficulties in choosing ISMS standards or frameworks, seeking external consultant services would be a good choice. In order to identify if external consultant service can help with choosing suitable ISMS standards or frameworks, further data analysis was carried out.

The results above (Question 14) were analysed against answers to Question 13 (if participants' companies had used external consultant services). Figure 4. 16 shows that 93.3% of respondents whose companies had no difficulties in choosing ISMS standards or frameworks had used external consultant services. However, this proportion reduced to 80.0% for the group of respondents whose companies had difficulties in choosing ISMS standards or frameworks. On the other hand, 6.7% of respondents whose companies had no difficulties in choosing ISMS standards or frameworks had not used any external consultant services. And this proportion increased to 20.0% for the group of respondents whose companies had difficulties in choosing ISMS standards or frameworks.

This trend indicates that companies with the help of external consultants were not likely to have difficulties in choosing suitable ISMS standards or frameworks. The results also prove the importance of external consultant services in helping with adopting ISMS standards or frameworks, especially in choosing suitable ISMS standards or frameworks.

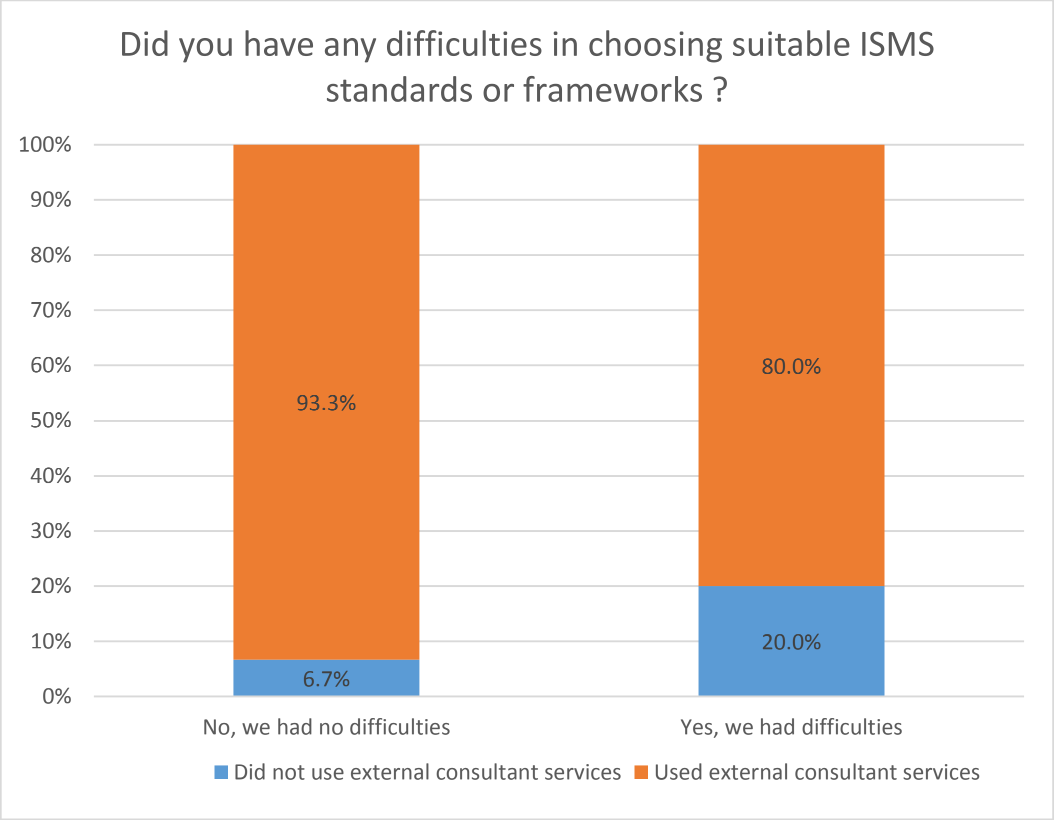


Figure 4. 16 Difficulties in choosing ISMS standards or frameworks

As one of the most important questions in the questionnaire, Question 15 (multiple choice) asked participants about the main challenges and barriers to adopting ISMS standards or frameworks. This question was designed to elicit opinions regarding challenges and barriers. As outlined in the literature review, key factors influencing information security management were identified – senior management commitment, external influences and human factors. Question 15 was designed from the three perspectives. Table 4. 7 illustrates how those choices were linked to the three identified factors affecting information security management.

Table 4. 7 Challenges and barriers

Key factors	Challenges and barriers
Senior management commitment	Budget constraints
	Business support
	Leadership and engagement of staff
	Senior management support
External influences	Obtaining certification to the standard

	Seeking external consultant services
Human factors	Defining the scope
	Change resistance
	Obtaining employee buy-in or raising staff awareness
	Conducting risk assessments
	Creating and managing ISMS documentation
	Reporting and maintaining ISMS
	Skilled resources
	Identifying required controls
	Culture change within organisations
	Understanding standards
	Project management

39 respondents answered Question 15. Figure 4. 17 shows an overview of the main barriers to adopting ISMS standards or frameworks. More than half of respondents indicated that defining the scope was the biggest challenge. This was followed by the challenge of change resistance (48.7%), obtaining employee buy-in or raising staff awareness (38.5%), conducting risk assessments (35.9%), and creating and managing ISMS documentation (35.9%).

It should be noted that the top five identified barriers were all human factors. And the sixth barrier was budget constraints (28.2%), which was part of senior management commitment. From the seventh to eleventh were reporting and maintaining ISMS (28.2%), skilled resources (23.2%), identifying required controls (23.1%), culture change within organisations (20.5%) and understanding standards (20.5%). And these barriers were part of human factors again.

Results indicate that only a few of respondents recognised barriers from senior management commitment as main barriers to adopting ISMS standards or frameworks – namely business support (17.9%) and leadership and engagement of staff (12.8%).

It was also noted that barriers from external influences received an extremely small number of votes. They were barriers to obtaining certification to the standard (7.7%) and seeking external consultant services (5.1%). There was only one response included in ‘Other’ category. And this barrier was information overloading.

From data analysis results identified above, it was noted that barriers of human factors were the main barriers to adopting ISMS standards or frameworks. Most companies were still facing barriers resulted by human factors. Therefore, to improve the robustness of information security systems, information security management should consider human factors, such as change resistance and staff awareness as key elements.

Findings noted that, above all, defining ISMS scope was the top barrier to adopting ISMS standards or frameworks in most companies. ISMS scope should be defined according to business needs, organisation structures, relevant technologies, locations and information assets.

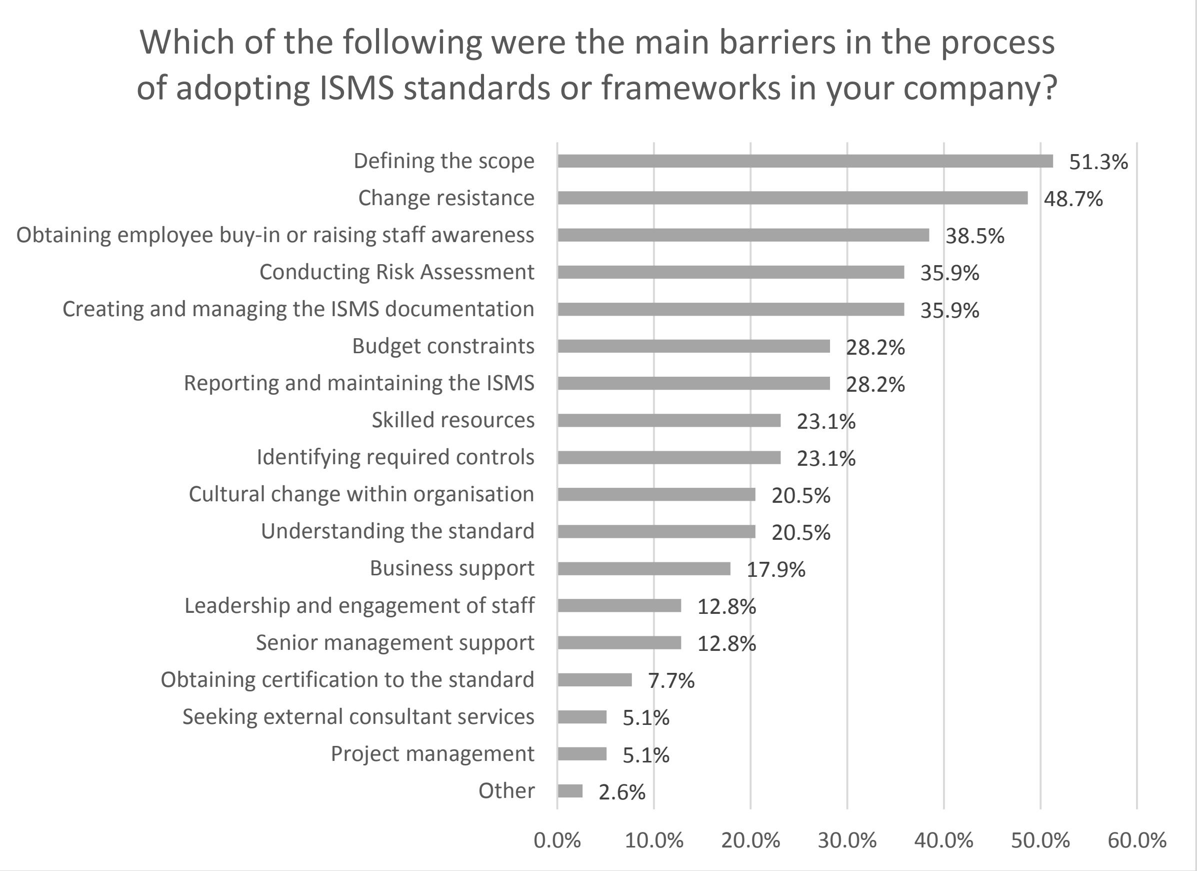


Figure 4. 17 Main barriers to adopting ISMS standards or frameworks

Question 16 asked participants if they had any challenges of convincing the board to implement ISMS standards or frameworks. 39 responses were collected from this question. Results show that 17 respondents (43.6%) indicated that they had no challenges of convincing the board to implement ISMS standards or frameworks. This was followed by that 8 respondents (20.5%) found that addressing the importance of the adoption was the biggest challenge of convincing the board to implement ISMS standards or frameworks. Another two identified challenges were securing sufficient budget allowance (18.0%) and ensuring the engagement of skilled staff (15.4%). Only one respondent indicated that estimating the return on cost savings was the biggest challenge. Table 4. 8 shows an overview of the results indicating that most companies had no challenges of convincing the board to implement ISMS standards or frameworks.

Table 4. 8 Challenges of convincing the board

Biggest challenge of convincing the board	**Response**
We had no challenges	43.6%
Addressing the importance of the adoption	20.5%
Securing sufficient budget allowance	18.0%
Ensuring the engagement of skilled staff	15.4%
Estimating the return on cost savings	2.6%

Question 17 (multiple choice) asked participants which control areas required by ISMS standards or frameworks were most concerned. 40 respondents answered this question. Figure 4. 18 shows the results indicating that the top three control areas required by adopted ISMS standards or frameworks where respondents had concerns were compliance (55.0%), assets classification and control (45.0%) and business continuity management (35.0%).

It was noted that only one response was collected under ‘Other’ category. And this response was noted - ‘how much lower will it reduce the rate of adverse events to the benefit of our customers’. Except ‘Other’ physical access control received the least votes (12.5%).

