ANALYSIS OF ISO 27001 COMPLIANCE IN TONGA ORGANISATIONS INFORMATION SECURITY.

Siumafua –i- Telvavivi Moala

A thesis submitted to the faculty of design and creative technologies
AUT University
In partial fulfilment of the requirements for the
Master of information security and digital forensics

School of Computing and Mathematical Sciences

Auckland, New Zealand
2020

DECLARATION

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

....

Signature

ACKNOWLEDGEMENTS

First and foremost, I would like to thank God for his kindness, mercies and guidance in my life and my family despite our many shortcomings.

Second, I would like to express my sincere gratitude to the New Zealand government for agreeing to fund my study and for all the staff at the AUT scholarship office for their kindness and continuous support.

Third, I would like to express my sincere thanks and gratitude to my supervisor, Prof. Brian Cusack, for not only agreeing to supervise this work but also for his guidance and continuous support. Without his advice and help, this work would not have been possible.

Finally, I would like to express my sincere thanks and gratitude to my daughter and her husband for looking things at home in Tonga and to my son, his wife and kids and my brothers and all families here in New Zealand for their help and support during my time here in New Zealand.

Malo ‘Aupito.
Tēnā rawa atu koe.
Thank you very much.

ABSTRACT

Information security is a critical issue today. According to Cisco (2019), the increasingly popular services such as “e-commerce, mobile payments, cloud computing, Big Data and analytics, IoT, AI, machine learning, and social media”, all increase cyber risks for users and businesses (p.16). Further compounding, the seriousness of information security threats is the increasing number of exploitable vulnerabilities found in most systems today. According to Katos et al. (2019), there were 2377 exploitable vulnerabilities or 8.65% of the total vulnerabilities identified in the study, that were found in mobile communication systems in 2018 and half of 2019. Vulnerabilities are found in systems in all business sectors, including critical sectors like energy, financial, and health. That is the challenge that many organisations faced today; how to effectively protect their information assets given the information security threats they are facing.

From the Tonga organisations’ perspective, information security became critical after the launching of the submarine cable in 2013. The submarine cable brought unprecedented change to the ICT services risk profile. The submarine cable not only lowers the cost of ICT services dramatically but also facilitates the launching of the 3G and 4G services in the country. While affordable ICT services mean more people and organisations take advantage of the services, unfortunately, the majority lack awareness of the information security threats that come with those technologies. Therefore, the majority are unprepared to protect their systems and the confidentiality, integrity and availability of their information.

Accordingly, this study aims to investigate the question “Is the holistic approach provided by ISO 27001 the best approach for Tonga organisations, given their unique organisational factors and threat environment, to establish effective information security?” In light of findings by recent information security studies, this study theorises that implementing ISO 27001 is the best approach (compared to ad-hoc approaches) for Tonga organisations to improve their information security and to protect their information against known and unknown information security threats.

The most direct method to answer the research question is to compare the information security of organisations who have implemented ISO 27001, against those who have not. However, time limitation and the lack of organisations in Tonga who have implemented ISO 27001 prevented the researcher from doing the direct approach to the study. Instead, the study theorises that the main research question can be answered by addressing a second question; “What are the impacts of implementing ISO 27001 on Tonga organisations’ information security management and information security?” Answering the first by answering the second question is viable because according to the findings in chapter 4, Tonga organisations by default are using ad-hoc approaches for their information security that is run by their IT departments and with a purely technological focus. Therefore, analysing the impacts of implementing ISO 27001, by default, compares holistic approaches (ISO 27001) against ad-hoc approaches (Tonga organisations’ information security) to determine the best method. Not only that, but analysing the impacts of implementing ISO 27001 on Tonga organisations’ information security also includes analysing organisational factors, such as, resources availability, and the effect on Tonga organisations’ ability to implement ISO 27001, thereby providing a comprehensive answer to the main study question.

Analysing the impacts of implementing ISO 27001 calls for a gap analysis of Tonga organisations’ information security, against ISO 27001 requirements. The study provided the ISO 27001:2013 and the Appendix controls to a group of experts for feedback. The IT security experts from different organisations in Tonga compared the documentation to the state of their organisations’ information security. The collected data were then quantitatively analysed using SPSS (version 27) to retrieve statistics about each organisations’ information security metrics. After quantitatively analysing the data then it was coded and qualitatively analysed using NVivo (release 1.0). The qualitative analysis aimed to identify information security-related rich concepts which could provide context to the previously retrieved statistics.

The gap analysis compared the outcomes of the quantitative and qualitative analysis against ISO 27001 requirements. The main focus is on how each approach (i.e. Tonga organisations’ ad-hoc approaches versus ISO 27001 holistic approach)

addresses different dimensions and Critical Success Factor(s) (CSF) of information security to minimise information risks to organisations' information assets. Moreover, the study established 14 hypotheses based on the research questions above and findings from recent information security studies reviewed in chapter 2, to guide the gap analysis. The study uses the outcome of the gap analysis (identified gaps) to test its hypotheses regarding the impacts (i.e. gaps) in implementing ISO 27001 in Tonga organisations' information security. Consequently, several findings emerged.

Firstly, the study affirmed that implementing of ISO 27001 will have significant positive impacts on the ability of Tonga organisations to address dimensions and CSFs of information security. The study reaches that conclusion because it identified substantial gaps between Tonga organisations' information security and ISO 27001 requirements. This means, implementing ISO 27001 will have significant positive impacts on Tonga organisations' ability to manage their information security effectively.

Secondly, the study affirmed that implementing ISO 27001 will have significant positive impacts on different characteristics of efficacious information security processes, and the Tonga organisations' ability to establish comprehensive information security. The study reaches that conclusion after surmising that by implementing ISO 27001, Tonga organisations' information security will be able to do positive things that their current ad-hoc approaches failed to do. These are: 1. Address dimensions and CSF of information security to minimise risks to an organisations' information assets. 2. Establish a continually improved information security system to keep up with changes to the organisations' information assets and threats environment. 3. Align their information security processes with their business processes.

This study contributes to research knowledge by providing an overview of findings by existing information security studies on information security and information security standards. Furthermore, it gives an overview of what information security looks like in organisations in small countries like Tonga. It also provides organisations with an overview of the benefits of implementing ISO 27001 on their information security. Specifically, employing systematic, holistic approaches, as provided by the ISO 27000 family of standards, is the best and most effectual way to address the ever-changing information security threats organisations face today. Finally, this study demonstrated the use of both quantitative and qualitative analysis to do a gap analysis of different organisations' information security, which is a departure from the usual maturity models-based studies.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ISM	Information Security Management
ISO	International organisations for standards
BSI	British Standards Institute
ISMS	Information Security Management System
PCI-SSC	Payment Card Industry Security Standards Council
PCI-DSS	Payment Card Industry Data Security Standard
COBIT	Control Objectives for Information and Related Technologies
ITIL	IT infrastructure library
CSF	Critical success factors
SANS	Sysadmin, Audit, Network, and Security
CSA	Cloud Security Alliance
IT	Information Technology
EGIT	Enterprise Governance of Information Technology
CSF	Critical Success Factor(s)
CBK	Common Body of Knowledge
EDP	Electronic Data Processing
EDPAA	Electronic Data Processing Auditors Association.
GDPR	General Data Protection Regulation
FERPA	US Family Educational Rights and Privacy Act
CMMI	Capability Maturity Model
BMIS	Business Model for Information Security
ICT	Information and Communications Technologies
ISG	Information Security Governance
ISA	Information Security Associations
ANSI	American National Standards Institute
GQM	Goal Question Metric

CHAPTER 1

INTRODUCTION

1.0 BACKGROUND

The dynamic nature of information security threat landscapes and the pervasiveness of information and communications technologies in today's society makes assessing and managing information security a priority for organisations. According to Cisco (2019) "Visual Networking Index: Forecast and Trends, 2017–2022", in 2022, there will be an estimated 28.5 billion devices connected to the internet (from 18 billion in 2017), 14.6 billion M2M (machine to machine) connections and smartphones will generate 44% of all Internet traffic. Hence, one of the most significant sources of information security threats is hardware and software vulnerabilities. Recent studies on information security threats and impacts of hardware vulnerabilities include studies by Chen et al. (2019), Gupta et al. (2019) and Wu (2020). Each study explores a specific type of attack that exploits hardware or software vulnerabilities. According to ENISA (2019), there were 2377 exploitable hardware vulnerabilities or 8.65% of the total (known) vulnerabilities in 2018 and the first half of 2019. Technological innovations and progress while beneficial to organisations, they also introduce vulnerabilities which added to the complexity and dynamics of an organisations' threat environment.

While technological vulnerabilities are significant threats, Human-based threats, especially insider threats, also pose danger to organisations. A study by Smyth et al. (2019) looked at the definition of "insiders", the risks they posed, and examples of publicized incidences of information security breaches by insiders that cost targeted companies millions of dollars. Insider threats are hard to detect and defend because the perpetrators have access and have intimate knowledge of the organisations' information systems. The seriousness of the problem is illustrated by the findings that human errors account for 95% of information security breaches in organisations (Vasileiou & Furnell, 2019).

Another recent development that complicates information security for organisations today is the pervasive use of cloud computing both by individuals and organisations. Cloud computing is attractive; it allows individuals and organisations to access resources and technologies they otherwise could not afford to purchase or build, support and manage themselves. Unfortunately, cloud computing tends to multiply information security risks. A survey by Kumar and Goyal (2019) identified 12 top threats and vulnerabilities at every layer of the cloud architecture. Notable examples of those vulnerabilities include the Google docs vulnerability, and the phishing attack on Salesforce.com (Bhardwaj & Kumar, 2011). The anonymity of the cloud also presents challenges; for instance, attackers can host tools, create fake profiles to hide data and identities, and it allows a malicious individual to collaborate and share expertise, toolkits and information with others (Dahbur et al., 2011).

Further compounding information security challenges for organisations is the constant progress of Information and Communications Technology (ICT) infrastructure and the rapid and unending digital technologies innovations. The complexity in technologies has led to "change in the cyberattacks forms, functions, and sophistication" (Tounsi & Rais, 2018, p. 212) over the years. Therefore, it is critical for organisations to look for ways to address information security threats in a systematic and holistic manner. Spremić (2013) argued the importance of holistic approaches to information security where everyone in the organisation is involved, and not just the technical staff. To treat information security purely as a technological issue is no longer sufficient to combat information security threats (Arbanas & Žajdela Hrustek, 2019; Soomro et al., 2016). Furthermore, Culot et al. (2019) argued that information security standards provide a "structured approach to cybersecurity" (p. 83), especially the NIST framework and the ISO 27001. Both frameworks "promote a clear definition of roles and responsibilities, encourage a substantial involvement of business leadership and promote risk management practices" (p. 83).

It is a view also held by Singh et al. (2014) who noted a shift in information security literature (in the past decade from 2014), Information security management (ISM) is no longer considered purely as an Information Technology (IT) department responsibility. Instead, it is a collective responsibility because information security involves management, cultural, organisational and behavioural aspects which cannot be addressed by existing technological focused, ad-hoc approaches.

Instead, information security requires an "holistic approach that applies multiple mechanisms for aligning organisational and sociological factors within the organisation combined with technological competencies" (Arbanas & Hrustek, 2019, p. 140). One of the main objectives of establishing Information security standards is to provide a standardized holistic approach to information security (Pinheiro & Ribeiro, 2005). Specifically, implementing the ISO 27001 standard allows organisations to establish coordinated and balanced information security processes aligned to their specific organisational and information security objectives and requirements (BSI, 2017a, 2020a).

1.1 Motivation

In the early 1990s, only a handful of companies (mostly banks) and government departments in Tonga had computer systems. Most of those systems were either standalone or have private satellite connections to overseas partners or central offices. In the middle of the 1990s, more and more companies had PCs, but most were still either standalone or connected to a private network. It was in the late 1990s that information technology awareness and usage expanded with the introduction of the first Internet Service in the country by Cable and Wireless PLC in 1997.

ICT development (which fuels the widespread usage of technologies) took a significant leap in 2000 after the Tonga Communications Corporation (TCC) took over from Cable and Wireless PLC (‘Ofa, 2008; Pacific Islands Report, 2000) and the government granted TONFON a license to operate in the country. TCC launched its Global System for Mobile (GSM) network in 2001 and the TONFON in 2002. In addition to GSM, TCC also launched an ADSL and a WiMAX network in 2006. In 2007 Digicel purchased TONFON (‘Ofa, 2011) and improved their systems and services resulting in stronger competition leading to better and cheaper services. In

2013, TCC launched 3/4G, fibre and ADSL networks and Digicel launched a 3G network both in anticipation of the launching of the submarine cable.

When the submarine cable was launched in 2013 (World Bank, 2013), ICT services had already reached every inhabited island in the country. The only limitation to services was the links to the remote islands which were still satellite-based. The launching of the submarine cables between the main island and outer islands (World Bank, 2019) in 2018 removed that limitations, meaning ICT services that were only available in the main island were now available all over Tonga. The onslaught of new technologies, services, and information availability, with the lack of awareness of those technologies' and associated risks and threats, lead to new challenges affecting both individuals and organisations (Laulaupea'alu & Keegan, 2019).

The submarine cable brought unprecedented change to the ICT services landscape and consequently, Tonga's information security threats landscape. Tonga is now part of an ever-increasing interconnected world and fast Internet access which brings with it higher risks of information security attacks and related crimes (Rudolph et al., 2020; Standards Australia, 2020). Finau et al. (2013) provided detailed examples of such attacks in the Pacific. For Tonga, the researcher has played significant roles in the development of ICT services since 1999, and was aware and was involved in investigations by police and Tonga Computer Emergency Response Team (CERT) of attacks, information security breaches, and electronic crime investigations in Tonga. The affordable and reliable services mean organisations are increasingly dependent on ICT services and information systems for their daily operations. The devastating and costly impacts of the submarine cables breaking in 2018 (Westbrook, 2019) highlighted increasing dependence on the technology. In direct contrast, the loss of the Intelsat satellite in 2005, cutting off all communications to many pacific islands (Gregory & Binning, 2005), was barely noticeable because not only were ICT technologies capabilities at the time limited, but the service was too expensive for many users as well.

While the satellite and the submarines cables incidences are rare; they highlighted several essential realities. First, organisations today, both public and private, are greatly dependent on ICT and information systems. Second, a successful attack on major ICT and information systems in the country, apart from the financial cost, could cause significant disruption to government and private organisation operations. Finally, it is not a question of if but when significant and repeat attacks will occur that will have significant effect on the country.

1.2 Research Aim

Given the dynamic nature of information security threats today and the organisations' ever-growing dependence on IT, Tonga organisations need a new approach to information security to protect their information assets. It is no longer enough to assume that no one is interested in compromising their organisations' information.

Studies have shown that threats can either be malicious or non-malicious (human errors). Attackers either want to take something out or just utilize an organisations' resources for their purposes (Jouini et al., 2014; Jouini & Ben Arfa Rabai, 2016; Jouini & Rabai, 2018). Specifically, all it takes to compromise an organisation's information assets, are a reliable connection (to the organisation) and vulnerable assets (technological vulnerabilities or by human error). Implementing information security standards allows organisations to establish an ISM system which employs a systematic, holistic approach to information security based on proven, widely accepted information security best practices. Therefore, the study aim is to investigate whether implementing ISO 27001 is the best approach for Tonga organisations to establish information security to protect their information assets by analysing the gaps between their current information security practices and ISO 27001 requirements.

1.3 Thesis Structure

This chapter provides a brief overview of information security, information security threats, and information security challenges faced by organisations today, especially Tonga organisations. It provides readers with a sense of the magnitude of the challenges faced by Tonga organisations today, and therefore, why the study is relevant and necessary. The last two sections discuss the aim of the research and the overall structure of the thesis, respectively.

In chapter 2, the study reviews information security, threats and challenges faced by organisations today, as well as proposed approaches to address them. The review provides a brief history of ISO with a detailed analysis of its ISO 27000 family of information security standards and a discussion of how organisations can assess information security standards. Moreover, it also provides a detailed analysis of ISO 27001 as well as some of the more prominent Information security associations today and their contribution to information security. Finally, a look at other information security standards and frameworks such as COBIT, ITIL and PCI-DSS, and how they relate to information security.

In chapter 3, the first step was to establish a research design to govern all research processes and then construct a research model based on the outcomes of the literature review in chapter 2 and the study objective. Based on the analysis of the research model, the researcher establishes several research questions, which in turn form the basis for hypothesis. The research questions and hypothesises determined the study research method, research data, and data collection tools.

The findings of the study, i.e. Tonga organisations' information security current practices, are presented in chapter 4. A comparative analysis of those findings is made against the ISO 27001 requirements in chapter 5. The results and analysis are followed by a discussion of the findings and the comparative analysis in relation to the study's research questions, hypotheses, and research limitations, in chapter 6.

Finally, chapter 7 provides a summary of the study, recommendations for organisations' information security based on the study findings, and suggestions for further studies.

CHAPTER 2
LITERATURE REVIEW

2.0 INTRODUCTION

Information security is a topic that has attracted a lot of attention due to the devastating impacts and consequences of Information security breaches (von Solms & von Solms, 2018; Swinhoe, 2020). Organisations are also more vulnerable to information security threats because organisation threat landscapes are getting more complex and challenging. This is compound by the shortage of skilled staff, and the increasing number of information security incidents (Cisco, 2020).

Information security was previously known as computer security, and defined as protecting computers, the information contained in them, and everything connected (building, network, disks and tapes). The Morris worm attack, as well as other virus and worm attacks during the 1980s and 1990s, brought computer security to the forefront and the attention of scholars, governments, and Technology organisations. It was then considered a technology problem to be solved by technology people. Consequentially, countermeasures were technological and focused mostly on computer security, communications security and physical security (Lehtinen & Gangemi Sr, 2006; Russell & Gangemi Sr, 1991).

The proliferation of Internet services, communications technologies and devices changed the security focus to information rather than devices (Price, 2002). Approaches to information security were also changing, as illustrated by Wood et al. (2000), who argued for a holistic approach to cyber defence. The study focused on critical infrastructure protection (i.e. power, military information systems, and others) from cyber warfare rather than information security. However, it presented a model that addressed information security as a set of coordinated processes that are management driven and includes planning, implementation, and information sharing (between organisations) in stages. This is a model found in information security standards like ISO 27001 today.

Several other studies around the same time noted the need for a holistic approach to information security because they pointed out that information security has technical and non-technical components. It included factors like information security awareness, and organisation culture (Martins & Elofe, 2002), as well as other factors documented by von Solms (2001) and Vroom and von Solms (2004). This has impacts on the efficaciousness of information security measures (Siponen, 2000). Two other vital factors are the organisations' management involvement in the information security processes (Knapp et al., 2006), and organisations establishing a comprehensive risk management program (Gerber & von Solms, 2005).

Moreover, studies around that period pointed out that holistically addressing information security is better. It is more efficacious than ad-hoc approaches many organisations employed at the time and still employ today (Eloff & Eloff, 2003b). That is why information security standards like ISO 27001, and others are important. They offer comprehensive processes of managing information security, and employ internationally accepted information security best practices that address information security critical success factors (CSF) (Al-Ahmad & Mohammad, 2013; R. Von Solms, 1999). This allows organisations to provide effectual protection for their information assets and processes.

The investigation of links between implementing information security standards and establishing efficacious information security processes, provide a theoretical basis for this study. The remainder of this chapter focuses on reviewing past information security studies that concern different aspects of information security standards, information security management (ISM), and effective information security. Section 2.1 examines information security standards and frameworks as well as organisations that authored or support those standards and frameworks. Section 2.2 explores assessing information security standards, while section 2.3 takes a detailed look at the ISO/IE 27001, and security control frameworks are in section 2.4. Finally, a summary of the findings and a conclusion are in section 2.5 and section 2.6, respectively.

2.1 STANDARDS FOR INFORMATION SECURITY

The oxford dictionary definition of a standard is “a level of quality, especially one that people think acceptable”. Standards for Information security specifies a set of processes (requirements) an information security management system (ISMS) must achieve. It ensures a (desirable) level of (measurable or perceived) quality of information security (Tofan, 2011) and therefore, business partners, customers, and suppliers can accept verification using second or third party auditing.

Information security standards are generally accepted information security principles that address information security from a very high-level viewpoint. The information security principles should provide clear information security features, assurances, and practices that are essential for protecting organisation information assets (Swanson & Guttman, 1996). To understand the impact of implementing ISO 27001, a user needs to understand information security standards, the roles they play, and why they are vital for organisation information security. According to Fal’ (2010), information security management (ISM) standards developed by the International organisation for standardization (ISO) has two main focus. The protection of organisations’ information that existed in various forms, and the development of protection mechanisms to mitigate damages caused by inadequate protection.

Implementing information security standards, such as an ISMS based on the framework, has challenges which lead to organisations completely ignoring them or they try to implement them but fail (Al-mayahi & Mansoor, 2012; Alshitri & Abanumy, 2014). The last 30 years has a growing number of information security associations formed to address those challenges mostly by sponsoring research, providing training for technical but also management staff, and certification programs to verify and demonstrate information security professionals’ skills and knowledge of information security.

Consequentially, section 2.1.1 reviews the International Organisations for Standards (ISO) contributions to the development of organisations’ information security. Specifically, the ISO 27000 family of standards. Section 2.1.2 reviews information security contribution of some of the more well-known information security associations today. Specifically, their training and certification programs, standards, frameworks and models. Finally, section 2.1.3 provides a summary of the section findings.

2.1.1 International Organisation for Standards

The international organisation for Standard or ISO is an independent international non-governmental organisation for standards. ISO was formally established in 1947 with 67 technical committees and released its first standard in 1951. ISO standards are market-driven and based on standards developed by its members. These are standards that have been tested and proven at national negotiations. ISO standards cover broad fields, like banking, Information Technologies, International shipping, health, food, environments and many others (Heires, 2008; ISO, n.d.). According to ISO (2019), at the time of the report, it has 164 members, 249 technical committees, and 22500 international standards. Today, ISO is one of the oldest and most active standards organisations. Though voluntary, ISO standards are well known and widely adopted by many organisations around the world, and in some cases, countries have incorporated them into their regulations (Heires, 2008).

2.1.1.1 ISO 27000 Standards

An ISO primary information security standard is the ISO 27000 family of standards (BSI, 2020a). The first standard ISO released was the ISO 27002 (BSI, 2017b) which provides code of practice for security controls. ISO released ISO 27001 (BSI, 2017a) after releasing ISO 27002; with ISO 27001 containing the same security controls as ISO 27002. ISO 27002, however, does not specify requirements like ISO 27001; instead, it provides guidelines on how organisations can select and implement appropriate security controls according to their needs. Figure 2.1 depicted the relationships between ISO 27001 and the rest of ISO 27000 standards.

The ISO 27000 family of standards are divided into three categories with ISO 27000, providing an overview of the ISMS as well as terms and definitions (BSI, 2020a). The first category of standards are standards specifying requirements which include ISO 27001, 27006 and 27009 (BSI, 2020a). ISO 27006 specifies requirements for accreditation of certification bodies that provide ISMS audits, and ISO 27009 specify requirements for modifying ISO 27001 security controls to meets sector-specific requirements.

The second category, according to ISO 27000, is standards specifying general guidelines for implementing an ISO 27001 based ISMS (BSI, 2020a). These standards include ISO 27002, 27003, 27004, 27005, 27007, 27008, 27013, 27014, 27016, and 27021. All provide guidance (detailed explanation and examples) on different aspects of an ISMS to help organisations understand and correctly implement 27001 requirements (BSI, 2020a).

Among the second category of standards are ones which are provided to help organisations understand every aspect of ISO 27001 requirements (BSI, 2020a). For instance, ISO 27002 provides detailed guidelines on ISO 27001 security controls, while ISO 27003 provides detailed guidelines on the general requirements (requirement 4 to 10) (BSI, 2017d), and ISO 27005 provides guidelines on the risk management processes (BSI, 2011). As noted by ISO 27003, “ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005 form a set of documents supporting and providing guidance on ISO/IEC 27001:2013” (BSI, 2017d, p. 6).

Like any business project, organisations need to weigh the resources it spends on establishing an ISMS against its benefit to the company, i.e. return on investment (BSI, 2014). ISO 27016 help organisations' senior management to prepare an information security business case for implementing an ISO 27001 based ISMS. According to ISO 27016, ISMS should support organisations’ objectives and “cost and benefit decisions should relate to the expected benefits from achieving a risk reduction by the deployment of planned controls” (BSI, 2014, p. 11).

Another important component of organisations’ information security is setting up a proper information security governance structure (Stoll & Breu, 2012). A properly set up governance structure with assigned roles and responsibility will help organisations manage their information security processes in a coordinated and systematic manner (Von Solms, 2005). While organisations can use other governance frameworks for setting up their governance structure, they also use the ISO 27014. It provides guidelines to help organisations set up an information security governance structure with assigned roles and responsibilities to manage the information security (BSI, 2013). To help organisations identify and fill the roles needed for effectual management of their information security, ISO provides ISO 27021. It provides guidelines on ISMS's roles intended outcome and required knowledge and skills. Competence areas include information security, ISMS planning, operation, support, performance evaluation, and continuous improvement. (BSI, 2017e).

For an ISMS to remain relevant, it must be able to adapt to changes in an organisations threat environment, requirements, and objectives (Haufe et al., 2016). The ISO 27000 family of standards comes with several standards to help organisations, continually improve their ISMS. For instance, ISO 27004 (BSI, 2016a) allows organisations to monitor and measure the performance of their ISMS. Furthermore, ISO 27007 helps organisations managed their ISMS by providing guidelines on how they can audit their ISMS internally (BSI, 2020b). Internal auditing helps an organisation to keep track of ISMS processes and performance. According to Pompon and Pompon (2016), "Internal audit exists to make the organization's security program stronger" (p. 277).

Another vital aspect of ISMS management is the ability of an organisation to monitor, assess and modify their security controls (Zeb et al., 2018). ISO provides ISO 27008 for that reason. It provides guidelines to help organisations monitor, assess and modify their information security control to improve their performances or align with their changing requirements and objectives (BSI, 2019b). The final standard in the second category is the ISO 27013 standard (BSI, 2020a). It provides guidelines on how to integrate ISO 27001 and ISO 20000-1. ISO 20000-1 specifies requirements for service management, comparable to ITIL. ITIL is a code of practice and not a standard (AXELOS Limited, 2019; BSI, 2015c). Service management focuses on service value creation. Under service management, information security is a service which facilitates co-value creation by protecting organisations' information assets (Agutter, 2019; AXELOS Limited, 2019).

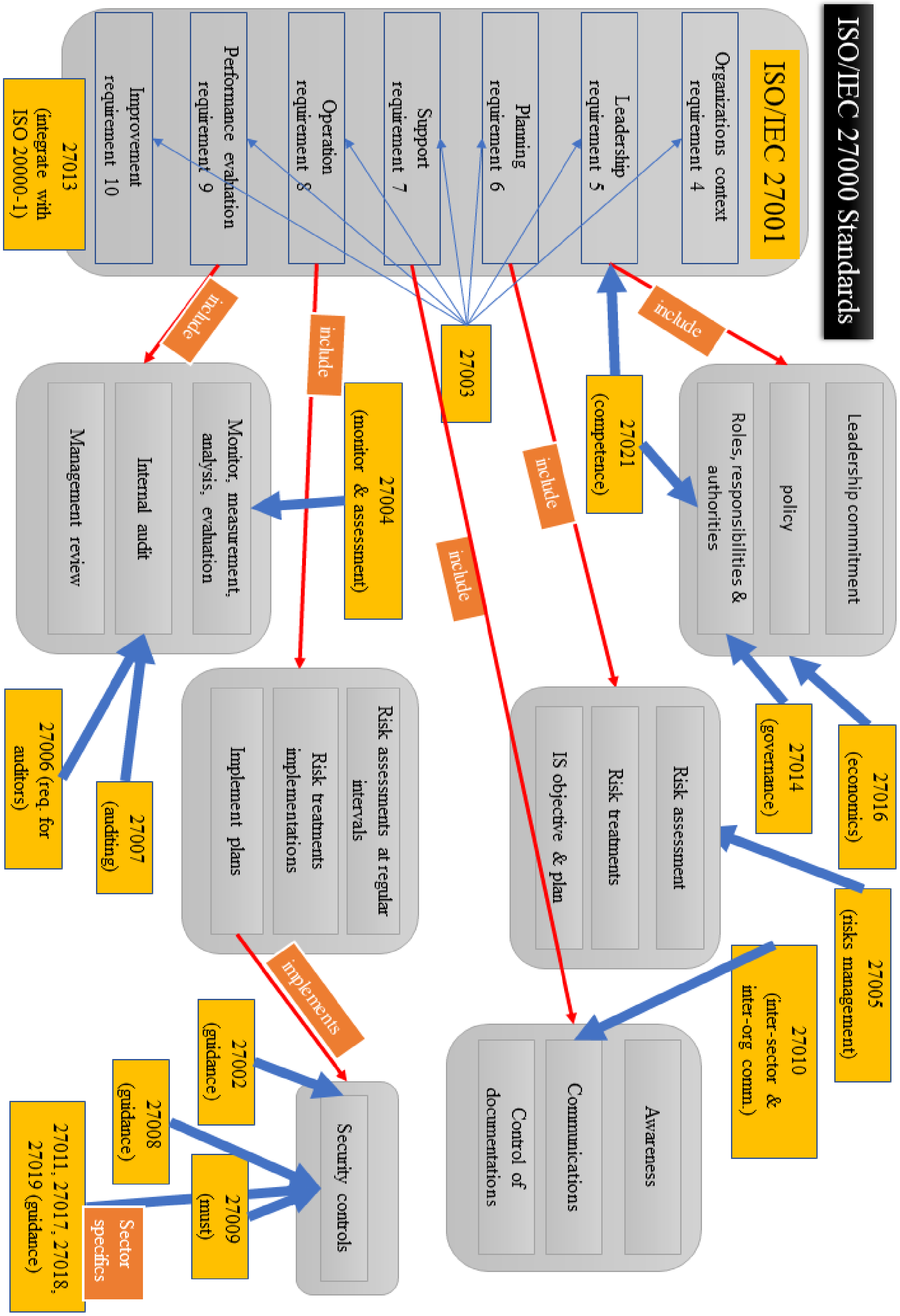


Figure 2.1: ISO 27000 standards

Adapted from analysis of BSI (2020a) and BSI (2017a)

The third category of standards, according to ISO 27000 standards, are standards that specify sector-specific guidelines and requirements (BSI, 2020a). Organisations should adopt them in conjunction with ISO 27009 (BSI, 2016b). ISO 27009 provides requirements for modifying the ISO 27001 security controls. Sector-specific standards include ISO 27010, which specify requirements for information sharing between organisations (BSI, 2015b). ISO 27011 specifies additional requirements for telecommunications organisations (BSI, 2016c). ISO 27017 specifies other requirements for cloud services both (cloud customers and providers) (BSI, 2015d). ISO 27019 specifies additional requirements for the energy industries (BSI, 2020c), and ISO 27018 which provides a code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (BSI, 2019a).

Among the sector-specific standards, ISO 27018 requires further analysis due to the importance of protecting individuals' online identity and their privacy. Personal identifiable information (PII) is any information that a third-party can use to identify a users' identity (BSI, 2019a). For example, name, ID number (social security number, licenses, company ID), phone and mobile number, residential or employment address, and others. It is even more crucial when such information is stored in the cloud and potentially misuse and abuse if it is leaked to the public (Katsuno et al., 2016).

PII inclusion in the European Union GDPR (General Data Protection Regulation) and the US Family Educational Rights and Privacy Act (FERPA), which gives users right to erasures (i.e. delete their PII upon request), illustrates the significance of the issue. Kelly et al. (2019) discussed the regulation (GDPR article 17), compliance challenges faced by organisations in tracking and erasing every piece of PII on request and suggests methods to help small organisations with hybrid (private and public) clouds to comply with the regulation. A similar study by Katsuno et al. (2017) discuss ways for educational institutions to protect students PII stored in public clouds while still in compliance with the FERPA. Specifically, ISO 27018 helps organisations who are cloud service providers to safeguard not only the privacy of their information but also that of their customers, suppliers and business partners.

2.1.1.2 ISO 27000 CONTENT

ISO formalises the ISO 27000 family of standards for information security by releasing of ISO 27000:2009. It provides an overview of an ISMS, summary of the roles of each standard, as well as terms and definitions used by the standards (BSI, 2020a). ISO 27000 defined an ISMS as a systematic approach for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives" (BSI, 2020a, p. 11). Information security is risk management; therefore, organisation information risks are assessed, analysed, prioritized, and then risk treatments are implemented according to the organisations' risks acceptance level (Blakley et al., 2001).

ISO 27001 sections 4, 5, 6, and 7 specified the requirements for establishing an ISMS. Furthermore, section 8 sets the requirements for ISMS operation, while section 9 and 10 specified the requirements for monitoring, reviewing, maintaining and improving the (BSI, 2017a). Earlier versions of the ISO 27000 refer directly to employing the Plan-Do-Check-Act (PDCA) improvement cycle on each of the implementation stages (Disterer, 2013); however, the latest version removed references to the PDCA improvement cycle. The ISO 27000 family of standards put great emphasis on the establishment sections because they deal with issues that are CSF for implementing an ISMS as listed in ISO 27000 section 4.6 (BSI, 2020a). A literature review by Tu and Yuan (2014) and Alnatheer (2015) of studies between 1998 to 2011 found that CSF affecting information security include business alignment; organisation support; Information Technology (IT) competence; risk management, information security policy, and performance evaluation. A more recent literature review by Arbanas and Hrustek (2019) which includes studies up to 2018 identified the same CSF with three additional factors, information security culture, budgeting and legislative pressure.