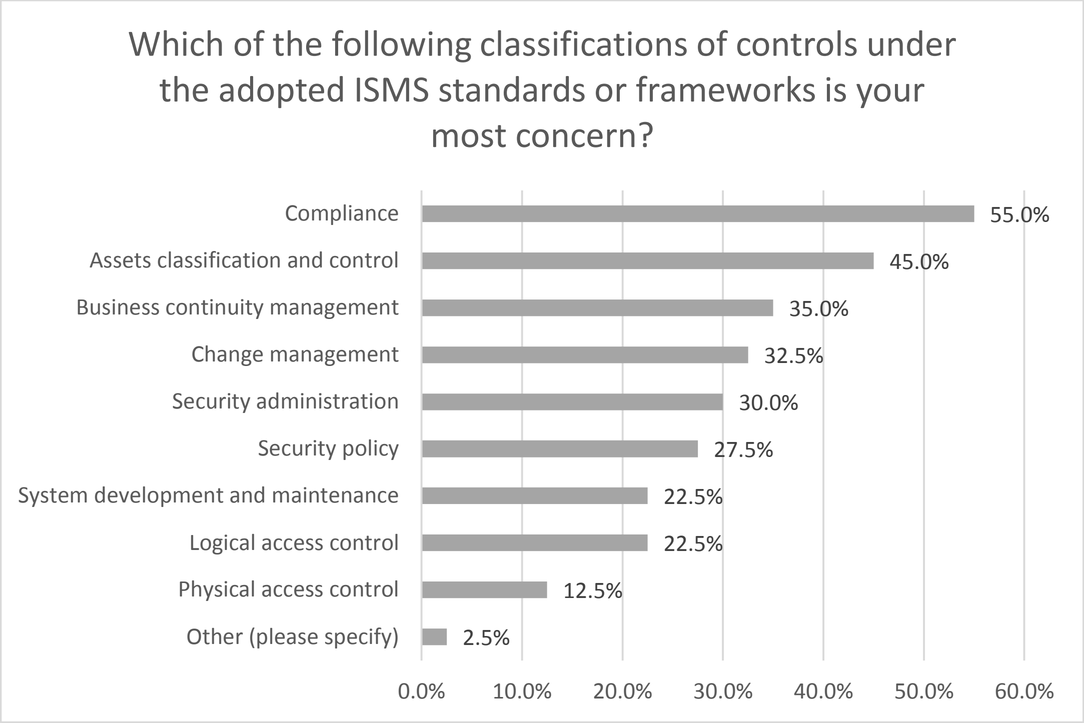


Figure 4. 18 Control areas where participants had concerns

Section 5 Benefits of adopting ISMS standards or frameworks

Implementing and maintaining an effective ISMS presents a systematic approach to managing the security of sensitive information within organisations. Adopting ISMS standards or frameworks delivers direct benefits for improving an organisation's information security posture. The purpose of this section was to analyse the information gathered about benefits of adopting ISMS standards or frameworks. Three questions were asked in this section including security breaches prevention (Question 18), benefits to the entire organisation (Question 19) and benefits to ICT team (Question 20).

As outlined in the literature review the number of security breaches has been significantly increased since 2014. The cost of breaches continues to soar for all sizes of business. From this perspective the biggest benefit that adopting ISMS standards or frameworks brings would be the increased ability of ISMS to prevent security breaches.

Question 18 asked participants if they agree that security breaches can be prevented by adopting ISMS standards or frameworks. 39 responses were collected from this question. Results show that 74.4% of respondents agreed that security breaches can be prevented by adopting ISMS standards or frameworks. Only 25.6% of respondents disagreed.

Question 19 asked participants what was the most important benefit that the adoption of ISMS standards or frameworks has brought to their companies. 39 respondents answered this question. 38.5% of respondents indicated that the most important benefit of adopting ISMS standards or frameworks was improved information security across the company. This was followed by improved staff information security awareness (23.1%), structured information security management (10.3%), and improved stakeholders' confidence in information security (10.3%).

It was noted that no respondents regarded improved competitiveness as the most important benefit of adopting ISMS standards or frameworks. Figure 4. 19 shows an overview of the results.

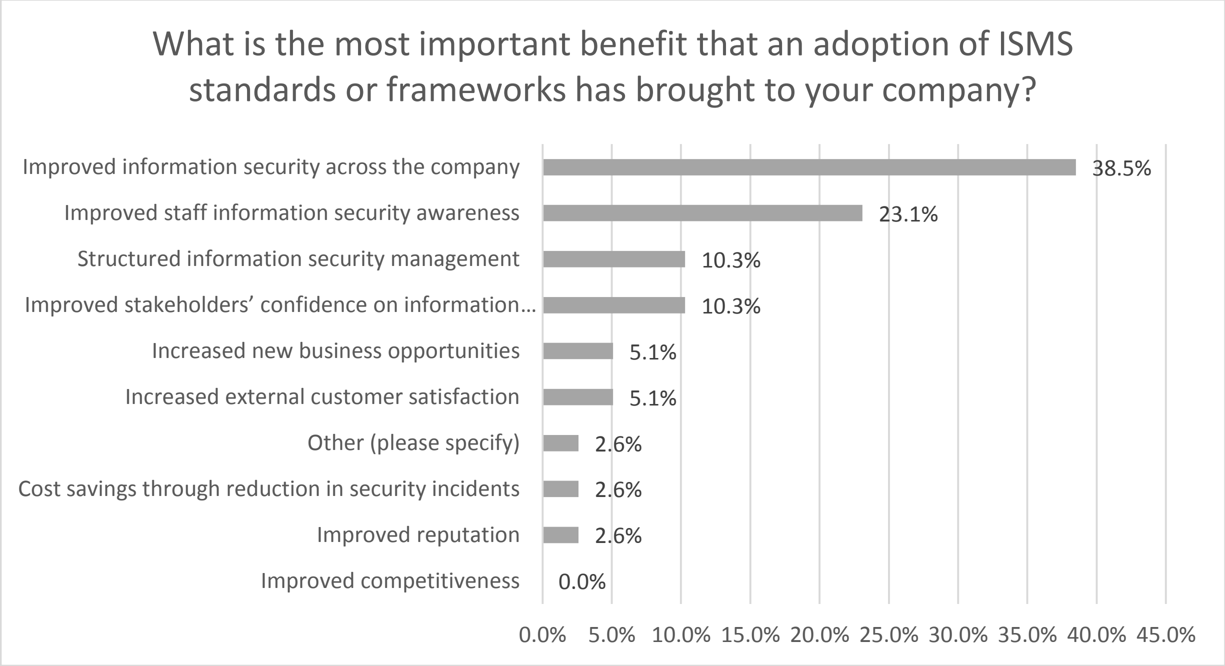


Figure 4. 19 Benefits to overall organisation

Question 20 asked participants what was the most important benefit that the adoption of ISMS standards or frameworks has brought to their ICT teams. 40 respondents answered this question. As shown in Figure 4. 20, 42.5% of respondents indicated that the most important benefit of adopting ISMS standards or frameworks for ICT team was improved ICT staff security awareness. And this was followed by structured ICT management (40.0%).

Only 3 respondents (7.5%) indicated that the most important benefit of adopting ISMS standards or frameworks was strategic projects management. And this was followed by reduced costs (5.0%).

It should be noted that there was an obvious gap between structured ICT management (40.0%) and strategic projects management (7.5%). The results shown in Figure 4. 20 concluded that the identified two most important benefits of adopting ISMS standards or frameworks for ICT team were improved ICT staff security awareness and structured ICT management.

It was noted that two respondents chose ‘Other’. And the two responses were:

- Policy support for process excellence, operational activity and control design;
- Improved security, reduced risks.

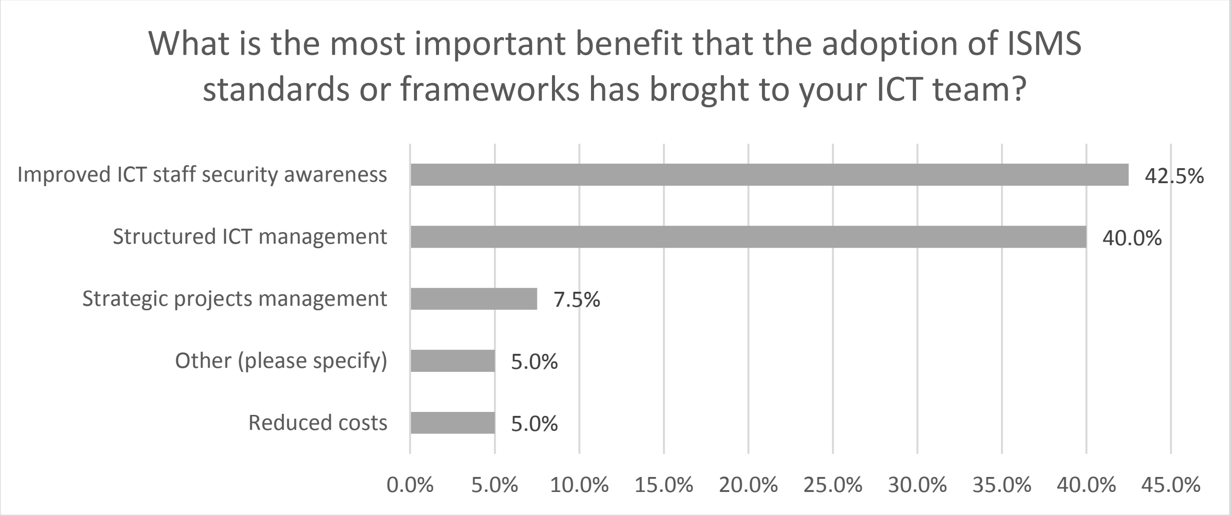


Figure 4. 20 Benefits to ICT team

Section 6 Plans for the future

Before adopting ISMS standards or frameworks, organisations need to know what challenges and barriers they are facing (section 4) and what benefits organisations can expect (section 5). However, there are still many organisations choosing not to adopt any ISMS standards or frameworks for various reasons. In order to improve the adoption level of ISMS standards or frameworks, it is necessary to know what those reasons are (Question 21) and how to increase the adoption rate (Question 22). This section continued to gather information about barriers to adopting ISMS standards or frameworks, but from participants who decided not to adopt any ISMS standards or frameworks.

Question 21 (multiple choice) asked participants why they had not adopted any ISMS standards or frameworks. 9 respondents answered this question. As shown in Figure 4. 21, 55.6% of them indicated that the main reason was the implementation cost. This was followed by the following three main reasons:

- I don’t think my company will benefit from this since we already have a good security management (44.4%);
- Implementation is too complex and we need to commit too many resources (44.4%);

- Lack of specialised staff or lack of related knowledge (44.4%).

Results above noted that the main reason why participants had not adopted any ISMS standards or frameworks was the overall implementation cost. According to Hinson (2008), the costs of implementing include:

- Project management and project resources cost;
- Organisational change processes and resources cost;
- Updating, developing, and testing of processes and controls cost;
- Certification cost;
- Operation and maintenance cost.

Findings above also noted that lack of resources and not aware of benefits were the other two main reasons of non-adoption.

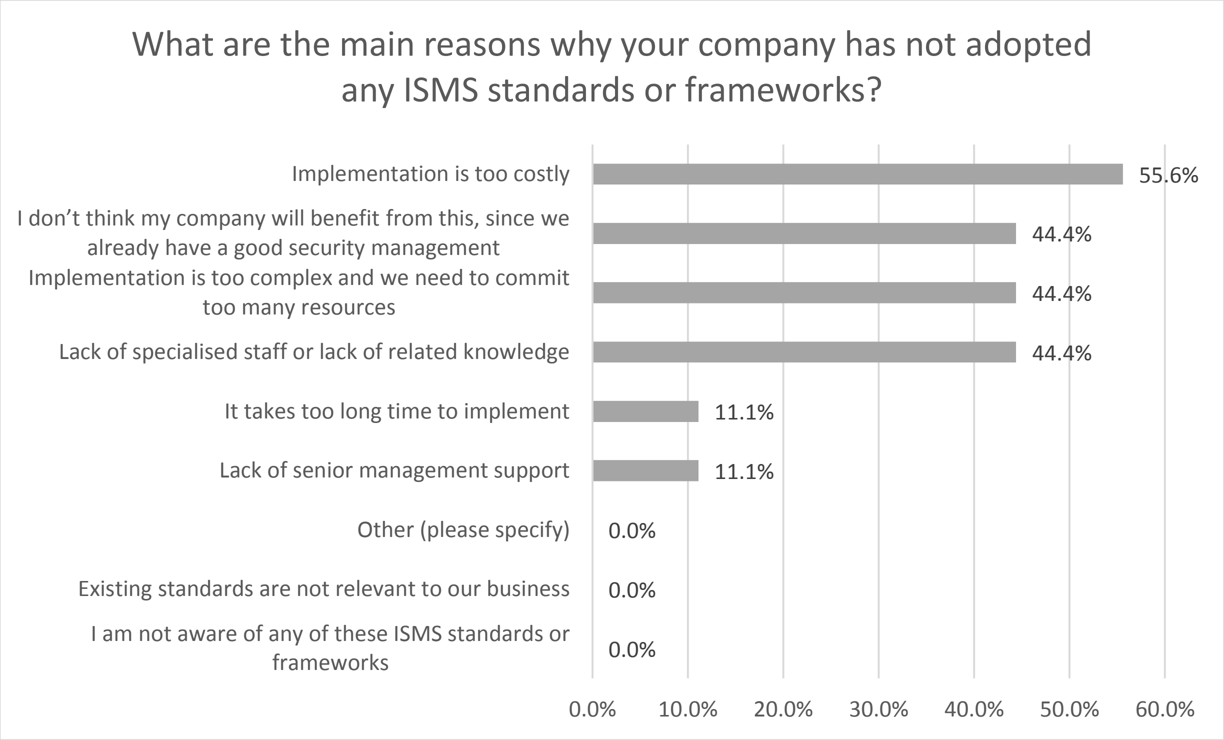


Figure 4. 21 Reasons why not to adopt ISMS standards or frameworks

Question 22 (multiple choice) asked participants their opinions on how to improve the adoption rate of ISMS standards or frameworks. 49 respondents answered this question. As shown in Figure 4. 22, 57.1% of them indicated that most existing ISMS standards and frameworks were too complicated. If the complexity of requirements was reduced, the adoption rate would increase.