All these CSF are in-line with ISO 27000 "critical success factors" (BSI, 2020a, p. 17) and are addressed in the establishment sections of the ISMS requirements. For instance, the organisation context section, addressed the identifying of organisations' information security needs, both internally and externally (legislation, partners)

(Humphreys, 2016). This process helps tailor an ISMS according to individual organisation requirements. For example, Kaban and Legowo (2018) discuss implementing ISO 27001 for a private bank, Velasco et al. (2018) discusses implementing ISO for a manufacturing company, and Fajar et al. (2018) discusses implementing ISO 27001 for a company utilizing cloud services. By understanding the organisation context, organisations can define the scope of their ISMS according to their requirements and business objectives, thus aligning information security processes with their business objectives (BSI, 2017d).

Another very important, or perhaps the most critical factor for information security management is management involvement, without which ISMS projects cannot start (Alshitri & Abanumy, 2014). Section 5 of ISO 27001 specifies requirements for leadership involvement in an ISMS with additional guidelines provided by ISO 27014 and ISO 27016 (BSI, 2013, 2014, 2017a). Management involvement at a minimum ensures the establishment of an information security governance structure, information security policy, and resources availability. They are also crucial in driving positive, active information security organisation culture. Without a positive, vibrant information culture where everyone in the organisation is involved in a meaningful way in information security, information security measures will not be efficacious (Mousavi & Kumar, 2019; Wiley et al., 2020).

Organisations need comprehensive information security to protect their information assets which means organisations need to close all possible attack routes from inside and outside the organisation. The challenge is to ensure all parts of an organisation information security infrastructure work together because any weak link would compromise the whole organisation and its information assets (Boyle & Panko, 2015). An essential part of a comprehensive information security plan is risk assessment (Eroğlu & Çakmak, 2016). This is included in ISO 27001 planning and operation requirements, with guidelines provided by ISO 27005. A literature review by Li et al. (2016) identified four stages of the risk assessment process, which are assets recognition, threats identification, vulnerabilities identification, and risk analysis. That is in-line with ISO 27005 risk assessment processes, which Pan and Tomlinson (2016) concluded that ISO 27001 provides a more accurate definition of each risk assessment stage than other risk assessment standards they studied.

2.1.2 Information Security Associations

Information security associations provide training, research and certification programs, with the aim of developing industry-ready information security professionals, ready to help organisations to plan, implement and manage their information security (ISACA, n.d.-a; ISC2, n.d.-c; SANS, n.d.-e). An analysis of cybersecurity certifications by Davis (2019) points out that information security is a new multi-disciplinary field; making it hard to create courses that meet both academic standards and industry needs. Furthermore, the fact there is no global body overseeing (i.e. standardized) certifications, means each information security organisation focuses on what they think essential for information security.

The lack of information security skilled professionals was highlighted by Northcutt (2005) when he discussed his experience working with information security staff and their lack of practical information security skills which led him to get involved in developing the Global Information Assurance Certification (GIAC) for SANS. A report by Assante et al. (2011) noted the shortage of skills information security professionals in the US, the drop in the number of university students enrols in computer science programs and the urgent need to train more information security professionals. A survey by the International Information System Security Certification Consortium (ISC2) also found that 56% of organisations surveyed believe there is a workforce shortage (Suby & Dickson, 2015).

The studies above emphasize the crucial role information security organisations play in the awareness, training, and educating of organisations, organisations' leaders and their staff on important aspects of information security. Information security organisations provide training for organisation leaders, middle management and technical staff to help organisations establish effective information security. Section 2.1.2.1 provides brief backgrounds on some of the most notable information security association today. Section 2.1.2.2 discusses the information security offerings of each organisation in 2.1.2.1, and section 2.1.2.3 provides an analysis of information security associations' certification programs.

2.1.2.1 Organisations

This section provides a brief background on some of the most notable information security associations today and a brief summary of their contribution to information security. They provide training and certification programs, authored frameworks, standards and models. Specifically, this section will discuss SANS in section 2.1.2.1.1, ISC2 in section 2.1.2.1.2, ISACA in section 2.1.2.1.3 and CSA in section 2.1.2.1.4.

2.1.2.1.1 SANS

The SANS (Sysadmin, Audit, Network, and Security) Institute was established in 1989, and is a cooperative research and education organisation. The programs have since reached 16500 security professionals; educating 30000 security professionals each year. In their words, SANS is by far the largest and most trusted source of information security training in the world. Furthermore, SANS offers programs that enable security professionals, system administrators, and network administrators to share lessons based on their experiences and find solutions to the problems they faced (SANS, n.d.-e).

SANS research and teaching programs are its main contribution to information security. It helps organisations to raise greater awareness of the importance of establishing effective information security as well as training information security professionals to facilitate the establishment of effective information security. The strength of its research and training programs are due to contributions by security practitioners from corporations, government agencies and universities from around the world (Thomas & Stoddard, 2011).

SANS also offers short-term training courses, both online and in-person and degree programs via it's SANS technology institute. It also offers several professional certifications for information security professionals covering different areas of information security, from management, audit, legal and technical areas like cyber defence, forensics and incident response and others (SANS, n.d.-c). Furthermore, SANS offers resources which are free to the public including its Information Security Reading Rooms (SANS, n.d.-d), Information Security Policy Project (free Security policy templates), and Internet Storm Centre (Internet early warning system) (SANS, n.d.-b).

2.1.2.1.2 ISC2

The International Information System Security Certification Consortium (ISC2) is an international non-profit organisation for security professionals with more than 150,000 certified members. It provides training, certification and peer networking for security professionals all over the world. ISC2 was established in 1989 and began by collecting and distilling both local and international information security information relevant to information security professionals. The database of collected information is known as its Common Body of Knowledge (CBK). CBK was finalised in 1992 and offered its first CBK-based certification in 1994 (ISC2, n.d.-b).

ISC2 certifications and training focus on each domain (area) of information security specified by its CBK. According to ISC2, they continually updated their CBK to reflect changes in organisations' information security environment (ISC2, n.d.-a; Stringer, 2008). According to a survey by ISC2 of 12000 security professionals in 2012, the affiliation organisation that matter most in terms of career development in the information security field is ISC2 with 66%. SANS was second with 32%, 31% for ISACA, 18% for OWASP, 16% for IEEE, and 13% for CSA (Suby & Dickson, 2015).

2.1.2.1.3 ISACA

ISACA, formerly known as the Information Systems Audit and Control Association but now known only by its acronym is a non-profit, independent membership association. ISACA provides certifications, standards, frameworks, and models and also publishes a technical journal, the ISACA Journal. Today ISACA has 145000 members in 180 countries. It represents a broad range of services. ISACA was first incorporated as an association in 1969 as EDPAA or Electronic Data Processing Auditors Association (ISACA, n.d.-a). According to ISACA, their goal is to use their globally accepted research and guidance, credentials and community collaboration to help professionals and organisations around the world realize the positive potential of technology (ISACA, n.d.-m).

ISACA held its first conference in 1973 and released its first regular publication, the Electronic Data Processing (EDP) auditor. It published its compilation of guidelines, procedures, best practices, and standards for conducting an EDP audit entitled "Control Objectives" in 1977. Between 1992 and 1996, ISACA made significant revisions to the document and changed the name to the Control Objectives for Information and Related Technologies (COBIT) (Lainhart, 2018). COBIT is an IT governance framework. It is one of the more popular IT governance and management framework today. ISACA has since added several other standards, frameworks and models that address areas like IT assurance, IT risks, and others to its portfolio of standards, frameworks and models (ISACA, n.d.-i).

ISACA also offers certification programs for IT practitioners. The first certification program was the Certified Information Systems Auditor (CISA) certification program, which was launched in 1978. CISA aim was to certify information technology internal and external auditors' knowledge and skills. Two years later, in 1981, they held the first CISA exam (ISACA, n.d.-a). Today, in addition to CISA, ISACA offers certifications on risk management, cybersecurity and other related areas (ISACA, n.d.-k).

2.1.2.1.4 CSA

Cloud Security Alliance (CSA) is an International organisation founded in 2008; it is the world-leading organisation in cloud computing security. Its focuses are on defining and raising awareness of best practices to ensure a secure cloud environment. CSA members consist of cloud solution providers and enterprises. Executive members include companies like Microsoft, Google, Oracle, Huawei and others (CSA, n.d.-a, n.d.-c)

CSA provides cloud security assurance programs which include a certification program for cloud solution providers, cloud users' certification, and a professional certification on cloud security. CSA hosts webinars and training around the world as well as funds cloud-related research by researchers from around the world (CSA, n.d.-e). As more and more services are moving to the cloud, CSA plays a vital role in the security of cloud computing. They contribute to the training of cloud security professionals and research and development of specific cloud security controls for cloud-based information security frameworks (CSA, n.d.-d, 2019b, 2020).

2.1.2.2 PROPRIETIES

While a few of the information security associations authored standards, frameworks, and models, targeting different aspects of information security, their main and common contributions to information security are through their training and certification programs. This section focuses on examining ISA's information security offerings and their contributions to the development of effective information security. Specifically, this section will discuss SANS contributions in section 2.1.2.2.1, ISC2 contributions in section 2.1.2.2.2, ISACA contributions in section 2.1.2.2.3 and CSA contributions in section 2.1.2.2.4.

2.1.2.2.1 SANS

According to its website, SANS is the largest source for information security training and certification. It offers 400 multi-day courses in 90 cities around the world, a work-study program for security professionals. SANS also runs the Information Security Reading Room, which is a database of more than 3000 research papers on information security covering 111 different research areas (SANS, n.d.-d). The research papers are free to organisations and the public, and it is a source of information on the latest studies on information security (SANS, n.d.-d). SANS research contributes to its common body of knowledge from which it bases its training and certification programs. Furthermore, SANS research also contributes to the development of the CIS Security

Control, which is a security control framework containing widely accepted security controls based on organizations' information security practices (SANS, n.d.-f).

SANS training and research support its main certification program, called GIAC (Global Information Assurance Certification). GIAC was started in 1999 to validate the real-world skills of organisations' information security professionals. GIAC certifications have seven categories, six of which focus on specific areas of information security such as cyber defence, penetration testing, incident response and forensics, industrial control systems, management, and developers (GIAC Certifications, n.d.; SANS, n.d.-c). Moreover, GIAC Certifications focuses on teaching information security professionals practical skills in the areas mentioned above (SANS, n.d.-a).

According to Northcutt and Frisk (2007), GIAC certifications distinguish from other certifications due to three factors. GIAC does not give certification without exam (grandfathered); each student exam is unique, i.e. no two students sit the same exam because exams are auto-generated from a pool of questions. Moreover, GIAC certification programs are overseen by a meritocracy-based advisory board, which consist of certified candidates who achieved a mark of 90 or above in their exam (Pike, 2008).

SANS also supports the Centre for Internet Security (CIS) security controls framework through its training and research programs. The CIS Security Controls contains 20 controls covering the different areas of hardware, software, network access and so on. Many of the controls map directly to ISO 27001 controls (SANS, 2016). According to SANS (n.d.-d), the security controls are efficacious because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a vast range of community, government and industry practitioners.

2.1.2.2.2 ISC2

The ISC2 main contribution to information security is through its training and certification programs, annual reports on information security and a skills framework called NICE. ISC2 training and certification programs cover various areas of

Information Security according to the eight domains of their Common Body of Knowledge (CBK) (ISC2, n.d.-a). The domains include security and risk management, asset security, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, security operations, and software development security (Warsinske et al., 2019).

CISSP (Certified Information System Security Professional) is ISC2's oldest professional certification program (Suby & Dickson, 2015). It is the first information security certification program accredited by ANSI to the ISO 17024 standard (Gregory & Miller, 2018). Unlike other ISC2 training and certification programs which focus on a particular domain, CISSP covers all eight domains of the CBK.

According to ISC2, CISSP certified information security professional demonstrate their skills and knowledge in effectively designing, implementing and managing a best-in-class cybersecurity program (ISC2, n.d.-e). The book titled "The Official (ISC)2 Guide to the CISSP CBK Reference" by Warsinske et al. (2019) covers ISC2's CBK domains in detail as well as specific requirements for passing the CISSP certification exam. Several papers (Davis, 2019; Smith, 2005; Tittel, 2006) considers CISSP as among or if not the best certification program available today. ISC2 also offers other certifications programs like CCSP, which enable information security professionals to demonstrate their skills and knowledge in designing, managing and securing cloud environment's data, applications and infrastructure (ISC2, n.d.-b). HCISPP enable Information security professional to demonstrate their proven skills and expertise in healthcare information security and privacy (ISC2, n.d.-h). Finally, SSCP is for information security professionals to exhibit their advanced technical skills and expertise in implementing, monitoring and administering IT infrastructure (ISC2, n.d.-i; Stringer, 2008).

ISC2 (certified) members are supported by its "Professional Development Institute" which provide training as part of its continuing education programs because (ICS) ^{2} certification programs require certified members to recertify every three years (ISC2, n.d.-d). In addition to its certification and training programs, ISC2 maintained and released several survey reports on Information Security. The reports are available to the public including “Cybersecurity Workforce study”, “Cyber Security Assessment in mergers and acquisition”, “Securing the partner ecosystem”, and “Women in cybersecurity”. The reports provide organisations and individuals with an overview of the current status of Information Security (ISC2, n.d.-c).

Finally, ISC2 authored and released a skills framework called NICE. The framework maps the ISC2 information security domains (areas like management and risks management) to tasks and the skills required. The framework intention is to make it easier for employers to restructure their information security program and to hire the right people for the right job. The ISC2 training and certifications programs provide the basis for its NICE skills framework (ISC2, n.d.-d).

2.1.2.2.3 ISACA

ISACA provides both professional certifications programs as well as information security standards, frameworks and models. ISACA initial focus is auditing, specifically IT and information security auditing (ISACA, n.d.-a). IT and information security auditing is increasingly becoming an essential part of information security and businesses operations because of increased dependence of organisations on IT and the growing threats to organisations' information assets (Al-Moshaigeh et al., 2019). The importance of information security auditing leads to many CPA (certified public accountant) programs integrating information security auditing into their programs or recommends CPAs taking one of the publicly available information auditing certifications like ISACA’s CISA certification program (Jadhav, 2018).

The ISACA CISA (Certified Information Security Auditor) certification program is one of the few certifications that focuses on information security auditing (ISACA, n.d.-c). CISA covers five knowledge domains, 1. The process of auditing Information Systems. 2. Governance and Management of IT. 3. Information Systems Acquisition, Development and Implementation. 4. Information Systems Operations, Maintenance and Service Management. 5. Protection of Information Assets (Davis, 2019).

Furthermore, according to ISACA, the program distinguishes itself from other programs due to several factors, no grandfathering options (certified via work experience), ANSI accredited according to ISO 17024 standards, and it has a requirement for recertification. Members recertify their skills and experiences by reporting to ISACA 25 CPE (Continuous professional education) hours and by paying an annual fee (ISACA, n.d.-c).

In addition to the CISA programs, ISACA offers other certification, listed in ISACA (n.d.-b). CRISC is for information security professionals to demonstrate their skills and knowledge in information security risk management and to implement and to maintain information systems controls (risk treatment) (ISACA, n.d.-g). CISM aim is to help Information technology professionals demonstrate their skills and knowledge in IT governance, program development and management (ISACA, n.d.-d). CGEIT is for Information technology professionals to demonstrate their skills and expertise in IT governance (ISACA, n.d.-b). CSX-P, according to ISACA, is for information security professionals to demonstrate their ability to perform globally validated, cybersecurity skills, covering five primary cybersecurity functions. Identify (threats), Protect, Detect, Respond, and Recover (from attacks) (ISACA, n.d.-h).

In addition to its training and certification programs, ISACA also provides standards, frameworks and models. For instance, COBIT is one of the most widely implemented Enterprise IT governance and management framework (ISACA, n.d.-f). Furthermore, ISACA also provides a risk management framework called “Risk IT” to help organisations manage their information security risks. They also offer an information security auditing and assurance framework which provides best practices guidance for information security audit and assurance (ISACA, n.d.-j).

Moreover, ISACA is also the author of Business Model for Information Security (BMIS) (ISACA, n.d.-l) and Capability Maturity Model Integration (CMMI) (ISACA, n.d.-e). BMIS is a model that takes a business-oriented approach to information security (Lawrence, 2017). “CMMI is a performance improvement model for organizations and projects that want to achieve increasingly better performance and address and solve business challenges” (CMMI Institute, 2018, p. 6).

2.1.2.2.4 CSA

CSA focus is primarily on the security of cloud infrastructure, data and services and not on information security in general as with other information security associations. Their certification programs and training, therefore, focus only on cloud computing security (CSA, n.d.-e).

The cloud security alliance main security program is its STAR open certification framework for cloud providers (CSA, n.d.-b). The program allows cloud security providers to certify their cloud infrastructure security against the CSA cloud controls matrix. CSA cloud controls matrix is a code of practice of security controls for cloud security (CSA, 2019c). The STAR program has three levels. Level one is self-assessment, i.e. cloud providers access their own compliance, level 2, is when third-party auditors assess organisations' compliance, and level 3, is when cloud providers cloud solutions are continuously audited both by the cloud provider and by third-party auditors. While STAR is a voluntary framework, CSA provides the CAIQ (continuous assessment initiative questionnaire) tools (CSA, 2020) to allow cloud consumers to assess a cloud provider’s level of compliance, which can force cloud providers compliance if cloud consumers demand it.