This was followed by increasing awareness. 53.1% of respondents reported that many of ISMS standards and frameworks were not popular resulting in non-adoption. In order to increase the adoption rate awareness of these ISMS standards and frameworks should be increased. ISMS awareness training is the fast way to obtain awareness and knowledge on ISMS and related standards or frameworks.

Results also noted that more than half of respondents (51.0%) indicated that the cost of implementation was too high. On the contrary, lower cost will result in more companies adopting ISMS standards or frameworks.

Only two respondents chose the 'Other' option. One of them reported that assessment requirements should be reduced for cross certifications.

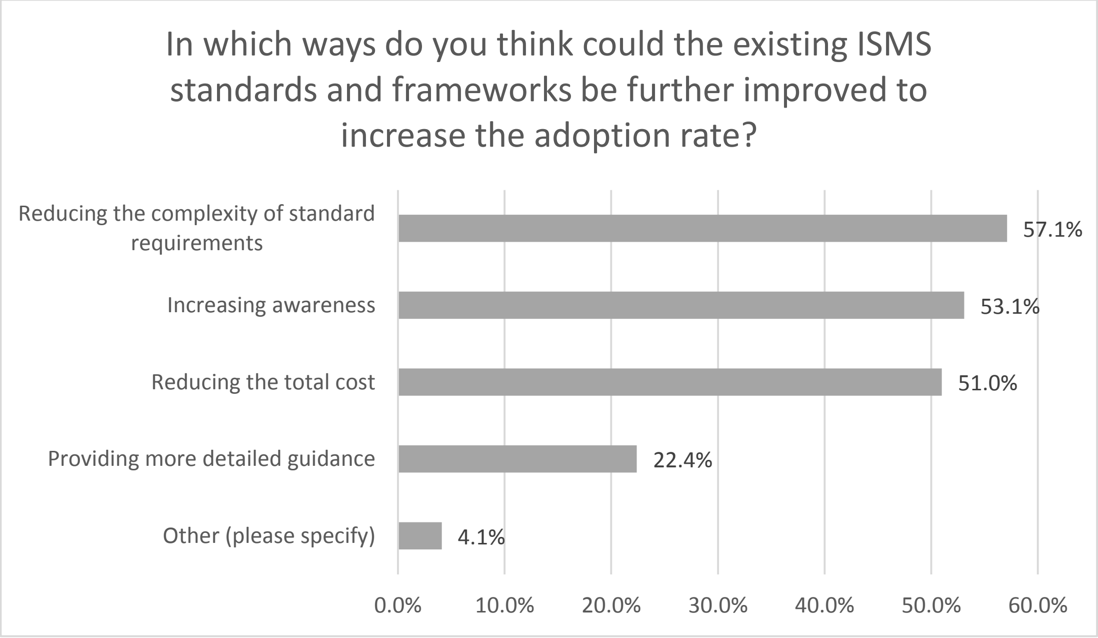


Figure 4. 22 How to improve the adoption rate

4.5 Summary of Findings

This chapter has presented data analysis and findings of all sections of the research survey with the purpose of exploring two research questions focused on challenges and barriers to adopting ISMS standards or frameworks. Primary data was collected from an online survey that was distributed and advertised on LinkedIn and information security related forums. Collected data was analysed via SurveyMonkey®, Excel and designed Python scripts.

From the data collected in section 1 and section 3 of the survey, the results confirmed that:

- Companies in information technology, financial services, banking and insurance were likely to have a formalised ISMS established and maintained;
- Companies with dedicated senior executives were likely to have a formalised ISMS established and maintained;
- 82.4% of companies with more than 500 full-time employees had established and maintained formalised ISMS;
- 73.2% of companies had adopted at least one ISMS standard or framework;
- Companies in information technology, financial services, banking, insurance and consulting were likely to have adopted ISMS standards or frameworks;
- 92.9% of companies with more than 2,000 full-time employees had adopted ISMS standards or frameworks;
- 50.0% of companies with less than 100 full-time employees had adopted ISMS standards or frameworks;
- ISO 27001, NIST Cyber Security Framework, and PCI DSS were the top three most popular ISMS standards or frameworks adopted by companies;
- More than half (55.6%) of respondents indicated that the cost of adoption process was high;
- 73.3% of respondents reported that the main driver of adopting ISMS standards or frameworks was to improve information security posture;
- 82.2% of respondents indicated that they had used external consultant services for adopting ISMS standards or frameworks.

From the data collected in section 4 of the survey, the results confirmed that:

- 76.9% of respondents reported that they had no difficulties in choosing ISMS standards or frameworks;
- Companies with the help of external consultants were not likely to have difficulties in choosing suitable ISMS standards or frameworks.
- More than half of respondents reported that the main barrier to adopting ISMS standards or frameworks was defining the scope;

- 55.0% of respondents reported that compliance was the most concerning control area.

From the data collected in section 5 of the survey, the results confirmed that:

- 74.4% of respondents agreed that security breaches can be prevented through adopting ISMS standards or frameworks;
- 38.5% of respondents reported that the biggest benefit of adopting ISMS standards or frameworks was improved security across the company;
- 42.5% of respondents reported that the biggest benefit of adopting ISMS standards or frameworks for ICT team was improved ICT staff security awareness.

From the data collected in section 6 of the survey, the results confirmed that:

- 55.6% of respondents reported that the implementation was too costly and this was the main reason why their companies had not adopted any ISMS standards or frameworks.
- 57.1% of respondents reported that the complexity of ISMS standards or frameworks needs to be reduced to increase the adoption rate.

The research findings suggest that human factors were the main barriers to adopting ISMS standards or frameworks. Therefore, in order to improve the robustness of information security systems, information security management should consider human factors, such as change resistance and staff awareness as key elements. The next chapter details the conclusions, recommendations of the study, research limitations and opportunities for future research.

Chapter 5 – Conclusions and Future Work

5.1 Introduction

This chapter presents the conclusions from data analysis carried out as part of this research, demonstrates how the research questions were answered, and lists the key findings. Additionally, a discussion on the generalisability of findings is presented. Lastly, limitations of the research and future research directions are outlined.

5.2 Research questions and objectives

The primary objective of this research was to examine the factors influencing the adoption of ISMS standards or frameworks. Existing studies (Chapter 2 – Literature Review) have identified certain factors, though very few have synthesised exactly what influences the adoption of ISMS standards or frameworks. Since there is a gap between existing literature and the research questions presented here, quantitative research was designed to answer the following questions:

1. What are the challenges and barriers to adopting ISMS standards or frameworks?
2. What are the concerns of senior management when adopting ISMS standards or frameworks?

In order to answer the questions above, this quantitative research was designed into two main stages – a theoretical review stage and confirmatory stage. The theoretical review stage was carried out by exploring existing literature related to information security, ISMS management, and ISMS standards or frameworks. The results of the theoretical review stage indicate that the following three factors affect information security management within organisations.

Senior management commitment is critical to successful information security management. Many studies (Soomro et al., 2015; Barton et al., 2016; Van Kessel, 2012) have identified that information security should be considered and implemented from a managerial perspective to ensure information security objectives and activities are aligned with business objectives, which can only be achieved with senior management commitment and support. In this case, senior management is required to have sufficient security-related knowledge to ensure they have correct understanding of what is required. Another reason why senior management commitment is necessary for effective information security management is that they have the privileges of leadership and governance.

External influences, such as increased reporting of security breaches, high cost of security breaches (both directly and potential cost), technology changes, and regulatory forces have a significant impact on information security management by affecting the quality of IT controls that is regarded as critical in business (Li et al., 2007). Within various external influences, regulatory compliance is the most concerning for organisations as noncompliance results in a fine (Hu et al., 2007; Ghose & Raian, 2006). For instance, GDPR, Sarbanes-Oxley Act (SOX), and the Public Company Accounting Oversight Board (PCAOB) all have direct influences on information security management within organisations. On the other hand, regulatory changes require senior management's prompt consideration to ensure that amended business practices supported by IT systems and operational processes are compliant with new regulations (Grant Thornton, 2017).

Human factors play a significant role in information security management within organisations. Although technical controls are in place within most organisations to automate business processes and avoid human errors, information security is still determined by human actions because these systems are designed, implemented, and maintained by humans. A well-designed ISMS still has to rely on people in relation to information security awareness, senior management support, security knowledge and skillsets, and communication (Alavi et al., 2014; Soomro et al., 2015; Rocha Flores et al., 2014). Currently, human factors are the most vulnerable parts of information security management within organisations. Considering that some forms, such as irrational behaviour, can adversely affect the function of information security systems, human factors should be addressed at all stages of system design and in line with information security requirements (Alavi et al., 2014). Without the effective management of human factors, organisations will be facing insider threats that pose security risks due to their knowledge of information assets and privileged access to information systems.

Conclusions of the confirmatory stage are presented in the following section.

5.3 Research Findings

Chapter Four identified a number of key findings, summarised below.

Findings on the establishment of ISMS:

- Companies in information technology, financial services, banking, and insurance were likely to have a formalised ISMS established and maintained;
- Companies with dedicated senior executives were likely to have a formalised ISMS established and maintained;
- 82.4% of companies with more than 500 full-time employees had established and maintained formalised ISMS.

Findings on adoption status of ISMS standards or frameworks:

- 73.2% of companies had adopted at least one ISMS standard or framework;
- Companies in information technology, financial services, banking, insurance, and consulting were likely to have adopted ISMS standards or frameworks;
- 92.9% of companies with more than 2,000 full-time employees had adopted ISMS standards or frameworks;
- 50.0% of companies with less than 100 full-time employees had adopted ISMS standards or frameworks;

Findings on adopted ISMS standards or frameworks:

- ISO 27001, NIST Cyber Security Framework, and PCI DSS were the top three most popular ISMS standards or frameworks adopted by companies.

Findings on adoption costs:

- More than half (55.6%) of respondents indicated that the cost of adoption process was high.

Findings on main drivers:

- 73.3% of respondents reported that the main driver of adopting ISMS standards or frameworks was to improve information security positioning.

Findings on external resources:

- 82.2% of respondents indicated that they had used external consultant services for adopting ISMS standards or frameworks.

Findings on challenges and barriers:

- 76.9% of respondents reported that they had no difficulties choosing ISMS standards or frameworks;
- Companies, with the help of external consultants, were not likely to have difficulties in choosing suitable ISMS standards or frameworks;
- More than half of respondents reported that the main barrier to adopting ISMS standards or frameworks was defining the scope;
- Human barriers were the main issue with adopting ISMS standards or frameworks;
- 55.0% of respondents reported that compliance was the most concerning control area;

- 55.6% of respondents reported that the implementation was too costly and this was the main reason why their companies had not adopted any ISMS standards or frameworks;
- 57.1% of respondents reported that the complexity of ISMS standards or frameworks needs to be reduced to increase the adoption rate.

Findings on benefits

- 74.4% of respondents agreed that security breaches can be prevented through adopting ISMS standards or frameworks;
- 38.5% of respondents reported that the biggest benefit of adopting ISMS standards or frameworks was improved security across the company;
- 42.5% of respondents reported that the biggest benefit of adopting ISMS standards or frameworks for ICT teams was improved ICT staff security awareness.

5.4 Research questions and answers

The research was designed to examine factors influencing the adoption of ISMS standards or frameworks. This objective forms the basis of the following research questions:

1. **What are the challenges and barriers to adopting ISMS standards or frameworks?**

The outputs of Chapter 4 – Findings and Analysis show that the top five main challenges are defining the scope, change resistance, obtaining employee buy-in, conducting risks assessments, and creating and managing ISMS documentations. Findings support the view that main challenges of adopting ISMS standards or frameworks mainly come from human factors. As outlined in the literature review, although playing a significant role, human factors are still the most vulnerable parts of information security management. This results from the difficulties in analysing, modelling, qualifying, and controlling the human element (Alavi et al., 2014). Organisations never lack appropriate technical solutions, but always fail to handle human factors. To effectively manage information security, organisations should achieve a balanced approach between technical and human factors. Within information security management, risks related to human factors, such as the five identified challenges, should be dealt with using a risk management model. Within the risk management model, human factors are considered in two categories – driving and restraining forces. Driving forces promote expected goals and objectives, but restraining forces result in ineffective ISMS.