CSA also provides training and certificate programs aimed at cloud information security professional. Cloud CCSK, is a 2-day course and a certification program. Launched in 2011, it is the oldest cloud certification available today (Davis, 2019). It is aimed at Information security professionals to learn the best practices and recommendations for securing an organisation for the cloud covering all 14 domains in the CSA’s security guidance v4.0 (CSA, 2017). CSA split the course 60/40 between technical and business-driven content. The CCSK Plus version of the certification is CCSK plus practical labs. The certification exam is an open book exam, made up of 60 questions to be completed in 90 minutes (Thompson, 2018). In addition to CCSK, CSA also launched a new certificate called CCAK in 2020. According to CSA, CCAK is "the only credential for industry professionals that demonstrates expertise in the essential principles of auditing cloud computing systems" (CSA, 2019a, para. 1).

CSA also offers training courses like its ACSP training course (CSA, n.d.-b). ACSP is a technical, practical course focusing on cloud security and applied Develops (development, security, operation) for enterprise-scale cloud deployments. Specifically, ensuring security is integrated into the development and operation of cloud processes and not an add-on. ACSP focuses only on PaaS processes and does not cover SaaS, IS policies, IS risks or other governance-related issues.

2.1.2.3 CONTENT

Information security is becoming an indispensable part of organisation operations due to their dependence on information assets and technologies. Therefore, having or to have access to skills information security professionals is critical for the successful management and operation of information security functions and consequently, an organisations' resiliency. Unfortunately, today as Furnell et al. (2017) concluded; "the current and future demand for cyber-security skills looks likely to be outstripping supply" (p. 5). They point out that there are two issues organisations faced when it comes to hiring information security professionals, (1) the level of professionalism (skills, experience, and others) for information security professionals, (2) recognising the skills they need and finding people with those skills.

Today, there two pathways to addressing information security skills shortages. Students attend educational institutions and earn a formal degree in information security or attend training and get a professional certification on information security from one of the many information security certifications available today (Bishop & Frincke, 2004). The advantage of formal degrees is that students will have a more in-depth theoretical knowledge of information security. However, they are not necessarily qualified practitioners ready to work in information security (Furnell et al., 2017, p. 6). Professional certification is aimed to provide the supporting knowledge and skills for students to become qualified practitioners. Initially, people were sceptical of the viability and usefulness of certification (Rode, 2004; Smith, 2005). However, certification programs have developed and today play a vital role in training skilled Information security professionals. Most of the certification programs focus on demonstrating skills and knowledge regarding a specific (technical or managerial) skillset or area. ISA based their certifications areas of emphasis on their goals and a common base of knowledge (CBK) (Davis, 2019).

For instance, the SANS GIAC purpose is to assure organisations that GIAC certified members have the appropriate knowledge and skill required to fill roles in critical areas of information security. They formulated the program based on feedback collected from technical professionals and managers on what they think an information security professional should know (Northcutt, 2005). Consequently, instead of focusing on general knowledge of information security, GIAC certifications address specific areas of information security. For instance, audit, incident response and handling, firewalls and perimeter protection, intrusion detection, forensics, hackers' techniques, and operating systems security as well as application security like Apache, MySQL, and PHP (Northcutt, 2005).

Today, GIAC certifications has seven categories: Cyber defence, Penetrating (pen) testing, Incident response and forensics, management, audit and legal, Developer, Industrial Control System and GSE (GIAC security expert) (SANS, n.d.-c). Apart from several certifications under the management, audit and legal category, the majority of GIAC certification are technically oriented. For instance, cyber defence focuses on protecting hosts and networks; therefore, the topics covered are technical like host hardening and firewalls. Incidents response and the forensics focus on forensics tools and methods. Penetration testing, focuses on ethical hacking tools and techniques. Certifications under the management, audit and legal category, covers managing the technical aspect of information security (e.g. GSLC) but also governance (e.g. GSTRT) (GIAC Certifications, n.d.).

In contrast, ISC2 is an association by information security professionals for information security professionals; therefore, the primary focus of its certification is a high-level view of information security. For instance, its CISSP (Certified Information Systems Security Professionals) (ISC2, 2020) is based on ISC2's eight security domains for enabling information security professionals to demonstrate their knowledge and skills in all eight different areas of information security. The security domains include security and risks management, software development software, security operations, asset security, secure architecture and engineering, identity and access management, communication and network security, security assessment and testing (ISC2, n.d.-a). As ISC2 states, CISSP enables candidates to demonstrate they can effectively design, implement and manage cybersecurity programs. Most of ISC2 training and certification programs work together to facilitate (a pathway for) members passing its CISSP certifications.

One central point of difference between ISC2 and SANS certifications is ISC2 CCSP certification (ISC2, n.d.-b)which SANS does not have any comparable certification. CCSP, together with CSA's CCSK, is the only certifications available that deals with cloud security. CCSP according to ISC2, enable candidates to demonstrate their "advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at (ISC)²" (para. 2). CCSK contrastively, enables candidates to demonstrate their "competency in key cloud security issues through an organisation that specializes in cloud research" and their "technical knowledge, skills, and abilities to effectively use controls tailored to the cloud" (CSA, n.d.-a, " What are the benefits of earning your CCSK?").

Thompson (2018) provides a detailed comparison of the CCSP and CCSK certifications. He concluded that while CCSK has been around for a long time, it remains "highly relevant to security professionals who are seeking a course that delivers a general tactical and strategic understanding of the challenges and advantages of cloud" ("Concluding Thoughts on CCSK"). He also added that while CCSP expands the discussion on strategic issues, "it doesn't get into the same depth of tactical discussion that is found in the CCSK" ("Concluding Thoughts on CCSP").

While SANS, ISC2 focuses on information security in general and CSA focus only on cloud computing, ISACA focuses mostly on auditing. While in recent years it has branched out to other areas, its main focus is still in auditing, management and governance. Their certification programs are prime examples. For instance, CISA, which focus on auditing and controls, is still their main certification. Their other programs include CRISC, focuses on risk management and control, CISM focuses on ISM, CGEIT focuses on enterprise governance of IT, and its newer certification programs, CSX-P, which focuses on cybersecurity and CDPSE which focuses on privacy (ISACA, n.d.-c).

Despite criticism that certifications do not train information security professionals fast enough and not providing students with relevant experiences needed by organisations (Beveridge, 2019), information security associations are still offering more and more certifications today. Whilst all certification programs are all information security-related the focus and content of each information security association certification program is largely dependent on their purpose (Vasileiou & Furnell, 2019). The diversity is beneficial as all contribute to the development of information security professionals' skills in different areas of information security which is vital to organisations being able to establish effective information security (Alshitri & Abanumy, 2014).

2.1.3 Review

Information security required a holistic approach that deals with different dimensions of information security. Information security standards like the ISO 27000 family of information security standards, provides standards to help organisations develop an effective ISM that addresses all dimensions and success factors of information security.

The ISO 27000 main standard is ISO 27001, which provides requirements for an information security framework that organisations can follow to establish an information security management (ISM) system to manage their information security in a systematic, holistic manner. The rest of ISO 27000 standards provide guidelines to help organisations implement ISO 27001 according to their organisations' requirements, resources and information security and business objectives.

One of the major hindrance for organisations implementing and maintaining an effective ISM system and subsequently, effective information security is the lack of skilled information security staff. Information security associations help in this area by providing training and certifications programs to train information security professionals and provide organisations with proven skilled information security professionals when they need to fill various information security roles in their organisations.

Apart from providing training and certification programs, Information security associations also contribute by funding information security research, and authoring reports on the current status of information security. Some ISA also authored standards, frameworks and models to assist organisations with establishing effective ISM and consequently, effective information security.

2.2 Assessing Information Security Standards

It is postulated that for an information security standard to be successful, it must be able to answer 'yes' to several questions. Are businesses successfully using the standard? Are businesses benefiting, i.e. seeing a return on investment, from implementing the standard? Do the standards help organisations protect their information assets at an affordable price? Can other organisations affirm via third-party auditing that an organisation implementing the standard is secure enough to do business with? (Humphreys, 2011). Specifically, a major determining factor of a standard success is its measurability.

Standards provide a frame of reference for organisations to measure their standardized systems, products, and services against. For organisations to meet their security requirements and be able to confidently established business relationships with other organisations, it is necessary to develop a common standard as a frame of reference for participating organisations. A common standard of recognized information security best practice ensures desirable information security characteristics like confidentiality, integrity, availability, and non-repudiation of organisations' information assets (Herath et al., 2010; Tofan, 2011).

Assessing a standard is essential to ensure organisations' implement and are compliant with standards' requirements, and to ensure organisations achieve the desirable characteristics of the standard they chose to implement. A good example is the International English Language Testing System (IELTS) English exam. Passing

IELTS exam has two effects. First, passing the exam ensures student they have achieved a certain level of English proficiency (i.e. speak, read and write in English). Second, passing IELTS reassure others (i.e. immigration officials, education institutions) that you have achieved a certain level of English proficiency to enable you to work, run a business, or study in an English-speaking country (Dooey & Oliver, 2002).

Assessing an information security standard, ensure organisations implement the best security practice required by the standard as well as assess its effectiveness in protecting organisations' information assets (desirable characteristics or outcome). For the purpose of understanding how to assess standards, subsequent sections will look at type, motivation and criteria for accessing information security standards in section 2.3.1. Section 2.3.2 looks at assessment metrics. Section 2.3.3 look at examples of standards assessments and Section 2.3.4 looks at certification or third-party assessment.

2.2.1 CRITERIA

To identify the criteria for assessing an information security standard, one must first understand the purposes and objectives. According to Fal' (2010), the purposes of developing information security standards is (1) to protect organisations' information that existed in various form and (2) to develop protection mechanisms to mitigate damages due to inadequate information protection. Specifically, a standard based information security management (ISMS) should ensure the Confidentiality, Integrity and Availability of an organisations' information (BSI, 2020a; Tofan, 2011).

The criteria, therefore, for assessing information standards should provide answers to the question. How can a standard demonstrate it can achieve the objectives of protecting organisations' information? Or as Humphreys (2011) put it, what makes a successful information security standard? He answered his question with a list of criteria which include businesses being able to use the standard successfully. Companies saw financial (ROI) and other benefits from using the standard. Businesses being able to protect their critical assets at an affordable price. Businesses being able to use the standard regardless of sector and able to demonstrate “fit-for-purpose” via independent audit.

While Mr Humphrey criteria are valid on their own, they are too narrow and do not address critical areas like an organisations’ culture, security policy, and risk management. Furthermore, compliance or independent auditing only concerns the management of information security, and “technical audit requirements to prove that something is secure or not is outside the scope of the certification body” (Broderick, 2006, p. 10). Instead, information security standards, either process or control based, must address four crucial areas to be effective. Standards must employ a holistic approach in section 2.2.1.1. Standard’s functions and objectives must align with organisations’ processes, priorities and goals in section 2.2.1.2. Standards must use comprehensive risks management processes in section 2.2.1.3, and standards must have continuous improvement processes in section 2.2.1.4.

2.2.1.1 HOLISTIC APPROACH CRITERIA

A holistic approach to information security means “security from the beginning”, i.e. security is not an add-on but an integral part of the organisations’ processes. It means “proactive security”, i.e. proactively assessing the likelihood of attackers exploiting vulnerabilities and threats (Freeman, 2007). A holistic approach addresses what Von Solms and Von Solms (2004) refers to as the ten deadly sins of information security or critical success factors (CSF) in this study. Soomro et al. (2016), Arbanas and Hrustek (2019) provide recent literature reviews of these factors.

Specifically, assessing a standard should include evaluating how well the resulting framework addressed information security’ CSF. For instance, the organisations’ internal and external requirements; management involvement; information security policies; organisations’ culture or rather challenges organisation cultures presents; information security awareness; organisation of information security within organisations; and integration of information security processes with organisation processes.

2.2.1.2 BUSINESS ALIGNMENT CRITERIA

Another criterion to consider when assessing a standard is how well the resulting framework can align its objective with organisations' goals. Business alignment is critical to the effectiveness of information security. A lack of alignment between IT and business groups objectives leads to a security plan that does not reflect the needs of the business (Soomro et al., 2016). Information security objectives cascade down from stakeholders' goals and requirements to businesses' objectives and needs, and then to information security objectives and needs (Yunis et al., 2019). Herath et al. (2010) provide a detailed study on balancing and aligning business objectives and goals using a balanced scorecard model. Essentially, business-security alignment means businesses objectives, values and needs, determined acceptable level of risk and therefore, risk management and treatment processes but not the other way around (Tu et al., 2014). This means organisations should assess standards on how well they can align the functions and objectives with their business objectives and goals.

2.2.1.3 RISK MANAGEMENT CRITERIA

The next criterion is risk management. The argument by Blakley et al. (2001) that information security is information risk management is accepted as the starting point for any security activity. The problem lies not with their reasoning but the risk management process itself. Traditionally, the risk management primary focus was the identification and evaluation of risks to protect physical assets such as infrastructure and hardware (Gerber & von Solms, 2005). However, this is no longer enough given the pervasive use and organisations' overly reliance on technologies. As Bunker (2012), argued that "organisations need to manage information in a way that is both practical and cost-effective as well as being secure, maximizing the reduction in information risk" (p. 21). Specifically, consider information risks from every possible source, for instance, physical or environmental, people, culture, management and organisational risks, and technological risks (Papadaki et al., 2008). Consequently, organisations should assess standards on how effectively their risks assessment, analysis and treatment processes, are gained.

2.2.1.4 CONTINUOUS IMPROVEMENT CRITERIA

The final criterion is continual improvement. It is critical to assess standards, based on how well they can adapt to changes in an organisation information security environment, requirements and objectives. According to Humphreys (2016), the core of the continuous improvement processes is change. This is changes to ensure organisations are managing information security risks, to protect their information assets at all times. “While it is not easy to predict future development in the information security arena, it is clear that there must be continuous improvement in information security standardization and management”.

2.2.2 METRICS

Metrics involved at least two aspects that is, the measure and one or more reference points; and when it is compared for a meaningful result. (Krag, 2009). Combining data from metrics create indicators which provides useful information that metrics cannot provide on its own (Herrera, 2005). A measure is a one-time view of a measured parameter; for instance, five attempted unauthorized access, or percentage of unpatched vulnerabilities (Kajava & Savola, 2005).

Effective metrics and indicators depend on useful measurements. A good measure has several desirable properties, such as being clear, easy to use, objective, and repeatable (Atzeni & Lioy, 2006; Wang et al., 2008). Effective metrics are one that aligned with business goals and security objectives. It must have quantifiable values, simple to measure and results comparable. Metrics should enable corrective actions, security improvement and should target a certain audience, i.e. metrics for technical audiences should bedifferent from metrics for non-technical audiences (Ahmad et al., 2014).

With information security, however, developing effective metrics are not always easy due to the complexity and diversity of information security processes, therefore, it may not always be possible to formulate useful measurements and metrics for every information security process (Atzeni & Lioy, 2006).

Why is an information security metric important? Simple answer: one cannot manage what they cannot measure (Baker et al., 2007). Longer answer: The motivations for many studies and organisations' establishing effective information security metrics are for several reasons. Including but not limited to, the ability to quantify the effectiveness of information security programs, ability to improve information security processes' efficiency, provide useful information to assist management in their decision-making processes, and minimized costs and maximize ROI (Atzeni & Lioy, 2006; Baker et al., 2007).

Organisations today rely heavily on their information assets not only for their day to day operations but also for the (business) resiliency and continuity (i.e. being able to bounce back after a disaster). That means the (business) survival is more and more dependent on the security and resiliency of their information assets ("Comments on Standards in Information Security, Disaster Recovery, Business Continuity and Business Resilience," 2007). Hence, organisations need to ensure the effectiveness of their information security in protecting their information assets. To do that, they need to develop effective metrics.

One of the significant challenges, organisations face when developing effective information security metrics is coming up with measurements and metrics that could provide quantifiable answers to questions such as:

- How secure are the organisation information assets?
- How one knows when their information assets are secure?
- What are the most cost-effective solutions?
- How to calculate the degree of risks?
- How accurate are the risks predictions?
- Is the security program headed the right direction? (Krag, 2009).

Despite studies and progress in developing effective information security metrics, many of the metrics still do not provide adequate answers to the questions above. They still suffer limitations and shortcomings identify in 2005 by Ju An Wang, (2005). For instance, he posits that security metrics are (in many cases) qualitative rather than quantitative, subjective and lack timing aspects. It mostly focuses on measuring security now, which can be meaningless tomorrow.

His arguments and security metrics weaknesses he identified still hold today and remain significant challenges for organisations in developing effective information security metrics, for instance, developing useful metrics for information security assessment based on maturity levels. Information security maturity models provide a consistent, and repeatable way to measure process progress, from an initial state or level until it reaches a final maturity state (reach the process objective(s)) (Hohan et al., 2015; Proença & Borbinha, 2018). The maturity factors, however, are in many cases, qualitative and therefore, factor assessments can be subjective. Even quantitative metrics have qualitative aspects based on subjective analysis, and qualitative metrics tend to measure process progress rather than its effect. Process outcomes, i.e. degree of assets protection because you a process reached a maturity level N, is still mostly based on subjective analysis.