The increased reporting and the high cost of such security breaches means security expenditure becomes an important matter for organisations. The result shows more than half of participants indicated that implementing ISMS standards or frameworks is too costly, thus cost is one of the main barriers. Although the cost depends on company size, the ISMS scope, ISMS gap, and the capability to close any gap the average cost is generally high for most organisations, especially for SMEs because the qualification process is generally more expensive and they are more reliant on external consultant services. Although the advantages of adopting ISMS standards or frameworks outweigh the high costs, many SMEs regard the adoption as a lengthy, complex, and costly process, rather than a cost-effective investment.

The complexity of ISMS standards or frameworks is another challenge to adoption. More than half of participants indicated that the adoption process is too complicated and the complexity of those standards or frameworks needs to be reduced to improve the adoption rate. This complexity stems from two aspects – technological requirements and the standards themselves. Technological complexity is a challenge for security practitioners, given the complexity of systems, vulnerabilities (system or application), lack of effective and efficient security tools, mobility, and distributed access (Werlinger et al., 2009). Further, the growing dependence of organisations on technologies to drive business and to create a competitive advantage makes information security management within organisations extremely challenging, especially for managing the big picture and designing security policies that cover all possible configurations (Onwubiko & Lenaghan, 2009). Furthermore, some ISMS standards or frameworks are too complicated to read for non-professionals, which increases the level of difficulty for understanding standards or frameworks requirements.

2. **What are the concerns of senior management when adopting ISMS standards or frameworks?**

With the increased reporting of security breaches and the high cost of such breaches, information security concerns within organisations have been the top priority on senior managements' agenda. Senior management within an organisation has the ultimate responsibility for protecting the organisation's information assets. Although establishing an ISMS is a wise investment to ensure information confidentiality, integrity, and availability senior management still has concerns of implementing ISMS standards or frameworks. Generally, senior management concerns include whether:

- sufficient and reliable information can be provided to stakeholders concerning its information security risks and the status of information security;
- information security posture can be improved;
- regulatory requirements can be met;
- staff information security awareness can be improved;
- the cost of implementation is effective and efficient.

This research divides organisations into two groups – organisations that have already adopted ISMS standards or frameworks and those that have not. For those that have already adopted ISMS standards or frameworks, the main concerns are their current information security position, the ever-growing regulatory compliance requirements, and information security awareness among staff. Findings reveal that more than 60% of organisations have adopted ISMS standards or frameworks with intentions of improving their security and ensuring regulatory compliance. Findings also note that for the same group of participants, the most important benefits that such an adoption has brought is improved information security. For those that have not adopted any ISMS standards or frameworks, the main concern is the cost, according to more than half of participants. As mentioned above, many SMEs regard the adoption process as a lengthy, complex, and costly process.

Again, senior management concerns involve human factors and external influences. From the human point of view, the most significant concerns are security risks and the current status of security. Within an organisation, establishing a risk management model will be an effective way to monitor and manage risks caused by human factors. Risk management is basically a human activity that requires the provision of sufficient and reliable information to key stakeholders to obtain valuable perceptions of security risks. As human errors present serious threats to information security within organisations, staff information security awareness should be address to reduce human errors to an acceptable level. In relation to external influences, the cost of implementation and regulatory compliance requirements form the main concerns of senior management.

5.5 Generalisability of Findings

According to Saunders et al. (2016), generalisability is referred to as external validity that is to what extent research findings may be equally applicable to other research settings, such as other organisations.

As outlined in Chapter 3 – Methodology and Fieldwork, this quantitative research was carried out through an online survey designed based on the knowledge obtained from the literature review. While a quantitative research method was chosen via a structured online survey, a small amount of qualitative data was collected. An ‘Other’ option followed by an open text box was provided for the majority questions in the questionnaire to ensure participants could input accurate answers when the provided options did not include or represent their ideal answers. Because the size of qualitative data collected from the online survey was small and it did not increase the complexity of data analysis, qualitative data analysis methods were not considered for this research.

Ninety-two responses were collected through the online survey. According to a survey carried out by European Commission (2016), the number of enterprises in Ireland was 164,189 in 2016. The sample required was calculated using the following formula provided by SurveyMonkey® (2017):

$$\text{Sample Size} = \frac{\frac{z^2 \times p(1-p)}{e^2}}{1+\left(\frac{z^2 \times p(1-p)}{e^2 N}\right)}$$

Where,

Population Size = N;

Margin of error = e;

Number of standard deviations (z-score) = z;

The desired confidence level and corresponding z-score are listed in Table 5. 1.

Table 5. 1 Confidence Level and z-score

Desired Confidence Level	z-score
80%	1.28
85%	1.44
90%	1.65
95%	1.96
99%	2.58

In this research, N = 164,189, e = 10%, and the confidence level = 90%. The final expected sample size was 68, which confirms that the actual samples size is large enough to be representative. However, if the confidence level is improved to 95% and the other parameters remain the same, the expected sample size would increase to 96. In that case, the actual sample size is smaller than the expected sample size. Again, if the confidence level is improved to 95% and the margin of error is reduced to 5%, the expected sample size would increase to 384, resulting in an obvious gap between the expected sample size and the actual sample size. Future research is therefore required to improve the generalisability of the study.

5.6 Limitations of research

Although key findings were generated from data analysis results and those findings answered the research questions, this research was restricted to three main limitations – the research method, sample size and time horizon.

According to Saunders et al. (2016), inductive approaches are generally associated with qualitative methods, whilst deductive approaches are commonly associated with quantitative methods. A quantitative method was used in this research via a highly structured online survey and an inductive approach. Although there was no literature stating that a quantitative method cannot be used in an inductive approach to generate a theory or explain a phenomenon, participants' answers were restricted to pre-designed questions and options in the questionnaire. So there was a risk that participants' perceptions were not captured accurately. When the pre-designed choices did not include participants' ideal answers, an 'Other' option was provided for the majority of questions as an open text space. However, only a small amount of qualitative data was collected. It should be also noted online surveys have drawbacks:

- Dishonesty
- Lack of conscientious
- Differences in understanding and interpretation
- Hard to convey feelings and emotions
- Some questions are difficult to analyse
- Lack of personalisation
- Incomplete questionnaires

Another limitation of this research is sample size. Ninety-two responses were collected through the online survey. As mentioned above, the actual sample size is not sufficient to achieve a certain confidence level. Also, the collected responses were not evenly spread over business sectors, so the sample size was too small to analyse for some business sectors. Therefore, this research is limited in terms of generalising findings widely.

This research was conducted from January to August 2017. Considering the short time frame, a cross-sectional study was adopted, which means it only involved an assessment of the phenomenon at a particular time. Although the online survey was designed based on solid theories extracted from existing literature, perceptions of participants may change, which would ultimately affect data analysis results. For example, consider a company that does not adopt any ISMS standards or frameworks because of its high cost. Over time, under external influences, this company adopts ISO 27001, but they think their ISMS is very difficult to maintain for some reason. Then the challenge moves from cost to maintenance.

5.7 Future Research Opportunities

Several possibilities exist for future studies. One natural extension of this study is to build an empirical model comprising hypotheses generated from the findings above. This model should be subject to empirical testing with a deductive approach using quantitative research methods. This would provide further support and a greater understanding of information security management within organisations towards key factors influencing the adoption of ISMS standards or frameworks.

As mentioned above, three research limitations exist – the research method, sample size and time horizon. Future research is required to improve these aspects of the research:

- Qualitative research method through interviews should be considered;
- Sample size should be increased to ensure sufficient samples can be obtained in each targeted business sector;
- A longitudinal study should be considered to investigate this over a period of time. Measurements of the same individuals should be taken repeatedly through time.

While this research focuses on all world organisations, geographical locations were not identified in the online survey questionnaire, nor were national cultural factors. According to Rocha Flores et al. (2014), the national cultural factor, as a much broader and more profound factor, has influences on behavioural information security governance within organisations. Future research should investigate the relationship between national cultures and ISMS. This investigation would attempt to provide an analysis on how diversity in national culture could affect the adoption of ISMS standards or frameworks.

This research concludes that human factors are the main challenges of adopting ISMS standards or frameworks. Given that most organisations have made efforts to implement technical solutions to information security questions that are rooted in human factors, a natural extension will be an investigation of how human factors affect the adoption of ISMS standards or frameworks within organisations. This investigation would attempt to provide a richer and deeper insight of human factors in ISMS adoption and maintenance processes.

Adopting ISMS standards or frameworks within organisations is not an easy task. Future research should define exactly how organisations can adopt ISMS standards or frameworks. This would provide prescriptive and practical guidance and would address concerns to improve the adoption level of ISMS standards or frameworks.

5.8 Summary

Over the past decades, information security risks have become a top priority on senior managements' agenda because of increased reports of security breaches and the costs. Under various external influences, organisations are seeking ways to protect the information regard as the lifeblood of their business. As a result, organisations attempt to align their ISMS to the best practices – the published ISMS standards and frameworks. While it has been over 20 years since the first ISMS standards (BS-7799) were issued, the adoption level is still low.

This research addresses the importance of adopting ISMS standards or frameworks and identified three key factors (senior management commitment, external influences and human factors) that affect information security management from existing literature.

A quantitative research method was used in the form of an online survey following an inductive approach. This research presents statistical evidence that the main challenges of adopting ISMS standards or frameworks result from human factors, including defining the scope, change resistance, obtaining employee buy-in, conducting risk assessments, and creating and managing ISMS documentations. Except for human factors, external influences, such as the high cost of adoption and the complexity of ISMS standards or frameworks, also influence the adoption of ISMS standards or frameworks. The benefits of adopting ISMS standards or frameworks are also highlighted in the research, which include effectively preventing security breaches, improved information security postures, and improved staff information security awareness.

Based on the findings and existing literature, human factors and external influences are the two main senior management concerns when establishing ISMS within organisations. Concerns about human factors include security risks, risk management, and current security levels. External influence concerns mainly involve costs. Before the establishment of ISMS standards or frameworks, senior management are concerned if the investment will be cost-effective.

In answering the research questions, other interesting findings were identified, including findings on the establishment of ISMS, the adoption status and popularity of ISMS standards or frameworks. These findings provide a greater understanding of the current status of ISMS standards or frameworks adoption.

References

Aalders, R. & Hind, P. 2002. The IT manager’s survival guide. John Wiley & Sons Ltd. p.144

Advanced Network Systems. 2008. Why Your Organization Needs to Implement DLP - An Osterman Research White Paper. Available at: www.ostermanresearch.com [Accessed: 17 August 2017].

Alavi, R., Islam, S. & Mouratidis, H., 2014. LNCS 8533 - A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. LNCS, 8533, pp.297–305. Available at: http://download.springer.com.elib.tcd.ie/static/pdf/596/chp%253A10.1007%252F978-3-319-07620-1_26.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F978-3-319-07620-1_26&token2=exp=1488746007~acl=%2Fstatic%2Fpdf%2F596%2Fchp%25253A10.1007%25 [Accessed March 5, 2017].

Alberts, C. & Dorofee, A. 2002. Managing Information Security Risks: The OCTAVE^{SM} Approach, Addison Wesley Publishing.

American Association for Public Opinion Research, 2016. Final Dispositions of Case Codes and Outcome Rates for Surveys. Available at: http://www.aapor.org/AAPOR_Main/media/publications/Standard-Definitions20169theditionfinal.pdf [Accessed July 9, 2017].

Ashenden D. 2008. Information Security Management: A Human Challenge?, Information Security Technical Report (2008), doi: 10.1016/j.istr.2008.10.006

Ashford, W., 2016. EU data protection rules affect everyone, say legal experts. ComputerWeekly.com. Available at: http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts [Accessed April 23, 2017].

AXELOS, 2014. THE IMPORTANCE OF ITIL, A Global View. Available at: https://www.axelos.com/Corporate/media/Files/Research/The_Importance_of_ITIL_-_A_Global_View.pdf

AXELOS. 2017. What is ITIL Best Practice? AXELOS. Available at: https://www.axelos.com/best-practice-solutions/itil/what-is-itil [Accessed March 19, 2017].

Barlette, Y. & Fomin, V. V. 2009. The Adoption of Information Security Management Standards: A Literature Review. Cyber Security and Global Information Assurance (pp. 119–140). IGI Global. Available at: https://doi.org/10.4018/978-1-60566-326-5.ch006 [Accessed: 16 August 2017].

Barton, K.A., Tejay, G., Lane, M. & Terrell, S. 2016. Information system security commitment: A study of external influences on senior management. Computers & Security, 59, pp.9–25.

Barton, K.A., Tejay, G., Lane, M., & Terrell, S. 2016. Information system security commitment: A study of external influences on senior management. Computers & Security 59: p.9–25.

Björck, F., 2004. Institutional theory: A new perspective for research into IS / IT security in organisations. Available at: https://www.researchgate.net/profile/Fredrik_Bjoerck/publication/224745894_Institutional_theory_a_new_perspective_for_research_into_ISIT_security_in_organisations/links/54ec59140cf27fbfd76f7091.pdf [Accessed April 23, 2017].

BOEHMER∗, W. 2009. Cost-benefit trade-off analysis of an ISMS based on ISO 27001. International Conference on Availability, Reliability and Security. 2009

Bonner, E., O’Raw, J., & Curran, K. 2011. Implementing the Payment Card Industry (PCI) Data Security Standard (DSS), TELKOMNIKA, Vol.9, No.2, Agustus 2011, pp. 365~376. Available at: http://journal.uad.ac.id/index.php/TELKOMNIKA/article/download/1326/710.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2010. INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. MIS Quarterly Vol. 34 No. 3 pp. 523-548

Burrell, G. & Morgan, G., 1979. Sociological Paradigms and Organisational Analysis, Elements of the Sociology of Corporate Life. Heinemann Education Books.

Calder, A. 2009. Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide - Best Practice. Van Haren Publishing.

Cater-Steel, A., Toleman, M., Tan, W.G. 2006. Transforming IT Service Management – the ITIL Impact, 17th Australasian Conference on Information Systems. 6-8 Dec 2006, Adelaide.

Cherdantseva, Y., Hilton, J. 2013 A Reference Model of Information Assurance & Security. Available at: http://rmias.cardiff.ac.uk/

Chmura, J. 2016. THE IMPACT OF POSITIVE ORGANISATIONAL CULTURE VALUES ON INFORMATION SECURITY MANAGEMENT IN THE COMPANY. 7(1): p.87–98. Available at: http://dx.doi.org/ [Accessed November 27, 2016].

Coburn, A. 2010. Fitting PCI DSS within a wider governance framework. Available at: http://ac.els-cdn.com/S1361372310701214/1-s2.0-S1361372310701214-main.pdf?_tid=9c68daac-0c1f-11e7-a042-00000aacb35f&acdnat=1489871736_3a3dfc2dd922acd55ed639b964ff60bb [Accessed March 18, 2017].

Colwill, C. 2010. Human factors in information security: The insider threat - Who can you trust these days?, Inform. Secur. Tech. Rep. (2010), doi:10.1016/j.istr.2010.04.004

Coyler, A. & Clement, A. 2005. Aspect-orientated programming with AspectJ. IBM Systems Journal. 2005. 44(2): 301-308.

Crotty, M., 1998. The foundations of social research: Meaning and perspective in the research process. Sage.

Devos, J, & Van de Ginste, K 2015. Towards a Theoretical Foundation of IT Governance - The COBIT 5 case, Electronic Journal of Information Systems Evaluation, 18, 2, p. 95, Publisher Provided Full Text Searching File, EBSCOhost, viewed 19 March 2017.

Dimensional research. 2016. CYBERSECURITY FRAMEWORKS AND FOUNDATIONAL SECURITY CONTROLS CYBERSECURITY FRAMEWORKS AND FOUNDATIONAL SECURITY CONTROLS. Dimensional Research. November 2016.

Dojkovski, S., Lichtenstein, S., & Warren, M.J. 2006. CHALLENGES IN FOSTERING AN INFORMATION SECURITY CULTURE IN AUSTRALIAN SMALL AND MEDIUM SIZED ENTERPRISES. ECIW2006: proceedings of the 5th European conference on Information Warfare and Security, Academic Conferences Limited, reading, England, pp. 31-40. Available at: http://hdl.handle.net/10536/DRO/DU:30006079 [Accessed March 12, 2017].

Easton, G. 2009. Critical realism in case study research. Lancaster University Management School. Available at: https://pdfs.semanticscholar.org/0b45/912540bd97c3325da1eedb665bce6f611aaf.pdf [Accessed May 12, 2017].

European Commission. 2016. 2016 SBA Fact Sheet – Ireland. European Commission. Ref. Ares (2016) 6625664

European Commission. 2016. Reform of EU data protection rules. DG Justice and Consumers. Available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm [Accessed March 14, 2017].

European Union Agency for Network and Information Security. 2015. Information security and privacy standards for SMEs. Available at: https://www.enisa.europa.eu/publications/standardisation-for-smes

Fomin, V. V, Vries, H.J. De, Nl, hvries@rsm, & Barlette, Y. 2008. ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption. ResearchGate (September, 2008). Available at: https://www.researchgate.net/publication/228898807

Franke, U., & Brynielsson, J. 2014. Cyber situational awareness - A systematic review of the literature. Computers & Security 46: p.18–31. Available at: http://ferryas.lecturer.pens.ac.id/NetSa_Papers/Cyber situational awareness %E2%80%93 A systematic review of the literature.pdf [Accessed March 24, 2017].

Ghonaimy, M.A., El-Hadidi, M.T. & Aslan, H.K. 2002. Security in the information society. Kluwer Academic Publishers, USA.

Ghose, A. & Rajan, U., 2006. The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare. Available at: http://www.econinfosec.org/archive/weis2006/docs/37.pdf [Accessed April 23, 2017].

GONZALEZ, J.J. & SAWICKA, A., 2002. A Framework for Human Factors in Information Security. Available at: https://www.researchgate.net/profile/Jose_Gonzalez74/publication/228684288_A_framework_for_human_factors_in_information_security/links/02e7e53720ad4cfbb3000000.pdf [Accessed March 25, 2017].

Grant Thornton. 2017. General Data Protection Regulation requirements - creating, protecting and enhancing value in your business. Available at: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---gdpr.pdf [Accessed April 23, 2017]

Gray, D.E., 2009. Doing research in the real world. Second Edition. Sage.

Hinson, G. (2008). The financial implications of implementing ISO/IEC 27001 & 27002: a generic cost-benefit model, IsecT Ltd., 1-4.

Holgate, J., Williams, S.P. & Hardy, C.A., 2012. Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations. Available at: https://www.researchgate.net/profile/Susan_Williams14/publication/266506949_Information_Security_Governance_Investigating_Diversity_in_Critical_Infrastructure_Organizations/links/54747f790cf2778985abe311.pdf [Accessed March 25, 2017].

Hu, Q., Hart, P., & Cooke, D. 2007. The role of external and internal influences on information systems security – a neo-institutional perspective. Journal of Strategic Information Systems 16: p.153–172. Available at: www.elsevier.com/locate/jsis [Accessed March 22, 2017].

Humphreys, E. 2011. Information Security Management System Standards. Datenschutz und Datensicherheit - DuD, January 2011, Volume 35, Issue 1, pp 7–11. Available at: https://link.springer.com/article/10.1007/s11623-011-0004-3

Humphreys, E. 2011. Information Security Management System Standards.

Humphreys, T. 2006. State-of-the-art information security management system with ISO/IEC 27001:2005. ISO Management Systems, 15-18.

IBM. 2015. IBM 2015 Cyber Security Intelligence Index. IBM. Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=SEJ03278USEN&attachment=SEJ03278USEN.PDF&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US [Accessed March 26, 2017].

Imszennik, J. 2016. ISO 27001: Role of Top Management and Its Importance. Schellman. Available at: https://www.schellmanco.com/blog/2016/01/iso-27001-role-of-top-management/

ISACA. 2017. COBIT FAQs. Available at: http://www.isaca.org/knowledge-center/cobit/pages/faq.aspx#1[Accessed March 19, 2017].

ISO. 2013. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

ISO. 2016. ISO/IEC 27001 Information security management. Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed March 15, 2017].

IT Governance Institute. 2007. COBIT 4.1 Excerpt. Rolling Meadows, IL 60008 USA. Available at: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

IT Governance. 2013. INFORMATION SECURITY & ISO 27001. IT Governance Ltd. Available at: http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf [Accessed March 15, 2017].

IT Governance. 2016. ISO 27001 Global Report 2016. Available at: www.itgovernance.co.uk [Accessed November 26, 2016].

IT Governance. 2017. ISO 27001 Risk Assessments. IT Governance Ltd. Available at: https://www.itgovernance.co.uk/iso27001/iso27001-risk-assessment [Accessed March 18, 2017]

Johnson, P. & Clark, M., 2006. Business and Management Research Methodologies. Sage Publications Ltd.

Kajava, J., Varonen, R., Anttila, J., Savola, R. & Roning, J. 2006. Senior Executives Commitment to Information Security -from Motivation to Responsibility. Available at: http://www.ee.oulu.fi/research/bisg/files/pdf/pdf_1013.pdf [Accessed April 17, 2017].

Kerr, D.S., & Murthy, U.S. 2007.The Importance of the COBIT Framework IT Processes For Effective Internal Control over the Reliability of Financial Reporting: An International Survey. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.178.6513&rep=rep1&type=pdf [Accessed March 19, 2017].

Khyavi, M.H. & Rahimi, M. 2015. The Missing Circle of ISMS (LL-ISMS). Available at: http://dl.acm.org/citation.cfm?id=2751972 [Accessed March 12, 2017].

Klahr, R., Amili, S., Shah, J.N., Button, M., & Wang, V. 2016. Cyber Security Breaches Survey 2016. Department for Culture (UK Government), Media & Sport 2016. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf [Accessed March 12, 2017].

Knapp, K.J., Marshall, T.E., Rainer, R.K., & Morrow, D.W. 2006. The Top Information Security Issues Facing Organizations: What Can Government Do to Help? Available at: http://www.infosectoday.com/Articles/topissues.pdf [Accessed March 21, 2017].

Kraemer, S., Carayon, P. & Clem, J., 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Comput. Secur. (2009), doi:10.1016/j.cose.2009.04.006

Lee, N. & Lings, I., 2008. Doing business research: a guide to theory and practice. Sage Publications Ltd.

Li, C., Lim, J.H., & Wang, Q. 2007. Internal and external influences on IT control governance. International Journal of Accounting Information Systems 8 (2007) 225-239

Liang, H., Saraf, N., Hu, Q., & Xue, Y., 2007. Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. Source: MIS Quarterly, 31(1), pp.59–87. Available at: http://works.bepress.com/qing_hu/40 [Accessed April 23, 2017].

Ma, Q., Schmidt, M.B. & Pearson J.M. 2009. An Integrated Framework for Information Security Management, Review of Business, St. John’s University, 30(1), 58-69.

McFadzean, E., Ezingeard, J. N. & Birchall, D. 2006. ANCHORING INFORMATION SECURITY GOVERNANCE RESEARCH: SOCIOLOGICAL GROUNDINGS AND FUTURE DIRECTIONS. Available at: https://www.researchgate.net/profile/Elspeth_Mcfadzean/publication/38176020_Anchoring_information_security_governance_research_Sociological_groundings_and_future_directions/links/0c960522450afa33ba000000.pdf [Accessed March 20, 2017].

Neuman, L.W., 2011. Social research methods: Qualitative and quantitative approaches: Seventh Edition. Pearson.

Nugroho, H. 2014. CONCEPTUAL MODEL OF IT GOVERNANCE FOR HIGHER EDUCATION BASED ON COBIT 5 FRAMEWORK. Journal of Theoretical and Applied Information Technology 20(602). Available at: www.jatit.org [Accessed March 19, 2017].

Onwubiko, C. and Lenaghan, A.P., 2009. Challenges and complexities of managing information security. *International Journal of Electronic Security and Digital Forensics*, *2*(3), pp.306-321.

Orlikowski, W. & Baroudi, J.J. 1990. STUDYING INFORMATION TECHNOLOGY IN ORGANIZATIONS: RESEARCH APPROACHES AND ASSUMPTIONS. Centre for Research on Information Systems, Information Systems Department, New York

University. Available at: https://archive.nyu.edu/jspui/bitstream/2451/14404/1/IS-90-04.pdf [Accessed May 11, 2017].

Palthe, J., 2014. Regulative, Normative, and Cognitive Elements of Organizations: Implications for Managing Change. Management and Organizational Studies, 1(2), pp.59–66. Available at: http://www.sciedu.ca/journal/index.php/mos/article/view/4666.