The remainder of this section reviews two different approaches to establishing metrics for measuring information security management system (ISMS) performances. Section 2.2.2.1 reviews the goal-question-metric approach and the section 2.2.2.2 reviews maturity model-based metrics approach.

2.2.2.1 GQM

One of the popular approaches to establishing information security assessment models is the Goal-Question-Metric (GQM) approach. GQM is a top-down approach starting with setting information security goals, asking one or more questions, i.e. identifying indicators, about each goal; whereby answers to questions lead to the attainment of those goals and choosing one more metrics that answer each question (Koziolek, 2008). Organisations' information security goals depending on an organisations' context include evaluating and improving ISMS processes, improvement of information security processes and an organisation's process integration, and provide data to justify and validate information security costs (Tashi & Ghernaouti-Hélie, 2007).

One advantage of the GQM approach is that there is a direct link between metrics and goals which allows organisations to collect data according to their goals, hence reducing measurement overheads (Dalton, 2019; Koziolek, 2008). Implementing GQM involves four phases, planning, definition, data collection, and interpretation (Koziolek, 2008). The planning phase, in the context of information security standards, involved identifying ISMS processes that should be a target for assessment. In other words, one could integrate a GQM planning phase with the ISMS planning phase. Ideally, for ISMS, all processes should be a target for assessment and improvement (Wright, 2006). The definition phase involved establishing goals, questions and metrics according to organisations' information security objectives. The data collection phase involves collecting data and measurements according to goals, questions and metrics established during the definition phase. The final stage, the implementation phase, involves interpreting the data according to the metrics established earlier (Koziolek, 2008).

In their paper, "Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments", Hajdarevic et al. (2017) use a GQM approach to establish security metrics to measure the effect, i.e. risks from BYOD. In their study, they selected ISO 27001 BYOD related controls then identify goals, formulate questions and derive metrics from measuring the effectiveness of controls in minimising risks from BYOD enabling policy. Other studies use GQM to develop metrics for assessing information security, for example Gonçalves et al. (2016). They proposed using GQM to develop metrics to determine information security quality of services, with goals derive using DEMO, a communicative action model. Halabi and Bellaiche (2017) use GQM to develop measurable metrics to quantify the performance of cloud information security services. Weldehawaryat and Katt (2018) use GQM to define information security, assurance metrics based on vulnerabilities and an organisations' information security requirements.

2.2.2.2 MATURITY MODEL

Another type of metrics utilized by many studies uses maturity models. The first maturity model, CMM or the Capability Maturity Model, was developed in 1986 to access capabilities of software companies. The model success is the reason why researchers studied and adapted it to different fields like business process, Information technology (IT), and information security (Proença & Borbinha, 2018). Maturities are discrete states or degrees along a path of evolutional progress of capabilities (being mature, capable, and secure). From ad-hoc and chaotic to discipline, organise and secure (Le & Hoang, 2016; Proença & Borbinha, 2018).

Information security maturity models can either be processes, controls, best practices oriented or hybrid (Alencar Rigon et al., 2014). For instance, O-ISM3 has five capabilities levels; namely, initial, managed, defined, controlled, optimized. The maturity levels are the same as the capabilities levels; however, organisations can select security policies, either from O-ISM3 predefined security processes or from an information security standard according to their resources and requirements. Factors for each maturity level can either be processes, i.e. ISMS processes, controls or policies oriented. A detailed analysis and comparison of existing maturity models can be found in studies by Hohan et al. (2015) and Le and Hoang (2017).

In addition to adopting existing maturity models, organisations can develop their own maturity model that best fit their resources and requirements. For instance, after analysing several maturity models for assessing an ISO 27001 based ISMS, Proença and Borbinha (2018) proposed a new maturity model, they argued best fit ISO 27001 requirements. Their new model consists of five levels adopted from the PDCA improvement cycle (which ISO 27001 uses). The levels are initial, planning, implementation, monitoring and improvement. Requirements or factors for each level follow the requirements for each PDCA phase. Other maturity models either developed for specific purposes or to overcome limitations with existing models, can be found in a literature review study by Rabii et al. (2020).

Using information security maturity models allows organisations to identify gaps, i.e. current state of its information security (Schmid & Pape, 2019) and areas that need improvement. It also helps organisations management processes, risk assessments and support improvements of internal processes and controls (Alencar Rigon et al., 2014).

2.2.3 Examples

This section discusses studies that focus on practical assessments of information security standards. Since the ISO 27000 family of standards are the most widely adopted information security standard today, most of the case studies reviewed here use it as the reference standard. Specifically, the case studies reviewed below provide examples of how studies and organisations assess information security standards.

For instance, Al-mayahi and Mansoor (2012) conducted a gap analysis of several e-government departments in the UAE to determine their level of compliance with the ISO 27001 standards. To make it easier to identify and allocate responsibilities for implementing and managing security controls within each department, they group the security controls domains (categories) into three categories, management, technical and operational controls. For example, the responsibilities for the management controls could be allocated to management, technical responsibilities to IT and operational responsibilities to human resources. Each of those sections will then be responsible for the department's compliance for the controls allocated to them.

To conduct the gap analysis, they first established a maturity model based on the COBIT maturity model. The maturity values of the model were based on a departments' information security requirements, i.e. what they expect from their ISMS. For example, at maturity level zero: no acknowledgement of the needs for controls. At level one: some acknowledgement of the need for security controls. At level two: full implementation of controls but no documentation. At level three: full implementation and documentation of controls. At level four: full implementation and documentation of controls with risk management processes in place and finally at level five: a fully functioning ISMS with continuous risk management processes in place.

To assess each department compliance, they formulated questions based on controls allocated to each section within a department then select relevant staff from each section of each department and interviewed those using formulated questions. They use the data collected from the interviews to determine the maturity level of each section within each department. Sections maturity level scores identify gaps in their implementation and therefore, actions each section need to take to increase their maturity level. For instance, if IT who is responsible for the technical controls has a level three maturity. This means they have not established any risks management and continuous improvement processes.

The above example demonstrates how a process or control-oriented information security standard could be accessed in practice using a maturity model. While it does not directly assess how effective the implemented standard is in protecting information assets, it does ensure organisations fully implemented the said standard. To access the effectiveness of an implemented standard, organisations can develop quantitative metrics using approaches such as GQM. A study by Ahmad et al. (2014) provided a theoretic example for organisations to develop quantitative metrics to access the effectiveness of controls and the resulting ISMS as a whole. In their study, they use GQM to develop metrics based on ISO 27001 security controls. ISO 27001 divided its security controls into several categories. Each category has one or more control objectives, and each objective has one or more controls. By turning each security control into a security goal, they formulate one or more questions whose answers fulfil that goal. Formulating specific questions allows organisations to develop specific metrics to measure and provide answers to those question.

For example, one of ISO 27001 controls is “A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices” (BSI, 2017a, p.11). ISO 27001 provided a detailed explanation and guideline on the purpose and expected outcomes of the control (BSI, 2017b). This helps organisations formulate questions that lead to metrics that measure the effectiveness of the control. A question such as, “how many security instances caused by mobile devices”, can lead to metrics like “daily connected mobile devices”, “daily mobile devices related security instances”, and others. Those metrics means that the company has to collect data on the number of connected mobile devices, the number of mobile devices-related security instances.

The metrics from all the questions combined provide (1) quantifiable measurement of each control performance, (2) measurement of each control effectiveness, (3) can be used as maturity value to measure the overall performance of the ISMS, (4) and can tailor questions and metrics to measure control's effectiveness concerning the organisation security and business objectives. The Nasser and Nasser (2017) study provides an example of using a quantitative maturity model to assess an ISMS. They developed a quantitative maturity model based on the COBiT maturity model to assess the state of information security in the Yemeni Academy for Graduate Studies with ISO 27001 as the reference standard.

They based the maturity value of each level on information they gathered after surveying and interviewing staff in the Yemeni Academy. For example, they assigned a value between 0 and 0.5 for level zero (non-existence). The rest of the maturity levels include level one, 0.51 and 1.50, level two, 1.51 and 2.50, level three, 2.51 and 3.50, level four, 3.51 and 4.50, and level five, 4.51 and 5.0. If the average score of all controls within the domain is <= 0.5, then that domain is assigned maturity level zero, if >= 1.51 and <=2.50 a maturity level one. They calculated the score for each domain by formulating questions regarding each control. The researchers designed the questions to gather as much information from Yemeni Academy staff regarding the extent of security control implementation. Each question is allocated a score depending on the answers. The average score of all questions is the control maturity value.

2.2.4 Certification

Information security standard certification is the process of auditing organisations' ISM to verify the compliance of their information security processes and procedures to an information security standard. Certification assessments which are conducted by an accredited third-party auditing firm provide an international benchmark on assessing organisations' information security (Humphreys, 2016). Specifically, organisations certified to a standard means they have all implemented the same information security best practices mandated by that standard.

Certification is a way for organisations demonstrate to business partners, suppliers, customers and the organisation's management that (1) the organisation is applying all information security best practices to protect its information assets. (2) The organisation's information security is "fit for purpose". (3) The organisation is operating a secure computing environment, employing internationally accepted security best practices to protect their information assets. (4) Minimising the risk of the organisation paying fines or compensation from failing to meet national and international legal and other requirements (Disterer, 2013; Humphreys, 2016).

In addition to its security-related advantages, certification is a way to open new business opportunities. An organisation which has an internationally certified ISM in place is more likely to attract more customers and business partners given the high priorities organisations put on information security today. According to Disterer (2013), it is a probable reason for the high number of ISO 27001 certified organisations in Asia. The rationale: US and European companies would more likely to outsource their operation and services to companies with internationally certified ISMS than to non-certified companies.

The certification process varies depending on each security standard requirements and each organisation's internal processes. For instance, Ferreira et al. (2014) documented the processes, timeline and challenges the State of Minas Gerais (Brazil) took in their effort to certify their ISO 27001 based ISMS. The study objective was to ensure the State's information security is up to standard to protect their information assets, processes and services in preparation for the launching of the State's electronic invoice system. The certification process involved three phases, phase I, gap analysis, phase II, implementation, and phase III, auditing. The process started in 2009, and by the time of their writing, the certification process was still ongoing. Another similar study on the certification process is the Abu Dhabi Gas Industries Ltd. (GASCO) Case Study. GASCO employed the same three phases' process the State of Minas used, i.e. gap analysis, implementation and auditing. (Abu Talib et al., 2012).

Several conclusions come from the above studies, including, organisations must have skilled staff, the certification process can be expensive, and may take a long time. While theoretically, getting certified has advantages as mentioned earlier, some studies conclude that certification is more obligatory rather than because of any real business benefit (Hsu et al., 2016). In other words, certifying standards takes time, and money and processes vary depending on organisations' internal processes and requirements.

2.3 ISO 27001

ISO 27001 is an information security standard which specifies requirements for an information security management system (ISMS). In 2005, the international organisation for standards (ISO) adopted BS 7799 part 2 as ISO 27001:2005. In 2013, ISO released ISO 27001:2013 replacing ISO 27001:2005. ISO 27001 is control-oriented and is the primary standard in the ISO 27000 family of information security standards (BSI, 2017a, 2020a; Disterer, 2013). An analysis of ISO 27001 structure is given in section 2.3.1, security controls in section 2.3.2 and assessments in section 2.3.3.

2.3.1 STRUCTURE

ISO 27001 consists of two major sections. The first section specifies the overall requirements for an ISMS, and the second, specify the security controls. ISO 27001 has seven major requirements. Organisations' context, leadership, planning, support, operation, performance evaluation and improvements (BSI, 2017a).

2.3.1.1 ORGANISATIONS' CONTEXT.

The organisations' context requirements consist of four sub-requirements. (a) Identifying an organisation information security needs, (b) understanding the needs and expectations of interested parties, (c) determining the scope of the ISMS, and (d) establishing an Information security management system (BSI, 2017a).

The first two requirements are critical because different organisations have different information systems and assets, which each has its risks and vulnerabilities. For instances, a private bank (Kaban & Legowo, 2018) will have other information assets and priorities than a manufacturing company (Velasco et al., 2018) or a company utilizing public cloud services (Fajar et al., 2018). Furthermore, by understanding internal and external requirements, organisations would then be able to define an accurate scope of their ISMS; their first steps toward establishing an ISO 27001-based ISMS.

2.3.1.2 Leadership.

The leadership requirement state that top "management shall demonstrate leadership and commitment concerning the information security management system" (BSI, 2017a, p. 2). Leadership requirement consists of three sub-requirements; Leadership commitment, information security policy, information security structure with assigned roles, responsibilities and authorities. Those three requirements are part of the factors studies identified as critical success factors (CSF) for implementing an effective ISMS (Hui-Lin et al., 2014; Kwok & Longley, 1997; Tu et al., 2014).

2.3.1.3 Planning.

The planning requirements specifies activities organisations must implement during the planning phase of implementing an ISO 27001 based ISMS. Like any project, the planning stage is critical for its success. ISO 27001 based ISMS planning stage includes risk management operations (i.e. information security risks assessments, and treatments), and setting the ISMS objectives.

ISO 27001:2013 specifies a risk-based ISMS framework (Humphreys, 2016); therefore, risk assessment is a critical and vital component of the ISMS. A comprehensive risk assessment differentiates between effective and ineffective ISMS. The guidelines for information security assessment for an ISO 27001 based ISMS is provided by ISO 27005. Risk assessments consist of three processes, risk identification, risk analysis and risk evaluation.

Risk identification involves identifying information assets and asking what attack possibilities that could compromise that asset. The process involves identifying the organisations' assets, identifying information security threats, vulnerabilities, existing controls, and consequences (BSI, 2011). A literature review of information risk assessments by Pan and Tomlinson (2016) identified the importance of assets identification in helping organisations identify their risks efficiently. Risk identification is cover in detail by Wei et al. (2018). ISO 27001, however, avoids going into specifics because organisations have vastly different information assets.

Risk analysis, on the other hand, answers questions like how serious the risk is (i.e. risk level) and the likelihood of exploiting vulnerabilities and consequences. Organisations can conduct preliminary risk analysis using qualitative methods and a more detail analysis using quantitative methods on more severe vulnerabilities (take more time) identified by the qualitative methods. ISO 27005 divided risk analysis into assessments of consequences, assessments of incident likelihood, and risk level determination (BSI, 2011). A study by Ayatollahi and Shagerdi (2017) conducting information security risk assessment of hospitals in Iran provides a practical example of how organisations can conduct risks analysis using qualitative and quantitative methodologies.

The final stage in the risk assessment process is risk evaluation. In this stage, organisations decide depending on internal and external requirements, likely consequences, and what the acceptance level for each risk is. Specifically, information security risks are organized and prioritised before preparing a risk treatment plan. Risks prioritization is important for several reasons; organisations do not have unlimited resources to treat every risk; critical risks are urgent (by consequence or requirements like legislative and others); and to ensure a systematic risk treatment plan.

ISMS risk treatment processes are concerned with selecting and implementing security controls to modify risks (Prabhakar & Varati, 2018). A comprehensive risk assessment output is the difference between having an effective or ineffective risk treatment plan. According to ISO 27005, risk treatment options include modifying risks, retaining risks, avoiding risks and sharing (with external parties) risks. Risks modifications involved implementing security controls to treat a risk until the risks reach an acceptable level (for the organisation).

Risks retention concerns with organisations deciding an acceptable level of risk and whether they merit further action (i.e. risk modification). Risk avoidance applies to risks that organisations decide that are too costly or time-consuming to treat, or the risk is too high, therefore, better to remove the sources of those risks. Risks sharing are risks that organisations share with external partners (service providers, e.g. cloud solution providers, business partners, and others). The goal of the risk treatment process is to bring all risks to an acceptable level from an organisation perspective according to their priorities and objectives (BSI, 2011).

The final stage of ISO 27001 based ISMS planning is setting the ISMS objectives and a plan to achieve them. The information security objective should tie together requirements of earlier stages (i.e. organisation internal and external needs, policy, and risk assessments and treatments). According to ISO 27001, the objectives should be measurable if practical, communicated to all stakeholders, and kept up to date. After setting their information security objectives, organisations should formulate and document a plan on how to achieve those objectives. Once organisations finalized their information security plan, they can decide on the resources required, staff responsible, deadlines for completing each of their objectives, and how to measure the achievement of each objective(BSI, 2017a).

2.3.1.4 SUPPORT

The fourth requirement is the support requirement. The support requirement consists of three sub-requirements; resources, competence, awareness, communication and documentation control. From an ISO 27001 perspective, at this stage, all planning has been completed and properly documented, ready for the organisation to assess and allocate resources (financial and staff) for implementing those plans.

For instance, organisations needed to ensure they have the right staff to ensure successful implementation of their ISMS project. They can either train their own staff or hire external experts (individuals or consultancy company) (BSI, 2017a). ISO also provides ISO 27021 to help organisations determine the right staff for each of their ISMS roles. The NICE skills framework by ISC2 is another competence framework that can help organisations identify the right people for each ISMS role.