Pansiri, J., 2005. Pragmatism: A methodological approach to researching strategic alliances in tourism. Tourism and Hospitality Planning & Development, 2(3), pp.191-206.

Papadakis, V.M., Lioukas, S., & Chambers, D. 1998. Strategic Decision-Making Process: The Role of Management and Context, Strategic Management Journal, Vol.19, No.2 (Feb., 1998), pp115-147 Available at: http://www.aueb.gr/Users/papadakis/articles/academic/SMJ_Paper_Papadakis.pdf

Parker, C.B. 2017. Insider threats often ignored, FSI, Stanford. Available at: http://cisac.fsi.stanford.edu/news/insider-threats-often-ignored [Accessed March 26, 2017].

Peppard, J. 2007. The conundrum of IT management*. European Journal of Information Systems 16: p.336–345. Available at: http://ai2-s2-pdfs.s3.amazonaws.com/fb46/bcf97dc64b6824e5f1a039f3df0c28424ec5.pdf [Accessed March 11, 2017].

Pfleeger, S. L. & Stolfo, S. J. 2009. Addressing the Insider Threat, IEEE Computer and Reliability Societies. Available at: http://ids.cs.columbia.edu/sites/default/files/10-13.pdf [Accessed March 26, 2017].

Ponemon Institute. 2015. 2015 Cost of Data Breach Study: United Kingdom, IBM Security. Available at: http://www-03.ibm.com/security/data-breach/

Public Company Accounting Oversight Board (PCAOB). 2004. An Audit of Internal Control over Financial Reporting Performed in Conjunction With an Audit of Financial Statements. Public Company Accounting Oversight Board. Available at: https://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_2.aspx [Accessed April 23, 2017]

Radhakrishnan, S. 2015. COBIT Helps Organizations Meet Performance and Compliance Requirements, COBIT Focus, pp. 1-5, Business Source Complete, EBSCOhost, viewed 19 March 2017.

Raggad, B.G., 2010. Information security management: concepts and practice. CRC Press.

Ramsey, DB. 2016, DATA SECURITY: EVOLVING LEGAL DUTIES AND CHALLENGES FOR FRANCHISE SYSTEMS, Journal Of Internet Law, 20, 3, pp. 3-17, Business Source Complete, EBSCOhost, viewed 18 March 2017.

Ring, Tim. 2013. A breach too far? Computer Fraud & Security, 2013(6), 5–9. Available online 13 June 2013. Available at: http://www.sciencedirect.com/science/article/pii/S1361372313700526

Rocha Flores, W., Antonsen, E., & Ekstedt, M. 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security 43: p.90–110.

Sahibudin, S., Sharifi, M., & Ayat, M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. Second Asia International Conference on Modelling & Simulation. Available at: http://users.du.se/~h13freog/IK2014/04530569.pdf [Accessed March 19, 2017].

Sallé, M. 2004. IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing. Available at: http://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf [Accessed March 19, 2017].

Sarbanes-Oxley Act. 2002. Sarbanes-Oxley Act of 2002. Available at: http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf. [Accessed: 17 August 2017].

Saunders, M., Lewis, P. & Thornhill, A., 2016. Research methods for business students, seventh edition, Pearson Education.

Sayer, A., 2010. Method in Social Science: Revised 2nd Edition. Routledge.

Sharma, N., & Dash, P.K. 2012. Effectiveness of ISO 27001, as An Information Security Management System: An Analytical Study of Financial Aspects. Far East Journal of Psychology and Business 9(3): p.42–55.

Soomro, Z.A., Shah, M.H., & Ahmed, J. 2015. Information security management needs more holistic approach: A literature review. International Journal of Information Management 36(2): p.215–225.

SurveyMonkey. 2016. Privacy Policy | SurveyMonkey. Available at: https://www.surveymonkey.com/mp/policy/privacy-policy/ [Accessed May 23, 2017].

SurveyMonkey. 2017. Sample Size Calculator. SurveyMonkey. Available at: https://www.surveymonkey.com/mp/sample-size-calculator/ [Accessed June 15, 2017]

Susanto, H., Almunawar, M.N., & Tuan, Y.C. 2011. Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS 11(23): p.113505–6969.

The Economic Times. 2017. Global information security spending to hit $86.4 billion: Gartner. Available at: http://economictimes.indiatimes.com/tech/ites/global-information-security-spending-to-hit-86-4-billion-gartner/articleshow/60083744.cms [Accessed: 16 August 2017].

Udo, G.J. Privacy and security concerns as major barriers for e-commerce: a survey study, Information Management & Computer Security 9/4 [2001] 165-174, MCB University Press.

Ukidve, A., Smantha, D.S., & Tadvalkar, M. 2017. Analysis of Payment Card Industry Data Security Standard [PCI DSS] Compliance by Confluence of COBIT 5 Framework. Journal of Engineering Research and Application www.ijera.com ISSN 7(11): p.2248–962242. Available at: http://www.ijera.com/papers/Vol7_issue1/Part-1/H0701014248.pdf [Accessed March 18, 2017].

Van Kessel, P. 2012. Fighting to close the gap Key findings from EY's Global Information Security Survey 2012. Available at: http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf [Accessed March 21, 2017].

Van Zadelhoff, M., 2016. The Biggest Cybersecurity Threats Are Inside Your Company, Harvard Business Review. Available at: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company [Accessed March 26, 2017].

Walsham, G., 2001, The Emergence of Interpretivism in IS Research. The Management School, University of Lancaster. Available at: http://gkmc.utah.edu/7910F/papers/ISR%20emergence%20of%20interpretivism%20in%20IS%20research.pdf [Accessed May 12, 2017]

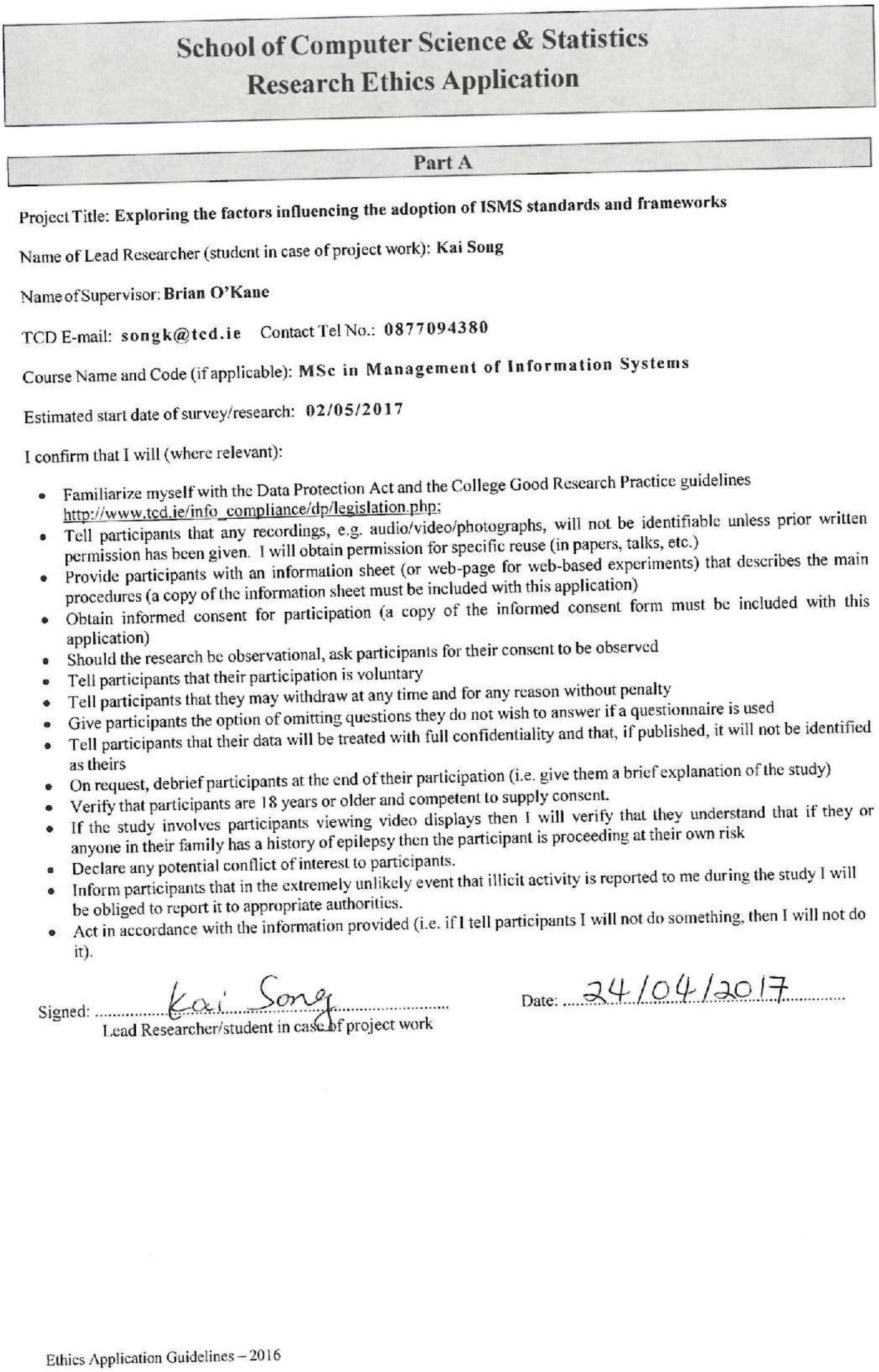
Werlinger, R., Hawkey, K. & Beznosov, K. 2009. An integrated view of human, organizational, and technological challenges of IT security management.

Information Management & Computer Security Vol. 17 No. 1, 2009 pp. 4-19. Available at: http://ai2-s2-pdfs.s3.amazonaws.com/eeae/67445a628743b0f6ed0371d7c44e59aaf1dc.pdf [Accessed March 26, 2017].

Whitman, M.E. 2004. In defense of the realm: understanding the threats to information security. International Journal of Information Management 24(1): p.43–57. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0268401203001282 [Accessed March 22, 2017].

Appendices

Appendix A: Ethics Approval



School of Computer Science & Statistics
Research Ethics Application

Part A

Project Title: **Exploring the factors influencing the adoption of ISMS standards and frameworks**

Name of Lead Researcher (student in case of project work): **Kai Song**

Name of Supervisor: **Brian O'Kane**

TCD E-mail: **songk@tcd.ie** Contact Tel No.: **0877094380**

Course Name and Code (if applicable): **MSc in Management of Information Systems**

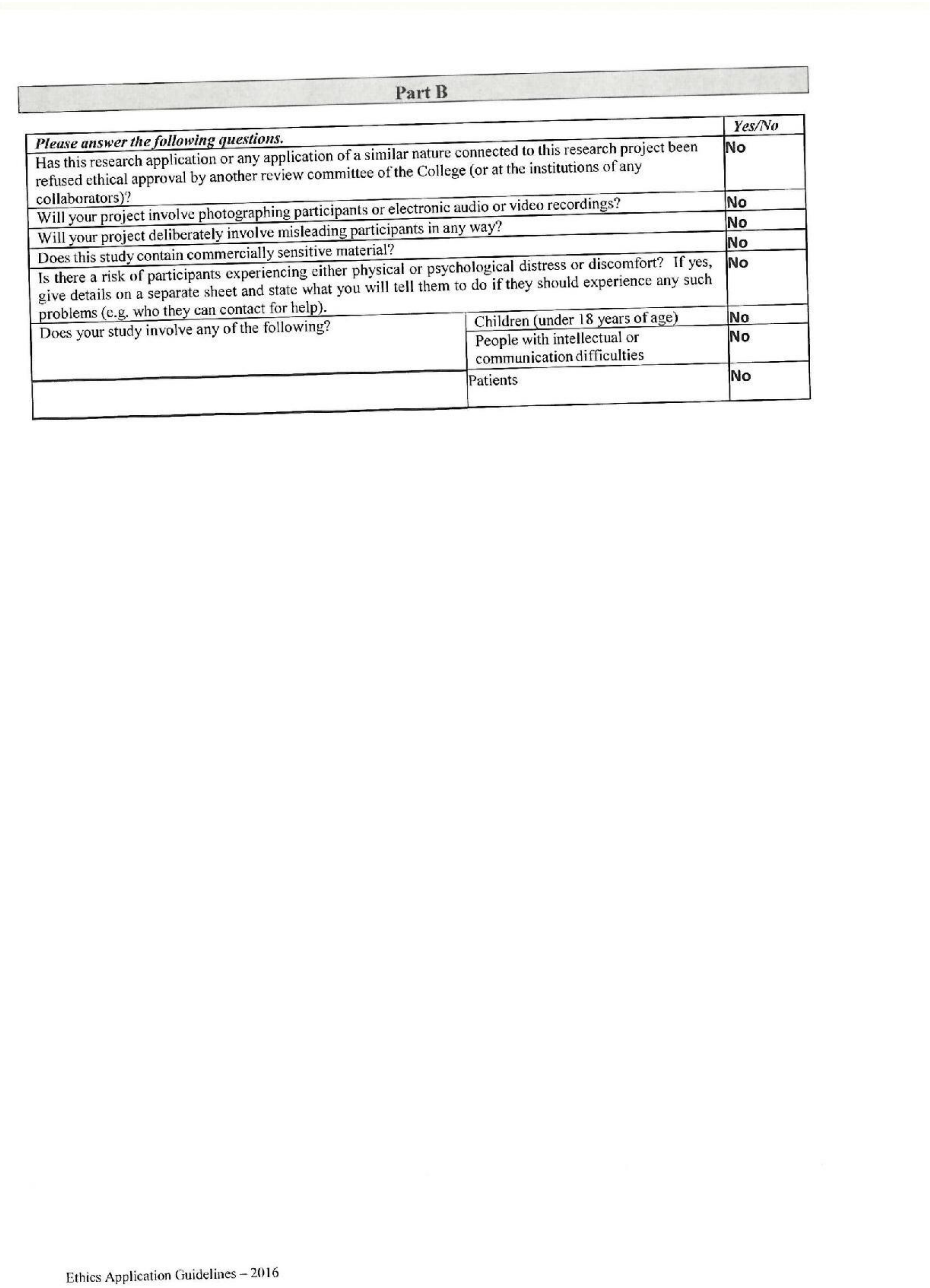
Estimated start date of survey/research: **02/05/2017**

I confirm that I will (where relevant):

- Familiarize myself with the Data Protection Act and the College Good Research Practice guidelines http://www.tcd.ie/info_compliance/dp/legislation.php;
- Tell participants that any recordings, e.g. audio/video/photographs, will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (in papers, talks, etc.)
- Provide participants with an information sheet (or web-page for web-based experiments) that describes the main procedures (a copy of the information sheet must be included with this application)
- Obtain informed consent for participation (a copy of the informed consent form must be included with this application)
- Should the research be observational, ask participants for their consent to be observed
- Tell participants that their participation is voluntary
- Tell participants that they may withdraw at any time and for any reason without penalty
- Give participants the option of omitting questions they do not wish to answer if a questionnaire is used
- Tell participants that their data will be treated with full confidentiality and that, if published, it will not be identified as theirs
- On request, debrief participants at the end of their participation (i.e. give them a brief explanation of the study)
- Verify that participants are 18 years or older and competent to supply consent.
- If the study involves participants viewing video displays then I will verify that they understand that if they or anyone in their family has a history of epilepsy then the participant is proceeding at their own risk
- Declare any potential conflict of interest to participants.
- Inform participants that in the extremely unlikely event that illicit activity is reported to me during the study I will be obliged to report it to appropriate authorities.
- Act in accordance with the information provided (i.e. if I tell participants I will not do something, then I will not do it).

Signed: ....Kai Song.... Date: ....24/04/2017....
Lead Researcher/student in case of project work

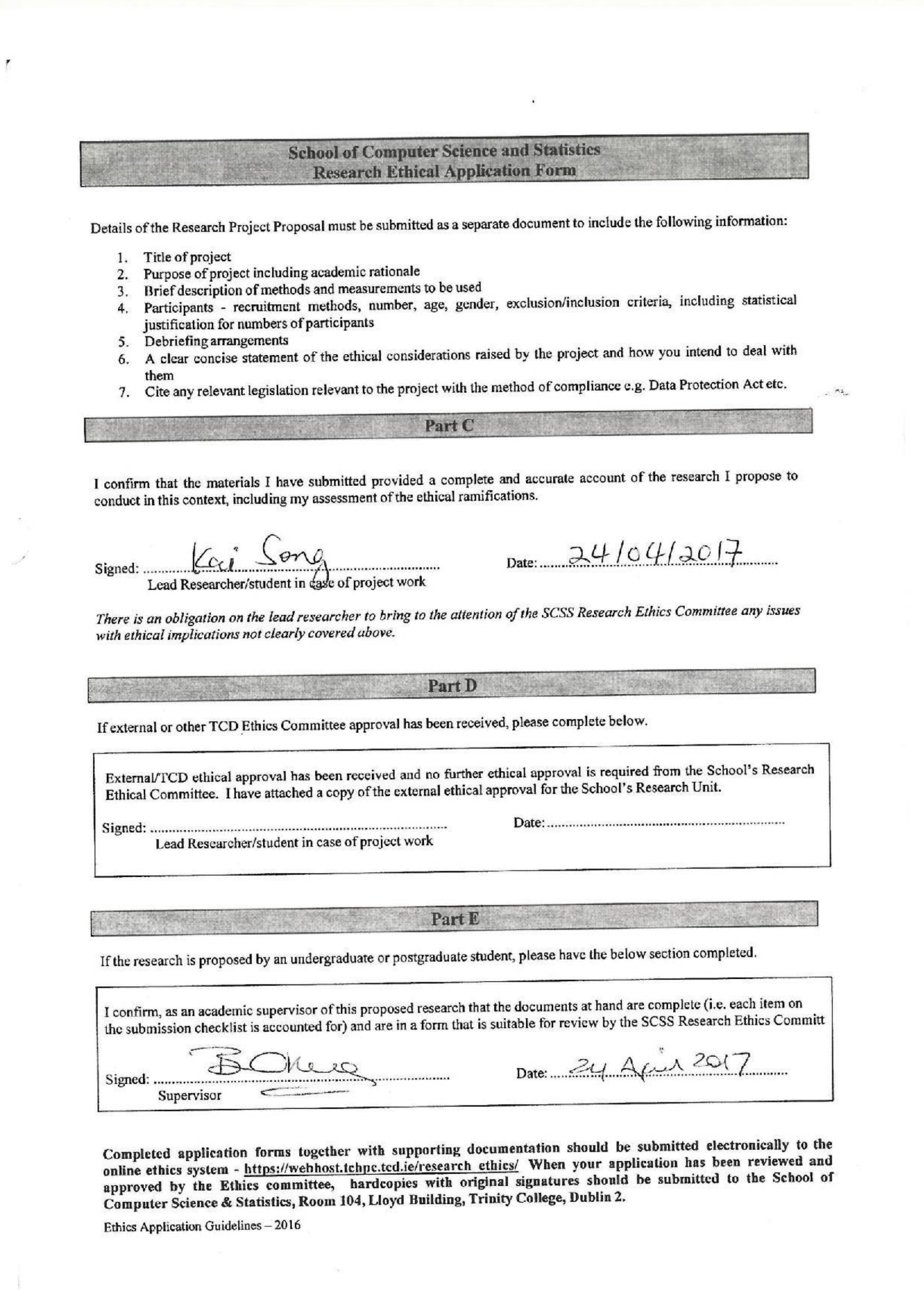
Ethics Application Guidelines – 2016



Part B

Please answer the following questions.		*Yes/No*
Has this research application or any application of a similar nature connected to this research project been refused ethical approval by another review committee of the College (or at the institutions of any collaborators)?		No
Will your project involve photographing participants or electronic audio or video recordings?		No
Will your project deliberately involve misleading participants in any way?		No
Does this study contain commercially sensitive material?		No
Is there a risk of participants experiencing either physical or psychological distress or discomfort? If yes, give details on a separate sheet and state what you will tell them to do if they should experience any such problems (e.g. who they can contact for help).		No
Does your study involve any of the following?	Children (under 18 years of age)	No
	People with intellectual or communication difficulties	No
	Patients	No

Ethics Application Guidelines – 2016



School of Computer Science and Statistics
Research Ethical Application Form

Details of the Research Project Proposal must be submitted as a separate document to include the following information:

1. Title of project
2. Purpose of project including academic rationale
3. Brief description of methods and measurements to be used
4. Participants - recruitment methods, number, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants
5. Debriefing arrangements
6. A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them
7. Cite any relevant legislation relevant to the project with the method of compliance e.g. Data Protection Act etc.

Part C

I confirm that the materials I have submitted provided a complete and accurate account of the research I propose to conduct in this context, including my assessment of the ethical ramifications.

Signed: Kai Song
Lead Researcher/student in case of project work

Date: 24/04/2017

There is an obligation on the lead researcher to bring to the attention of the SCSS Research Ethics Committee any issues with ethical implications not clearly covered above.

Part D

If external or other TCD Ethics Committee approval has been received, please complete below.

External/TCD ethical approval has been received and no further ethical approval is required from the School's Research Ethical Committee. I have attached a copy of the external ethical approval for the School's Research Unit.

Signed: ....
Lead Researcher/student in case of project work

Date: ....

Part E

If the research is proposed by an undergraduate or postgraduate student, please have the below section completed.

I confirm, as an academic supervisor of this proposed research that the documents at hand are complete (i.e. each item on the submission checklist is accounted for) and are in a form that is suitable for review by the SCSS Research Ethics Committ

Signed: ....
Supervisor

Date: 24 April 2017

Completed application forms together with supporting documentation should be submitted electronically to the online ethics system - https://webhost.tchpc.tcd.ie/research_ethics/ When your application has been reviewed and approved by the Ethics committee, hardcopies with original signatures should be submitted to the School of Computer Science & Statistics, Room 104, Lloyd Building, Trinity College, Dublin 2.

Ethics Application Guidelines – 2016

Appendix B: Information Sheet for Participants

TRINITY COLLEGE DUBLIN

INFORMATION SHEET FOR PROSPECTIVE PARTICIPANTS

Research Title:

Exploring the factors influencing the adoption of ISMS standards or frameworks

Lead Researcher:

Kai Song – Trinity College Dublin, School of Computer Science & Statistics

Supervisor:

Brian O'Kane – Trinity College Dublin, School of Computer Science & Statistics

Lead Researcher Contact Details:

Name: Kai Song

Phone: +353 (0) 87 709 4380

Email: songk@tcd.ie

Expect Duration of the Research:

The expected duration of this research is between May to August 2017.

Background to the Research:

In the world of new technologies, information is often regarded as the lifeblood of business: it is a key corporate resource and it must be managed effectively, in a proactive manner, to ensure organisational competencies. The rapid development of new technologies has increased business opportunities; it has also caused information security issues, such as data breach, consumer privacy issue, identity theft and other online threats, which have been deemed a top priority on senior management's agenda. As a result of the continued escalation of cyber-attacks and the increasingly regulated data protection landscape, it is imperative for organisations to establish, implement and maintain an effective Information Security Management System (ISMS) to manage their information assets. An ISMS is a set of policies and procedures defined by an organisation for systematically managing sensitive information to ensure that the principle of confidentiality, integrity and availability is adhered to.

The intense global competition and highly digital information-dependent business drive organisations to optimise and standardise their information security management processes. Since 1990 many institutions have published ISMS standards and frameworks as best practices for implementing and maintaining information security, such as ISO

27001, COBIT, ITIL, and PCI DSS. The benefits of adopting these standards and frameworks are evident. However, these standards and frameworks are, in fact, not well adopted.

This research proposes to examine factors influencing the adoption of ISMS standards and frameworks. This research will also try to identify challenges and barriers of adopting ISMS standards and frameworks within organisations. An overview of management perceptions and concerns will be presented in this research.

The Procedures relevant to the participant within this particular study:

The lead researcher invites you to participate in this research based on the fact that you are an ICT professional. You can keep a copy of this information sheet for your records. You are also required to read and agree to the terms and conditions in the accompanying Participant Consent Form. It is important to advise that your participation is voluntary, confidential and you can withdraw from this research at any time and for any reason without penalty.

In the research, you will be requested to complete a set of questionnaires in an anonymous online survey which should not be more than 15 minutes. Each question is optional. Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised. Data will only be collected through an anonymous online survey. No interviews, recordings or videos will be required. It will be appreciated if all questions are completed. However, do feel free to omit any question you are unwilling to complete as there is no penalty whatsoever. The topics covered in the questionnaires include, but not limited to, company profile (company name is not required), interviewee profile (interviewee name, contact details and any other personally identifiable information are not required), information security environment, challenges and barriers of adopting ISMS standards or frameworks, benefits of adopting ISMS standards or frameworks, and plans for future.