It is also critical to communicate details of the ISMS project (motivation and justification, policy, objectives) internally within the organisation (to ensure everyone is aware of their roles, and relevant changes to organisations' processes and procedures, if any). Organisations at this stage should determine what information they need to communicate to who and when. For instance, to the government due to legislation requirements, to business partners due to partnership agreements, and suppliers and customers (BSI, 2017a).

A well-communicated information security policy facilitates developing a positive information security culture which is critical to the effectiveness of an ISMS. A well-implemented and maintained ISMS is useless if employees do not support and follow information security processes and procedures (Stewart & Jürjens, 2017). Therefore, a well-formulated information security awareness program can have positive effects on an organisations' information security culture and vice versa (Wiley et al., 2020).

Finally, organisations must ensure the continuous maintenance of documentation of all processes (ISMS scope, policy, plans, controls selections, and others) using a versioning system. A well-formulated and updated documentations help with internal auditing, management review, external auditing for certification (if desired), and review by business partners, new staff to get up to date with the project quickly, and continuous improvement of the ISMS.

2.3.1.5 OPERATION

The operation requirements specify activities organisations must perform during the operation phase of an ISMS. Activities include implementing the risk treatment plan, ensures updated documentation, and ensure organisations determined their outsourced processes (i.e. to solution providers, business partners, and others). Security controls are in place to manage those processes (BSI, 2017a). An important part of the operation phase is regular risk assessment since it contributes to the long term continuity, and the effectiveness of the ISMS. Continuous, regular risks assessment is critical due to the changing nature of threats and vulnerabilities (Stewart et al., 2015).

2.3.1.6 MONITORING, MEASURING, ANALYSIS AND EVALUATION.

These requirements dictate processes for “monitoring, measuring, analysis and evaluation” (BSI, 2017a, p. 7) of the ISMS, doing regular internal audit and management review. ISO 27004 and ISO/IEEE 15939:2017 provide detailed explanation of the measurement model used, guidelines, and examples on how to monitor, measure, analyse and evaluate the ISMS (BSI, 2016a, 2017c). A comprehensive measurement and evaluation plan helps organisations not only to evaluate the ISMS implementation but also to assist management with their decision making regarding the future of the ISMS project.

The ability to measure and evaluate the ISMS processes enable organisations to measure the overall effectiveness of the ISMS project by identifying and measuring information security indicators over time. Indicators or targets are measured information value when measuring a particular entity (project, processes, and controls). For instance, the percentage of ISMS completion and the information security incidents; such information will give the organisation indication on the effectiveness of the ISMS. Another target/indicator is the percentage of policy reviewed or percentage of policy reviewed and the information security incidents. Those are measurement targets/indicators for policies (an identity). For internal usage, measurements can be done by the internal auditing teams or by second party information security auditors. ISO 27007 provides guidelines for internal auditing (BSI, 2020b) both for internal auditors (first-party) and external auditors (second party).

2.3.1.7 CONTINUOUS IMPROVEMENT

The continuous improvement requirements emphasise the need for organisations to improve their ISMS continuously. Continuous improvement is critical for the continued effectiveness and relevancy of the ISMS. Organisations' compliance (to ISMS policies and requirements) is not a product but a continuous process that needs continual maintenance (review, modify and update) to gather data on the dynamism of the organisation information security environment (H. Stewart & Jürjens, 2017).

The 2005 version of ISO 27001 continuous improvement was based on the PDCA improvement cycle with auditing as the tool for measuring the ISMS performance for management review. Auditing as a tool for continuous improvement, however, was criticized because its focus is mainly on measuring an organisations' compliance (with policies and best practices). It does not measure the effectiveness of audited policies and best practices. Another criticism is that auditing results depend mainly on the skills and experience of auditor(s) as well as other factors which makes auditing output unpredictable (i.e. it's subjective) and therefore unreliable as a performance measurement tool (Hohan et al., 2015).

The need for a reliable way to measure the ISMS performance led to the release of ISO 27004 in 2009 which provides guidelines on how to measure, analysed and evaluated the performance of an ISO 27001 based ISMS. In doing so, it removed auditing as the only tool for continuous improvement because organisations can develop their measurements and metrics to measure the ISMS performance according to their requirements.

The 2013 version of ISO 27001 (current version) also removed references to the PDCA improvement model thereby removing the emphasis on the order of implementation (of the ISMS requirements) (Prabhakar & Varati, 2018; Shojaie et al., 2014). Organisations, however, can still apply the PDCA improvement cycle by allocating ISMS requirements to each of the PDCA stages. For instance, The Planning phase can include the context of the organisation, leadership and planning requirements, the Do phase can include the support and operation requirements, the Check phase include performance evaluation requirements, and the Act phase can include the continuous improvement requirements (Carvalho & Marques, 2019). The main difference is that auditing is no longer the main tool for continuous improvement. Studies also proposed using maturity models for measuring, analysis and evaluating

ISMS performance for continuous improvement (Alencar Rigon et al., 2014; Hohan et al., 2015).

2.3.2 Controls

Security controls made up the majority of ISO 27001. Specifically, ISO 27001 has 114 security controls divided into 35 objectives and 14 categories. (BSI, 2017b). ISO 27002 provided the same controls but with guidelines on how to select and implement the security controls (BSI, 2017b). ISO 27001 based ISMS achieves information security by requiring organisations to select and implement security controls which deal with an organisations' information security policies, procedures, processes, organisation structure, and hardware and software functions (BSI, 2017b). From the organisation perspective, Humphreys (2016) categorisation of the same security controls provides an overview of the controls: 1. Policies and procedures. 2. Human resource security. 3. Access control methods. 4. Operation security. 5. Communications security. 6. Physical and environmental security.

Table 2.1 lists all the security control categories, objectives for each category and the number of controls per objective. As noted from the controls objectives in Table 2.1 and appendix A of ISO 27001, the ISO 27001 security controls are generic (BSI, 2017a). They lack specific implementation details because they focus on specifying control outcomes instead of specific implementation details. It enables organisations with diverse information environment and needs to implement the standard regardless of organisations' type, size and resources. For example, in the UAE, organisations from different sectors such as banking, health, industries, and government departments all implement the standard despite their diverse information environment and requirements (Abu Talib et al., 2012).

A simple analysis of the security controls in ISO 27001 Appendix A, demonstrates the advantage of leaving specific implementation details to organisations. For instance, control, A.13.1.1, stated that "Networks shall be managed and controlled to protect information in systems and applications"(BSI, 2017a, p. 17). It is a statement of expected outcome rather than specific requirements or processes. For SMEs, for example, they can meet the control requirements by merely implementing access control policies, and layered firewalls detailed by Boyle and Panko (2015).

ISO 27001 security controls lack of specific details mentioned above, led to criticism that the use of security controls for risk treatments is unclear and complicated due to their lack of detail, and the number of processes involved (Anttila & Jussila, 2017). While such criticism has merit, the standard is flexible enough for organisations to adapt and implement it according to their requirements and needs. For instance, instead of rigidly adhering to the ISO 27001 14 categories, organisations can re-organise security controls into categories based on threats, information assets risks, and information assets categories (Shojaie et al., 2014; C. Wang et al., 2018).

Reorganizing security controls into familiar and statically defined categories allows organisations to understand security controls by putting them into a context organisations can easily understand and fit into their environment (Shojaie et al., 2014; Wang et al., 2018). The categorisation of security controls into categories organisations can understand is a challenge. This includes selecting, documenting and stating "the relationships between the identified risks and what countermeasures were implemented – and why" (Wright, 2006, p. 1). A study by Achmadi et al. (2018) shows how categorisations can help organisations select the appropriate (in terms of cost and performance) controls according to their requirements. Categorisation and the flexibility of security controls are especially helpful to SMEs. It allows them to identify, select and implement security controls relevant to their requirements within their limited budgets and resources (Shojaie et al., 2014).

Security controls are the risk treatment tools of ISO 27001 based ISMS, therefore identifying, selecting and implementing the right controls is key for an effective ISMS (BSI, 2020a). Figure 2.2 below shows the control selection process, based on an organisation risk treatment plan (output of an organisation risk assessment process) and their information security objectives.

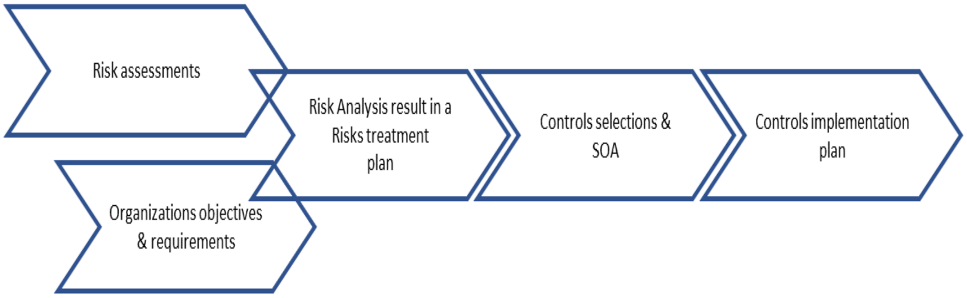

Risk assessments
Organizations objectives & requirements
Risk Analysis result in a Risks treatment plan
Controls selections & SOA
Controls implementation plan

Figure 2.2: Controls selection processes

Processes are implied but not specifically stated in ISO 27001.

During the planning phase an organisation conducts risk assessment and analysis of its information assets according to its business objectives, priorities and requirements, and has a risk treatment plan as the output. Security controls are selected and documented according to the risk treatment plan. During the operating phase, organisations implement the selected controls. These processes are repeated at regular intervals to keep up with the organisation's changing information assets and information security threat environment (BSI, 2017a).

The ISO 27002 standard is provided as a companion standard to the ISO 27001 standard; providing guidelines on control objectives and possible implementation scenarios. Specifically, the ISO 27002 helps organisations to make informed decisions on controls, and to select and implement them according to their risk treatment plans. As a result, the ISMS will be better aligned with the organisation information security and business objectives (BSI, 2017b).

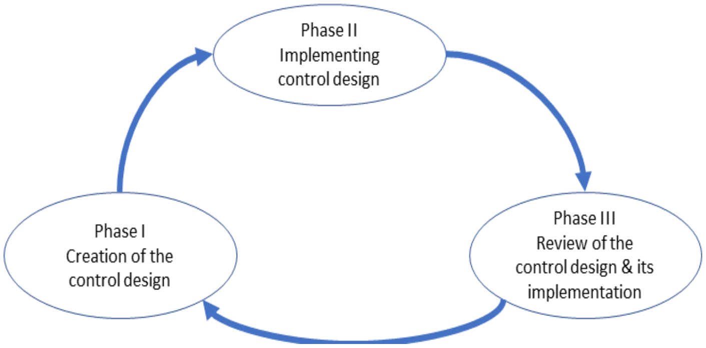

Phase II
Implementing control design
Phase III
Review of the control design & its implementation
Phase I
Creation of the control design

Figure 2.3: Generic controls management cycle in EU organisations

Adapted from Bachlechner et al. (2011)

According to ISO 27000, organisations' objectives should be to "monitor, evaluate and improve the efficiency and effectiveness of information security controls and to support the organization's aims" (BSI, 2020a, p. 16). In other words, security controls management is a key component of an ISO 27001 based ISMS. According to a study by Bachlechner et al. (2011), after interviewing information security professionals from various European organisations regarding their security control management processes. They came up with a three-phase, generic security control management cycle in Figure 2.3, which they contended summarised and captured control management processes employed by participant's (interviewees) organisations.

Table 2.1: Security controls, objectives and number of controls

	Categories	**Objectives**	**Controls**
A.5	Information security policies	(a) Provide management direction and support in accordance with business requirements and relevant laws and regulations	(a) 2
A.6	Organisation of information security	(a) To establish a management framework to initiate and control the implementation and operation of information security within the organisation (b) To ensure the security of teleworking and use of mobile devices.	*(a)* 5 *(b)* 2
A.7	Human resources security	(a) To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered (b) To ensure that employees and contractors are aware of and fulfil their information security responsibilities (c) To protect the organisation's interests as part of the process of changing or terminating employment	*(a)* 2 *(b)* 3 (c) 1
A.8	Asset management	(a) To identify organisational assets and define appropriate protection responsibilities (b) To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation (c) To prevent unauthorized disclosure, modification, removal or destruction of information stored on media	*(a)* 4 *(b)* 3 (c) 3
A.9	Access control	(a) To limit access to information and information processing facilities	*(a)* 2 *(b)* 6 *(c)* 1

		(b) To ensure authorized user access and to prevent unauthorized access to systems and services (c) To make users accountable for safeguarding their authentication information (d) To prevent unauthorized access to systems and applications	(d) 5
A.10	Cryptography	(a) To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and or integrity of information	(a) 2
		(a)	(a)
A.11	Physical and environmental security	(b) To prevent unauthorized physical access, damage and interference to the organisation's information and information processing facilities (c) To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations	(b) 6 (c) 9
A.12	Operations security	(a) To ensure correct and secure operations of information processing facilities. (b) To ensure that information and information processing facilities are protected against malware (c) To protect against loss of data (d) To record events and generate evidence (e) To ensure the integrity of operational systems (f) To prevent exploitation of technical vulnerabilities (g) To minimise the impact of audit activities on operational systems	*(a)* 4 *(b)* 1 *(c)* 1 *(d)* 4 *(e)* 1 *(f)* 2 (g) 1
A.13	Communications security	(a) To ensure the protection of information in networks and its supporting information processing facilities (b) To maintain the security of information transferred within an organisation and with any external entity	*(a)* 3 (b) 4
A.14	Systems acquisition, development and maintenance	(a) To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks (b) To ensure that information security is designed and implemented within the development lifecycle of information systems (c) To ensure the protection of data used for testing	*(a)* 3 *(b)* 9 (c) 1

A.15	Suppliers relationship	(a) To ensure protection of the organisation's assets that is accessible by suppliers (b) To maintain an agreed level of information security and service delivery in line with supplier agreements	*(a)* 3 (b) 2
A.16	Information security incident management	(a) To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	(a) 7
A.17	Information security aspects of business continuity management	(a) Information security continuity shall be embedded in the organisation's business continuity management systems (b) To ensure availability of information processing facilities	*(a)* 3 (b) 1
A.18	Compliance	(a) To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements (b) To ensure that information security is implemented and operated in accordance with the organisational policies and procedures	*(a)* 5 (b) 1

2.3.3 ASSESSMENTS

Assessing the implemented ISMS is critical to the effectiveness of any ISO 27001 based ISMS (Humphreys, 2016). This section reviewes three types of assessment identified by previous information security studies and according to the ISO 27001 requirements. First, section 2.3.3.1 reviews gap analysis assessments, section 2.3.32 reviews internal auditing assessments and section 2.3.3.3 reviews external auditing for compliance.

2.3.3.1 GAP ANALYSIS

Gap Analysis is the process of assessing existing information security against the ISO 27001 requirements. In most cases, studies conduct gap analysis using some type of survey; either by interviewing relevant staff or by using a questionnaire (Candiwan et al., 2016). Gap analysis is important not only prior (i.e. as part of planning) (Candra et al., 2017; Nasser & Nasser, 2017) but also during or after an ISMS implementation, to give to keep track of the implementation progress or identify areas to improve (Fajar et al., 2018). The studies reviewed below demonstrated two applications of gap analysis, i.e. assessment before implementation and assessment during or after implementing an ISMS.

The first study is by Kurnianto et al. (2018). Their study aimed to identify gaps in the Ministry of internal affairs, Indonesia's information security when compared to the ISO 27001 requirements and controls. The outcomes of their study were the identification of areas of weaknesses in the Ministry's information security which they put together in a roadmap and recommendation to the Ministry for improvement. Another study was by Al-mayahi and Mansoor (2012). They did a case study of four government departments in the UAE to "identify the weakness in the existing system and highlight associated risks to the UAE e-government" (para. 1). The study was part of the UAE government's preparation to establish an ISMS for its e-government services.

The second study by Candiwan et al. (2016) demonstrated using gap analysis as a way to identify areas of improvement of an organisation's existing ISM. They conduct the study in response to several security incidents in the organisation. They use a maturity model to analyse implemented security controls against ISO 27001 requirements. As a result of their analysis, they identified four areas of weaknesses, which were security policies, human resources security, access control and operational security. Another gap analysis study aimed to assess and improve an ISMS was by Fajar et al. (2018). Their case study focuses on assessing the information security of a company who has already implemented ISO 27001:2013. The motivation for the study was "to know the extent to which the process has been applied and what actions can be done to improve the performance of the application of ISO 27001: 2013" (p. 2). Their study identified several non-compliant security controls which they combined to form their study's recommendation to the organisation on areas to improve.

2.3.3.2 INTERNAL AUDITING

Another type of assessment is an internal audit for monitoring the progress of an ISO 27001 based ISM implementation or assessing an existing ISM for improving its efficiency and effectiveness (Humphreys, 2016). Internal auditing can be conducted by an internal auditing team or by business partners, consultancy firms, government, and other parties that have a vested interest in an organisation having effective information security (BSI, 2020b).

Internal auditing is an integrated component of any ISO 27001 based ISM because it is vital the health and continual effectiveness of organisations' information security (Broderick, 2006; Humphreys, 2016). In addition to the requirements in ISO 27001, the ISO 27000 family of standards comes with standards to help organisations effectively audit their ISMS. For instance, ISO 27004, provides guidelines on how organisations' can monitor, measure, analyse and evaluate their ISM (BSI, 2016a). An auditing team can later make use of such data to analyse organisations' information security. Another useful standard is ISO 27007, which provides guidance to help an organisation audit their information security (BSI, 2020b). ISO 27007 guidelines include how to manage an ISMS auditing programme, how to conduct audits, and also relevant competencies that ISMS auditors should have (BSI, 2020b). Another useful standard is ISO 27008, which aimed to help organisations, review and assess organisations' implemented security controls (BSI, 2019b).

Organisations can use Internal auditing to assess implemented controls according to previously established metrics and measurements, according to guidance provided by ISO 27004 or just assess the implementation status of each control using gap analysis as discussed in 2.3.3.1. The benefit of assessing controls based on ISO 27004 is that organisations can set goals, objective or target for each control and then established measurements and metrics to measure the performance of each control using those measurements and metrics (BSI, 2016a). Readers will find more details on measuring and auditing of ISO 27001 in a paper by Johnson (2014) and a book by (Humphreys, 2016).

2.3.3.3 COMPLIANCE AUDITING

The final assessment is the assessment for compliance and certification. In this assessment, organisations assess their ISMS by how they measure up to ISO 2700 based on seven key elements: establish, implement, operate, monitor, review, maintain and improve the ISMS (Tofan, 2011). A third-party, certified auditing body is the only body allowed to do compliance and certification auditing (Humphreys, 2016). The credentials, competences of auditors, and other requirements auditing bodies must fulfil to be able to audit ISO 27001 based ISMS is provided by ISO 27006 (BSI, 2015a).

While third-party auditing for certification is optional, a study by Park et al. (2010) on the effect of ISO 27001 certification of organisation performance found that (1) ISMS certification leads to positive public relations, better corporate image, which can lead to new customers and sales increase, (2) ISMS certification leads to information security reliability which leads to transactions stability, (3) ISMS certification leads to information security reliability which has positive effects on trust, and (4) ISMS certification helps motivate employees which leads to better employee capability and awareness of information security. According to Humphreys (2016), ISO 27001 certification allows organisations “to demonstrate that their information security was fit for purpose” (p. 16). Consequently, it gives the organisation customers, business investors, shareholders and trading partners, assurance of the effectiveness of their information security.

Despite positive appraisal of ISO 27001 certification discussed above, Park et al. (2010) acknowledge that it is difficult to translate the benefits of effective information security into (quantifiable) values. Specifically, ISMS certification benefit organisations, even if those benefits are not measurable. The conclusion is also reached by Hsu et al. (2016). They concluded, despite major limitations affecting the outcome of their study, that “the nature of ISO 27001 certification results in significant findings and that ISO 27001 is more an obligation but a competitive advantage” (p. 4847).

The previous discussion has highlighted the challenges organisations face in being motivated to certify their ISO 27001 based ISMS because its benefits are hard to quantify and measure. However, that the benefit of having effective information security is indisputable and quantifiable in financial value (costs of successful attacks), service and products quality and availability (customers by secure products and services), and good business reputation (Boyle & Panko, 2015).

The challenge is organisations proving their information security is effective. Producing statistics in many cases, prove nothing, what they need is to be able to measure their information security against an internationally accepted standard. That is where ISMS certification is beneficial because certifying an ISMS to an International Information standard, that contains internationally accepted information security best practices (Humphreys, 2011; Tofan, 2011), implies effective information security.

2.4 Security Control Frameworks

The common definition of the framework, according to Stamer et al. (2016), “is a structure underlying ‘something’ serving a specific purpose”. According to the (Oxford Learner’s Dictionaries, n.d.), it is “a set of beliefs, ideas or rules that are used as the basis for making judgements, decisions”. Unlike standards which specify specific requirements that organisations must implement, an information security framework provides a conceptual, high-level model of relevant policies, procedures, and processes, organisational structures, and other relevant factors, that facilitates effective management of Information Technology (IT), maximizing IT value while minimizing risks.

To better understand security control frameworks and how they fit in with other information security frameworks and standards, this section will focus on three of the most well-known security frameworks today in the following sections. Control Objectives for Information and Related Technologies (COBIT 2019) in section 2.4.1, Payment Card Industry Data Security Standard (PCI-DSS 3.1) in section 2.4.2 and IT infrastructure library (ITIL 4) in section 2.4.3.

2.4.1 COBIT 2019

COBIT is an IT governance framework whose objective is to support understanding, designing and implementing the management and governance of enterprise IT. ISACA first released COBIT in 1996 as guidance to auditors. They later added security controls guidance in 1998 with more functionalities added in subsequent versions in 2000, 2005 and 2007, culminating in the release of COBIT 5 in 2012, as a full framework for all governance activities. The latest version, COBIT 2019, was released in 2018 (Harisaiprasad, 2020; Tessin, 2016). According to Lainhart (2018), during the last two decades, starting from COBIT 5, COBIT focus has shifted to enterprise governance of information and technology (EGIT) due to organisations increasing dependence on IT for risk management and value generation.

What is enterprise governance of IT? According to Weill and Ross (2004), IT governance is the process of "specifying the decision rights and accountability framework to encourage desirable behaviour in IT" (p. 8). While the above definition points readers in the right direction, it lacks specificity, which leads to more questions than answers. It does not provide a complete picture of the why who, and how of IT governance, for instance, who allocate the decision right or what is desirable behaviour in IT. Another definition is found in a paper by De Haes and Grembergen (2004), they provided two definitions one of which is,

> *IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategy and objectives (para. 2)*

A combination of the two definitions, however, provide a clearer definition that encapsulates all aspects of IT governance. It is the process by which organisations (specifically, the board of directors and executive management) ensures that their IT resources (by specifying the decision rights and accountability framework) to help the organisation fulfil its objectives (while encouraging desirable behaviour to minimize risks). According to Hamidovic (2010), IT governance has five focus areas: 1. Delivering value. 2. Risks management. 3. Strategic alignment. 4. Resources management. 5. Performance measurement. The first two are desirable outcomes of IT governance (ITG) and the rest are drivers or enablers of IT governance.

IT governance is distinct from IT management, where IT governance is about assigning roles and responsibilities, i.e. determines who make the decisions, whereas management is concerned with making and implementing those decisions. Figure 2.5

depictes a simplified model of IT governance showing the relationship between governance and management.

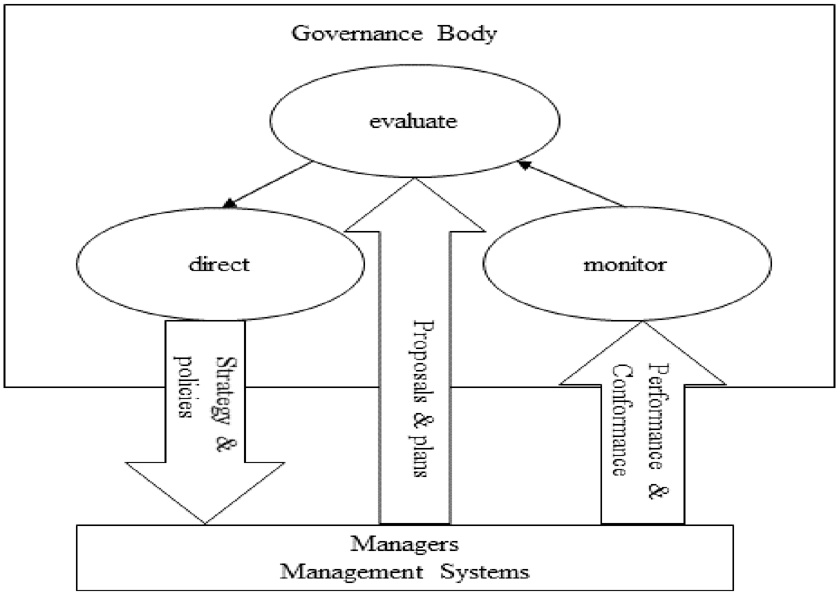


Figure 2.4: ITG Model

Adapted from Calder (2019)

Six principles govern the COBIT governance framework (Braga, 2020; Thomas, 2018).

- providing stakeholders value by using IT to facilitate value creation
- employs a holistic approach
- responsive to change
- has governance structure distinct from management
- tailored to enterprise context (size, resources, and requirements)
- All stakeholders (management, Enterprise Governance of IT (EGIT) board, auditors, and others) regularly working together constructively.

It means, for instance, that organisations COBIT based EGIT must be responsive to change. From individual processes and activities to the overall structure of the EGIT. Furthermore, organisations must tailor EGIT according to their context (objectives and requirements) to facilitate IT value creation. Specifically, organisations must design every objective, process, and activity to adhere to the above principles with no exception.

The COBIT 2019 consists of the core model, which is made up of 40 management and governance objectives, divided into five domains, one governance and four management, depicted in Figure 2.6 (Braga, 2020). Each objective has one or more processes with each process having one or more activities with each activity assigned a target capability level (i.e. ideal activities outcomes). Moreover, each objective must have an organisational structure which specifies roles and responsibilities for the processes and activities. It must also have information flows and items, to specify how processes relate to other processes (within the objective or other objectives). Furthermore, each objective must have people skills and competencies which specifies relevant competences of staff required to implement and manage processes and activities, to achieve the objective. Finally, each objective must have culture, ethics and behaviour, which specifies what cultural and ethical behaviours within the organisations that facilitate the achievement of the objective (Thomas, 2018).

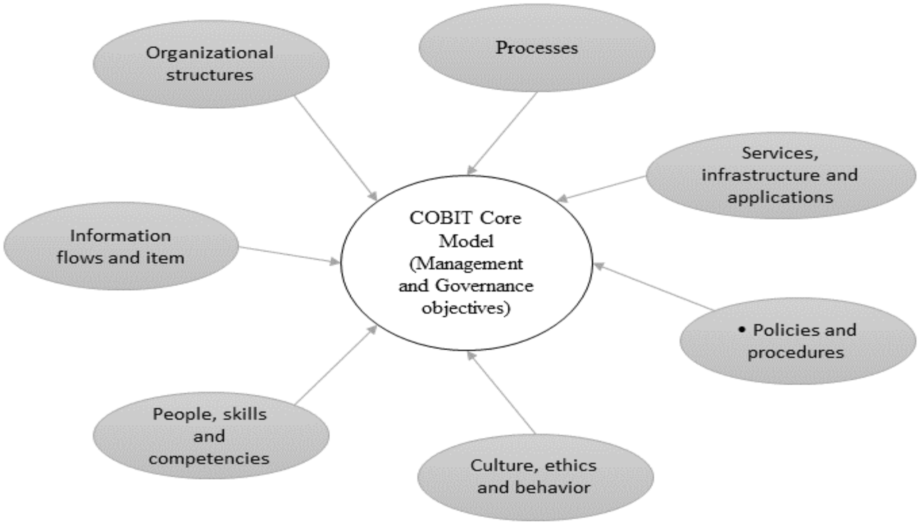

Organizational structures
Processes
Services, infrastructure and applications
Information flows and item
COBIT Core Model (Management and Governance objectives)
• Policies and procedures
People, skills and competencies
Culture, ethics and behavior

Figure 2.5: COBIT 2019 Core model & Components

Adapted from Braga (2020)

COBIT is an IT governance framework, meaning, it is a framework to govern all areas of an organisation’s IT, including information security. Therefore, unlike information security frameworks, it has a much broader focus. Consequently, its coverage of some areas are weak (Fazlida & Said, 2015) and not as detail as protocols like ISO 27001 or PCI-DSS. Several studies (Ozdemir et al., 2014) have attempted to compare these standards (COBIT, ISO 27001, and ITIL) and expresses sentiments such as "it is difficult to compare these standards", and misguided question like "Which one of the abovementioned standards should be applied to ensure information security?" It is obvious one cannot compare these standards are they focus on different areas and therefore, have a different emphasis.

However, a brief analysis of the protocols and frameworks, shows that they are complementary in many ways and not mutually exclusive (Mataracioglu & Ozkan, 2011). IT governance (COBIT) has the broadest focus since it deals with the overall governance of IT. IT Services management (ITIL), information security (ISO 27001, PCI DSS) has a much narrower focus. Figure 2.6 depicted overlapping functions of different standards within an organisation. As Mataracioglu and Ozkan (2011) stated, "several standards like ISO 27001, describe the duties more comprehensively than does COBIT" (p. 112), therefore, should consider standards like ISO 27001 when implementing EGIT.

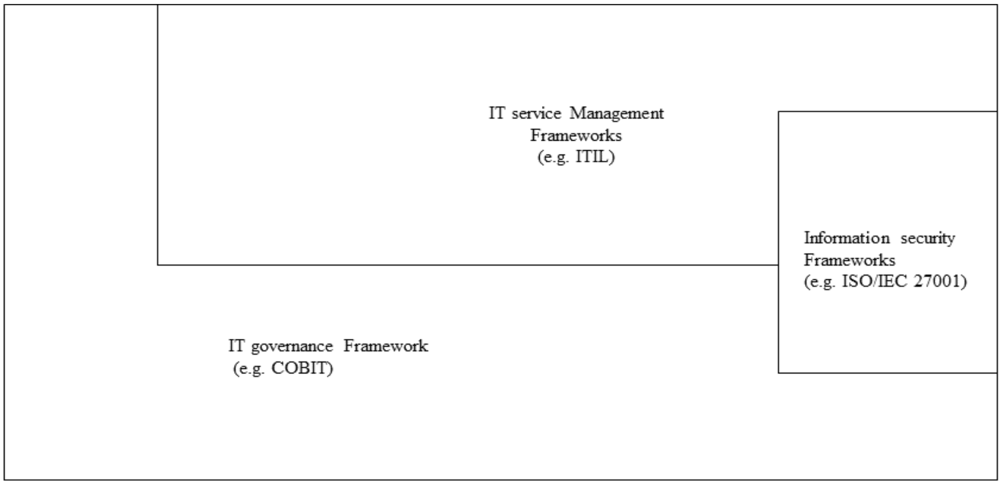


Figure 2.6 Overlapping Standards

Adapted from the reviews of ITIL, COBIT and ISO 27001

What it means is organisations can implement different standards and frameworks to provide comprehensive governance of organisations IT operations and services while ensuring the security of their information assets. For instance, Mataracioglu and Ozkan

(2011) provided a brief overview of how organisations can integrate COBIT and ISO 27001. Kusumah et al. (2014) did a case study integrating COBIT and ITIL. They concluded that "The suitable information security governance in service management systems for INTRAC is collaborative integration of COBIT 5 and ITIL framework" (p. 5). Another case study by Fathoni et al. (2019) uses COBIT and ISO 27001 to build an information security governance system for a bank in Indonesia. The framework was based on COBIT with ISO 27001 as a guide for the information security aspect of the established information security governance system.

Other studies have demonstrated that COBIT can be customized to focus on specific areas instead of all aspects of IT governance. For instance, a case study by Wolden et al. (2015) uses COBIT as an information security framework. Their study findings indicate that "with proper management of rules, responsibilities and policy, an organisation" can "enjoy the effective implementation of the COBIT 5 Information Systems (IS) security framework" (p. 1851).

2.4.2 PCI-DSS Version 3.1

PCI-DSS, which stands for Payment Card Industry Data Security Standard or the PCI Security Standard, is an information security standard, targeting organisations that handle credit/debit cardholders' information. These include major cardholders like American Express, Visa Inc., and MasterCard (Morse & Raval, 2008). The primary objective of PCI DSS is the security of the storage, processing and transmission of cardholders' data. A study by Morse and Raval (2008) provides details on the card payment industries, relationships between customers and merchants and the role PCI DSS plays within the industry, to ensure the security of cardholders' information.

PCI SSC released PCI DSS version 1.0 in 2005, version 2 in 2010 and version 3.0 in 2013. The current version, 3.2.1, was released in 2018. While initially, PCI DSS aimed to follow a three years release cycle, this was scrapped after the release of version 3.0. PCI DSS instead opted for a more frequent update to keep up with the dynamic nature of information security threats. For instance, PCI SSC released version 3.1 to deal with security threats posed by SSL and an early version of TLS protocols.

Version 3.1 required organisations to replace SSL and an early version of TLS with TLS version no earlier than 1.2 or IPsec (Calder & Williams, 2019).

The PCI DSS standard contains “standardised, industry-wide set of requirements and processes for security management, policies, procedures, network architecture, software design and critical protective measures” (Calder & Williams, 2019, p. 10). Unlike COBIT and ITIL, which provides a management framework for organisations to follow, PCI DSS is a standard with specific requirements that organisations that process, store or transmit cardholders’ data must implement to comply with the standard.

PCI DSS requirements consist of 6 control objectives and 12 requirements. Table 2.3 provides a list of control objectives and requirements. In addition to the main compliance requirements, additional requirements provided in Appendix A1, A2, and A3 for specific cases. The latest version of the standard, version 3.2.1 allows for more flexibility in how organisations can implement the standard, for instance, Appendix B allows organisations to employ compensating control instead of the required control as long as the risk to cardholder data is minimized. This flexibility is well suited for organisations with limited resources or circumstance beyond their control; they cannot implement the full control requirements (PCI SSC, 2018a).