All information obtained will be treated confidentially and no name of individuals or organisations will be saved in any format throughout the process. All the data collected from online survey will be encrypted and kept on the lead researcher’s laptop until September 30th 2017. The lead researcher’s laptop will be locked in a personal drawer in the secured building of Castleforbes Square (Dublin 1). Only the lead researcher has the access to the laptop and the data collected from online survey. All the data collected will be destroyed after September 30th 2017.

There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

Please note the following:

- You must be 18 years or older to participate in the research.
- No risks to you have been identified as a result of your participation in the research. However, you have the right to withdraw from the research at any time and for any reason without penalty.
- All information collected through the online survey is completely anonymous and not traceable to respondents.
- No interviews, recordings or videos will be required.
- High level encryption and password will be deployed on media containing data collected for this research.
- Data collected for this research will be used exclusively for academic purposes and in support of the MSc in Management of Information Systems.
- Data collected will be retained on the lead researcher’s laptop until September 30th 2017 and will be destroyed after September 30th 2017.
- Data collected will only be retained for this research and in line with due processes as stipulated by the Ethics Committee of the School of Computer Science and Statistics, Trinity College Dublin.

Conflict of Interest:

This research is conducted in partial fulfilment of Kai Song's MSc in Management of Information Systems, to be awarded by the School of Computer Science and Statistics, Trinity College Dublin.

I have no conflict of interest in relation to the topics covered in the research or in relation to any individual or organisation contributing to the research.

Publication:

The information gathered from online survey will form the basis of the analysis and findings section in the completed research. This research will subsequently be stored on Trinity College Dublin's database and can be accessed through normal publication procedures.

By participating in this research, you agree that this data may be used for such scientific purpose, and that you have no objection that the data is published in research and scientific publications in a way that does not reveal your specific identity.

A completed copy of the research can be made available to you upon request. Should you wish to clarify any aspect of the research processes please feel free to contact me.

Relevance:

Your participation in this research will enable us to understand the factors influencing the adoption of ISMS standards and frameworks. The information gathered from responses to this questionnaire will be used to create a foundation for further development of information security studies.

Further Information:

If you have further queries regarding this research or would like to have more detailed information, please feel free to contact me without hesitation.

Thank you for participating.

Kai Song

Email: songk@tcd.ie

School of Computer Science and Statistics,

Trinity College Dublin

Dublin, April 2017

Appendix C: Informed Consent Form

TRINITY COLLEGE DUBLIN

INFORMEDCONSENTFORM

RESEARCH TITLE:

Exploring the factors influencing the adoption of ISMS standards or frameworks

LEAD RESEARCHERS:

Kai Song – Trinity College Dublin, School of Computer Science and Statistics

BACKGROUND OF RESEARCH:

In the world of new technologies, information is often regarded as the lifeblood of business: it is a key corporate resource and it must be managed effectively, in a proactive manner, to ensure organisational competencies. The rapid development of new technologies has increased business opportunities; it has also caused information security issues, such as data breach, consumer privacy issue, identity theft and other online threats, which have been deemed a top priority on senior management's agenda. As a result of the continued escalation of cyber-attacks and the increasingly regulated data protection landscape, it is imperative for organisations to establish, implement and maintain an effective Information Security Management System (ISMS) to manage their information assets. An ISMS is a set of policies and procedures defined by an organisation for systematically managing sensitive information to ensure that the principle of confidentiality, integrity and availability is adhered to.

The intense global competition and highly digital information-dependent business drive organisations to optimise and standardise their information security management processes. Since 1990 many institutions have published ISMS standards and frameworks as best practices for implementing and maintaining information security, such as ISO 27001, COBIT, ITIL, and PCI DSS. The benefits of adopting these standards and frameworks are evident. However, these standards and frameworks are, in fact, not well adopted.

This research proposes to examine factors influencing the adoption of ISMS standards and frameworks. This research will also try to identify challenges and barriers of adopting ISMS standards and frameworks within organisations. An overview of management perceptions and concerns will be presented in this research.

PROCEDURES OF THIS STUDY:

The lead researcher invites you to participate in this research based on the fact that you are an ICT professional. You are required to read and agree to the terms and conditions in the Participant Consent Form. It is important to advise that your participation is voluntary, confidential and you can withdraw from this research at any time and for any reason without penalty.

In the research, you will be requested to complete a set of questionnaires in an anonymous online survey which should not be more than 15 minutes. Each question is optional. Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised. Data will only be collected through an anonymous online survey. No interviews, recordings or videos will be required. It will be appreciated if all questions are completed. However, do feel free to omit any question you are unwilling to complete as there is no penalty whatsoever. The topics covered in the questionnaires include, but not limited to, company profile (company name is not required), interviewee profile (interviewee name, contact details and any other personally identifiable information are not required), information security environment, challenges and barriers of adopting ISMS standards or frameworks, benefits of adopting ISMS standards or frameworks, and plans for future.

All information obtained will be treated confidentially and no name of individuals or organisations will be saved in any format throughout the process. All the data collected from online survey will be encrypted and kept on the lead researcher's laptop until September 30th 2017. The lead researcher's laptop will be locked in a personal drawer in the secured building of Castleforbes Square (Dublin 1). Only the lead researcher has the access to the laptop and the data collected from online survey. All the data collected will be destroyed after September 30th 2017.

There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

CONFLICT OF INTEREST:

This research is conducted in partial fulfilment of Kai Song's MSc in Management of Information Systems, to be awarded by the School of Computer Science and Statistics, Trinity College Dublin.

The lead researcher has no conflict of interest in relation to the topics covered in the research or in relation to any individual or organisation contributing to the research.

PUBLICATION:

The information gathered from online survey will form the basis of the analysis and findings section in the completed research. This research will subsequently be stored on Trinity College Dublin's database and can be accessed through normal publication procedures.

By participating in this research, you agree that this data may be used for such scientific purpose, and that you have no objection that the data is published in research and scientific publications in a way that does not reveal your specific identity.

A completed copy of the research can be made available to you upon request. Should you wish to clarify any aspect of the research processes please feel free to contact the lead researcher.

Individual results may be aggregated anonymously and research reported on aggregate results.

DECLARATION:

I am 18 years or older and am competent to provide consent.

I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.

In the extremely unlikely event that illicit activity is reported I will be obliged to report it to appropriate authorities.

I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.

I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.

I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.

As the survey is web-based, I understand that if I or anyone in my family has a history of epilepsy then I am proceeding at my own risk.

I understand that my participation is fully anonymous and that no personal details about me will be recorded.

I have received a copy of this agreement.

☐ I accept the terms and conditions in the form

☐ I do not accept the terms and conditions in the form

Statement of investigator's responsibility: The lead researcher has explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. The lead researcher has offered to answer any questions and fully answered such questions. The lead researcher believes that the participant understands his explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS:

Kai Song (songk@tcd.ie)

Phone: +353 (0) 87 709 4380

INVESTIGATOR'S SIGNATURE:

Date:

Appendix D: Online Survey Questions

Research Questionnaire

Before you start the survey, please note the following:

Each question is optional

In the extremely unlikely event that illicit activity is reported, please report it to appropriate authorities

To ensure replies are anonymised, please do not name third parties in any open text field of the questionnaire

Part 1 Company Profile

1. What is your company's business sector?

	Financial Services
	IT/Technology
	Manufacturing
	Insurance
	Consumer Goods
	Other

If other, please specify:

2. How many full time employees in your company?

	Less than 100
	101-500
	501-1000
	1001-2000
	2000+

3. Who are the key stakeholders for making ICT decisions in your company?

	CIO or CTO (Globally or Locally)
	ICT Director
	ICT Manager
	Other

If other, please specify:

Part 2 Interviewee Profile

4. What is your job title?

	CIO or CTO (Globally or Locally)
	ICT Director
	ICT Manager
	IT Consultant
	Compliance Manager
	Other

If other, please specify:

5. How many years of experience do you have in ICT management?

	Less than 5
	6-10
	11-20
	20+

Part 3 Information Security Environment

6. Has your company implemented a formalised Information Security Management System (ISMS)?

	Yes
	No

7. Who manages the ISMS in your company?

	ISMS Manager
	ICT Director
	ICT Manager
	CIO or CTO
	Outsourced to a third party
	Other

If other, please specify:

8. Has your company adopted any of ISMS standards or frameworks?

	Yes
	No, but we are in progress
	No, but we might in the near future
	No, and we are not planning to adopt any of ISMS standards or frameworks

9. Which of the following ISMS standards or frameworks have been adopted/are in implementation in your company?

	ISO 27001

	ISO 27032
	ISO 27018 (Cloud)
	COBIT
	PCI DSS
	ITIL
	Cyber Essentials
	NIST Cyber security framework
	CIS Critical Security Controls
	Other

If other, please specify:

10. What do you think about on average the costs of the whole ISMS standard/s or framework/s adoption process including the costs of obtaining certification/s?

	Very high
	High
	Neutral
	Low
	Very low
	I don’t know

11. What are the main driver/s for adopting ISMS standard/s or framework/s in your company? Please choose all that apply.

	To ensure regulatory compliance
	To meet contractual requirements
	To meet business needs
	Required when tendering
	To improve information security posture
	To gain a competitive advantage
	To improve stakeholders’ confidence when running business
	Other

If other, please specify:

12. Have you used any services of external consultants for adopting ISMS standard/s or framework/s including obtaining certification/s?

	Yes, mostly external
	Yes, mixed resources
	No
	I don’t know

Part 4 Challenges and barriers of adopting ISMS standards or frameworks

13. Did you have any difficulties in choosing suitable ISMS standard/s or framework/s in your company?

	No, we had no difficulties
	Yes, there are too many ISMS standards or frameworks related to our business
	Yes, there are very few ISMS standards or frameworks related to our business
	Other

If other, please specify:

14 Which of the following were the main barriers in the process of adopting ISMS standard/s or framework/s in your company? Please choose all that apply.

	Understanding the standard
	Defining the scope
	Identifying required controls
	Creating and managing the ISMS documentation
	Reporting and maintaining the ISMS
	Conducting Risk Assessment
	Budget constraints
	Senior management support
	Business support
	Cultural change within organisation
	Change resistance
	Skilled resources
	Obtaining employee buy-in or raising staff awareness
	Project management
	Leadership and engagement of staff
	Obtaining certification to the standard
	Seeking external consultant services
	Other

If other, please specify:

15. Which of the following do you think has been the biggest challenge to convince the board to implement ISMS standards or frameworks? Please only choose one.

	Securing sufficient budget allowance
	Addressing the importance of the adoption
	Ensuring the engagement of skilled staff
	Agreement on project plan
	Other
	We had no challenges

If other, please specify:

16. Which of the following classifications of controls under the adopted ISMS standard/s or framework/s is your most concern? Please choose all that apply.

	Security policy
	Assets classification and control
	Security administration
	Logical access control
	Physical access control
	Change management
	System development and maintenance
	Business continuity management
	Compliance
	Other

If other, please specify:

Part 5 Benefits of adopting ISMS standards or frameworks

17. Do you think security breaches can be prevented by adopting ISMS standard/s or framework/s?

	Yes
	No
	I don’t know

18. What is the most important benefit that the adoption of ISMS standard/s or framework/s has brought to your company? Please only choose one from the following.

	Improved stakeholders’ confidence on information security
	Improved information security across the company
	Structured information security management
	Improved competitiveness
	Improved staff information security awareness
	Improved reputation
	Increased external customer satisfaction
	Increased new business opportunities
	Cost savings through reduction in security incidents
	Other

If other, please specify:

19. What is the most important benefit that the adoption of ISMS standard/s or framework/s has brought to your ICT team? Please only choose one from the following.

	Strategic projects management

	Structured ICT management
	Reduced costs
	Improved ICT staff security awareness
	Other

If other, please specify:

Part 6 Plans for the future

20. What are the main reason/s why your company has not adopted any of ISMS standards or frameworks?

	Lack of senior management support
	Lack of specialised staff or lack of related knowledge
	Implementation is too costly
	Implementation is too complex and we need to commit too many resources
	It takes too long time to implement
	I am not aware of any of these ISMS standards or frameworks
	I don't think my company will benefit from the certification since we already have a good security management
	The existing standards are not relevant to our business
	Other

If other, please specify:

21. In which ways do you think could the existing ISMS standards and frameworks, as well as their adoption process, be further improved to increase their adoption rate?

	Increasing awareness
	Reducing the total cost
	Reducing the complexity of standard requirements
	Providing more detailed guidance
	Other

If other, please specify:

Thanks for helping out with our survey. We appreciate your feedback. Do you want to submit your answers?

	Yes, submit
	No, not submit, exit without submitting