For organisations to comply with the standard, they must implement all requirements of the standards. These include combinations of technical, management, and policies requirements. An example of a technical requirement is “organisations must configure firewall and router to restrict access by untrusted networks to systems that handle cardholder data”. An example of a policy requirement is “organisations must have a firewall and router configuration standards”. Specifically, each of PCI DSS’s requirements consists of sub-requirements which are either technical, management, policy requirements or information security best practices. Readers will find additional details on each of the requirements in the standard specification (PCI SSC, 2018a) and a book by Calder and Williams (2019). A quick reference guide for the standard can be found at (PCI SSC, 2018b), useful for organisations as a checklist of requirements they must implement for compliance.

PCI DSS compliance is critical for the security of cardholders' data and their customers. The number of successful attacks on cardholder data illustrates the importance of cardholder data. Calder and Williams (2019) discuss details of successful attacks on cardholder data with devastating consequences. Notable examples include the attack on British Airways, Ticketmaster UK, and Earl Enterprises.

Table 2.2: PCI DSS controls & requirement

Adapted from PCI SSC (2018a)

Control objectives	Requirements
Build and maintain a secure network and systems	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data **Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	**Requirements 3:** protect cardholder stored data **Requirements 4:** encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**Requirements 5:** protect all systems against malware and regularly update anti-virus software or programs **Requirements 6:** develop and maintain security systems and applications
Implement strong access control measures	**Requirements 7:** Restrict access to cardholder data by business need to know **Requirements 8:** Identify and authenticate access to system components **Requirements 9:** Restrict physical access to cardholder data
Regularly monitor and test networks	**Requirements 10:** Track and monitor all access to network resources and cardholder data **Requirements 11:** Regularly test security systems and processes
Maintain an information security policy	**Requirements 12:** Maintain a policy that addresses information security for all personnel

Consequently, PCI DSS compliance is a requirement of all major global payment brands. It means that every merchant, service providers and financial institutions that stores, processes or transmits payment card data in whatever form, regardless of business type and size, must comply. While PCI SSC does not penalise non-compliance directly, individual payment brands (provider) for instance, financial institution, have penalties which may include financial (penalty fee) or operational penalties (suspend operation) or both.

For organisations to certify their compliance, they have two options: 1. Conduct annual on-site security audit by a qualified security assessor (QSA) or internal security assessor together with results of quarterly network scans by an approved scanning vendor (ASV) (Coburn, 2010). 2. Conducting and submitting a Self-Assessment Questionnaire (SAQ) together with quarterly network scans. Whether organisations can choose option 1 or 2 depends on the number of transactions they process and whether they have suffered any successful attack (Calder & Williams, 2019). SAQ is a self-assessment tool provided by PCI SSC to help organisations which handle cardholder data to internally assess their compliance with the standard (Calder & Williams, 2019). The requirements for QSA is provided by (PCI SSC, 2008) and ASV qualification and requirements are specified by (PCI SSC, 2017).

Since PCI DSS has a much narrower focus than other frameworks and standards, it can be integrated and implemented as part of other frameworks like COBIT, ISO 27001, and ITIL. For instance, a comparative analysis of PCI DSS and ISO 27001 requirements (Lovrić, 2012) reveals PCI DSS requirements are within ISO 27001 requirements. Therefore, ISO 27001 compliance organisations only need “minor additional work, to also demonstrate their conformance with the PCI DSS” (Calder & Williams, 2019, p. 50) standard.

While PCI DSS aim is to protect cardholders’ data, it is general enough for organisations to implement it by itself or as part of other frameworks like ISO 27001 or COBIT to protect their critical data. PCI DSS requirements are much more specific and therefore actionable than other frameworks; meaning organisations can implement it quickly as a basis for more extensive implementation with ISO 27001 for example. Specifically, PCI DSS can be used as an information security framework to protect organisation information assets and not just cardholders’ data.

2.4.3 ITIL VERSION 4

The IT infrastructure library (ITIL), first published toward to end of the 1980s as a series of books containing best practices for IT service management (ITSM).

According to AXELOS Limited (2019), the maintainer of the guidance, it is the most widely adopted ITSM guidance in the world.

The UK Government agency, Central Computer and Telecoms Agency (CCTA) was the agency who created ITIL. They started working on ITIL to develop a common set of operational guidance to increase efficiencies in Government IT (Cater-Steel et al., 2009). CCTA later transfer ITIL to AXELOS, who is the current maintainer of the framework.

ITIL next major update, ITIL V2, consists of two books published in 2000 and 2001 (the Service Support V2 and the Service Delivery V2 respectively). While they publish additional titles over the years in support of the framework, those two books remained ITIL authoritative reference. It was not until 2007 that a new version, ITIL V3, was published. ITIL V3 changes its focus from technology to services with an emphasis on the five phases of IT Services lifecycle with each phase documented in one book for a total of five books. ITIL V3 has minor updates in 2011 (Bon, 2019; Cater-Steel et al., 2009). The current version, ITIL V4, was published in 2019.

A central premise of the framework is that organisations purpose is to create "value" for their stakeholders by offering services. A value is "the perceived benefits, usefulness, and importance of something" (AXELOS Limited, 2019, p.21); and service is "a means of enabling co-creation by facilitating outcomes that the customer want to achieve, without the customer having to manage specific costs and risks" (AXELOS Limited, 2019, p. 167). As in the definition of service and value above, "value", is always from a stakeholder (subjective) perspective.

For example, if "organisation" means the IT department, the stakeholder is the finance department. If the finance department staff cannot connect to their Wi-Fi anymore. The IT department (organisation) provides a service (troubleshooting and fixing the finance department Wi-Fi), the "value" created is that the finance department can access the Wi-Fi and staff can carry out their tasks. Other stakeholders may include the CEO who receive financial reports on time and other staff who will be getting paid on time.

ITIL based ITSM consists of several key concepts which support value co-creation (AXELOS Limited, 2019). The concepts include 1. Value co-creation. 2. Stakeholders which include organisations, service providers, service consumers and other stakeholders. 3. Products and services. 4. Service relationship. 5. Value: outcomes, cost and risks.

Value co-creation encourages cooperation between the organisation and stakeholders in value creation. From the example above, the IT department (organisation) works in cooperation with the finance department (feedbacks, assistance to accommodate technical works, and others) and this creates better value than if IT just went in and fixes what they think is the problem then left.

The concept of Products and services are central to an ITSM because service creates value and one or more products create a service. Organisations create products that are valuable to customers using a configuration (combinations) of resources the organisation have or have access to. These resources include people, technologies, value stream and processes, and partners and suppliers. The processes of managing resources, creating products and services and thereby facilitating value creation is the focus of ITSM.

The concept of “Service relationship” is about providers and consumers building relationships that enable value co-creation. In a service relationship, both parties can both be provider and consumer at the same time. From the example above, the IT department is the organisation and Finance is the stakeholder, instead of just fixing the Wi-Fi, IT also conduct training for Finance staff on what services IT offers that will help Finance. In return, Finance (organisation) now can do their job more efficiently, resulting in faster turnaround time on IT (stakeholder) and others, purchase orders.

The final concept, value: outcomes, costs and risks, emphasize the economic and risks factors of value creation. While value co-creation and building service relationship are important, service providers must and should weigh the costs and risks associated with providing a service against the Value created. The ITIL 4 service value system is depicted in Figure 2.7, which is a high-level overview of how all the components and activities of an organisation work together to facilitate value creation. The input can be a demand for a service, or an opportunity (business opportunity) arises for a service which results in the creation of a service value chain. A service value chain is a combination of activities that leads to the creation of product and services, which in turn facilitate values of co-creation.

The six activities are: Plan – ensure a shared understanding of the vision, current status, and improved direction of all four dimensions and all product and services across the organisation. Improve - ensure continual improvement of product, service and practices across all value chain activities and four dimensions of information security. Engage – good understanding of stakeholders needs, transparency, continual engagement, and good relationship with all stakeholder. Design and transition – ensure product and services continually meet stakeholder expectations for quality, cost, and time to market. Obtain/build – ensure service components are available when and where they are needed, and meet agreed specifications and deliver and support – ensure that services and delivered and supported according to agreed specifications and stakeholders' expectation (AXELOS Limited, 2019).

As depicted in Figure 2.7, all ITIL activities should be conducted with consideration of ITIL guiding principles and should be evaluated, directed, and monitored by a governance body made up of senior management who are responsible for activities compliance with policies and internal and external regulations. Activities are supported by ITIL management practices which are resources designed for performing work or accomplish an objective. ITIL divides its practices into 14 general, 17 service and three technical management practices. All management practices and the service value chain processes are continually monitored, assess and improved to ensure the ITSM system keeps up with the changes to remain relevant.

To ensure a holistic approach to service management, the whole ITIL SVS are subject to the four dimensions of services management, organisations and people, information technology, value stream and processes, and partners and suppliers. The organisation and people dimension concerned with human resources and competencies of staff, culture, organisational structure, roles and responsibilities, all of which are central to the success of the ITIL activities. The Information technology dimension is concerned with information and knowledge and the technologies required by ITSM activities as well as the relationship between different components. The suppliers and partners dimension is concerned with integration of suppliers and partners into the ITSM processes and the value streams and processes dimension concern with how different parts of the organisation work in a coordinated and integrated manner to facilitate co-value creation through product and services (Bon, 2019).

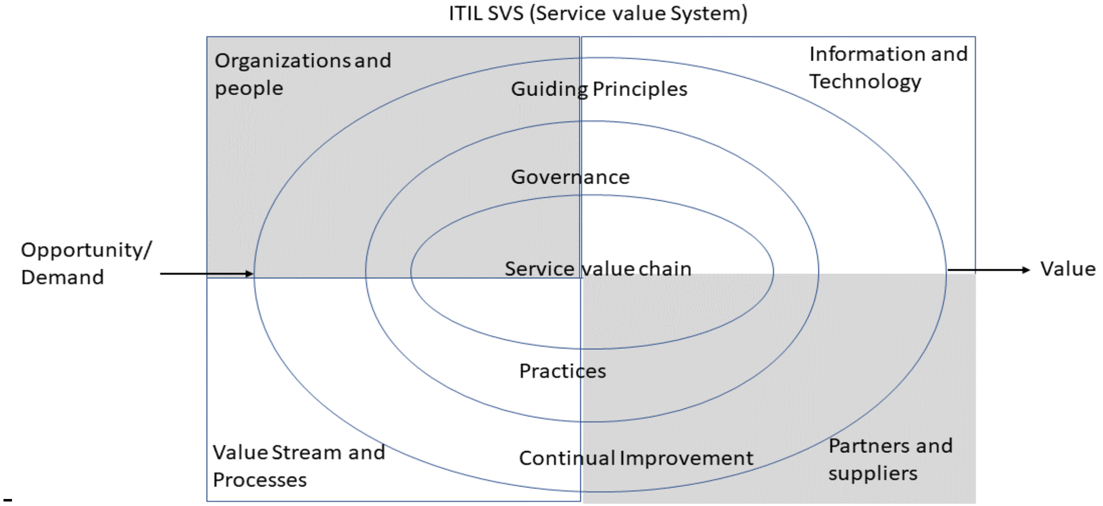


Figure 2.7: ITIL SVS

Adapted from Bon (2019) and AXELOS Limited (2019)

The ITIL focus is on services and value co-creation, as depicted in Figure 2.7. Its management practices are flexible enough to be easily integrated with other standards. ITIL does so by not specifying detail processes or procedures. It only specifies the need for the practice and that organisations implement it with consideration of the ITIL continual improvement model and ITIL guiding principles to support the service value chain activities that facilitate value creation.

ITIL flexibility means organisations could integrate other standards like ISO 27001, COBIT and others into its management practices. Kusumah et al. (2014) provides an example of integrating ITIL and another standard. In their study, they integrate ITIL and COBIT to develop an assessment model for holistic and integrated information security governance on a service management system for enterprises. In their study, they were able to map one or more ITIL management practices into 26 COBIT processes, essentially replaced ITIL management practices with COBIT processes.

Another similar study was by Haufe et al. (2016). In their study, they proposed a new processes framework for ISM by integrating ISO 27001, ITIL and COBIT. To develop their model, they use ISO 27001 as the base framework and integrate both ITIL and COBIT into it by analysing each framework processes, eliminate overlapping processes and then integrated the rest.

2.5 Summary of Issues

The pervasive use of technologies and organisations increasing dependent on it for their day to day operation give rise to the dynamic nature of organisations' information security threat environment. To counter information security threats, organisations should realise that information security has multiple dimensions, and purely technical solutions are no longer enough. In fact, given the number of successful breaches and the financial and operational consequences, one can safely conclude, purely technical solutions have failed.

Information security needs holistic approaches to assess and manage information security risks from different dimensions of information security: management involvement, human factors, and national and organisational information security culture. The search for holistic approaches to information security leads to the establishment of information security standards like the ISO 27001 family of standards. The ISO 27001 and ISO 27000 family of standards specifies an ISM framework comprised of internationally accepted information security best practices employing a holistic approach to address the dimensions of information security.

By implementing the standard, organisations would be able to manage their information security effectively because not only can they address all dimensions of information security, they can also align information security processes to their requirements and objectives. More importantly, ISO 27001 helps organisations to continuously improve their information security processes to remain relevant and deal with the organisation dynamic threat environment.

One of the main hindrances to organisations establishing effective information security is the lack of skilled information security professionals. Educational institutions are working to fill the gap by offering degree programs in information security; however, graduates of those programs are not ready as information security professionals. Information security associations like SANS, CSA, ISACA, ISC2 contribute by offering short term practical courses as well as certification programs. The fact is that there is no single body overseeing the training and certification programs. ISA develop their own programs according to their individually maintained CBK. Consequently, certification programs cover broad areas of information governance, service management and information security. Some certification program emphasizes hands-on training and focusing on a single area like GIAC programs and others like CISSP, which adopt a more broad approach, covering multiple areas in a single program.

While establishing useful measurement and metrics to measure an ISMS performance is challenging, it is crucial that organisations establish one in order for them to be able to monitor and assess ISMS performance. Assessing ISMS performance is important because it allows organisations to continuously improve their information security. The first step in assessing an ISMS performance is to identify the criteria for assessing ISMS effectiveness. According to review studies, common criteria for assessing the effectiveness of an ISMS include 1. Assessing an ISMS information security approach, i.e. does it addresses all dimensions of information. 2. Assessing the ISMS risks management processes. 3. Assessing the ISMS business alignment. 4. Assessing the continuous improvement processes of an ISMS. Based on those criteria, organisations can establish measurements and metrics using either GQM or maturity model approaches then start collecting performance data according to the defined measurements and metrics.

Finally, organisations can choose from different security frameworks and not just ISO 27001, to implement an ISMS. While each governance, service management and security frameworks have different focuses, they all have information security component. Therefore, organisations can adopt any of them either as a standalone framework or integrate it with another framework to implement effective ISM. For instance, while COBIT is an IT governance framework, and ITIL is a service management framework, studies have shown they can be adapted to use for ISM on their own or integrate with ISO 27001. The same for PCI DSS, while its focus is on protecting cardholders' data, the standard is flexible enough for organisations to implement to protect their information assets.

2.6 CONCLUSION

This chapter focuses on reviewing information security studies, organisations, standardizing bodies, frameworks and standards. The review aimed to provide an overview of information security challenges organisations face today, and different information security approaches to address those challenges. Having a clear understanding of information challenges and different approaches to information security provides a foundation to allow the researcher to develop a research design and a research model for the study. Subsequently, the research model facilitates the development of the research question(s) and hypothesises, which guide the rest of the study. Consequently, the review focuses on different areas of information security related to the overall objective of the study.

First, the focus was on reviewing information security standards and organisations that contribute to their development and maintenance. Specifically, the review focuses on ISO and the ISO 27000 family of standards of which ISO 27001 is a member. The aim was to get a better understanding of the standards, their roles in information security and why they are necessary. Furthermore, the section reviewed different information security associations, their contribution to information security, and their role in helping organisations to adopt information security standards. Specifically, the focus was on their contribution to the training of industry-ready information security professionals to help organisations improve their information security either by adopting standards or other appropriate measures.

Second, the review looked at the “why?” and “how?” of assessing information security standards. Specifically, the literature review focuses on identifying assessment criteria and how organisations can develop meaningful measurements and metrics not only to assess and improve information security processes but also to help management make informed decisions on the future direction of information security programs. In other words, understanding how standards are assessed, especially what are the criteria or characteristic of effective information security, significantly contribute to an organisation building effective information security.

Finally, the third and fourth sections focus on reviewing various information security standards and frameworks. ISO 27001 was reviewed in detail in order to understand its requirements and how it contributes to organisations establishing and effective information security. The other frameworks reviewed were COBIT, ITIL and PCI DSS. The aim of the review was to provide an overall picture of different standards and frameworks, how they related to each other, and the roles they play in organisations. For instance, understanding COBIT provides a good understanding of the role and importance of information governance in organisations. Moreover, understanding ITIL provides a clear picture of IT services management and the roles it plays in organisations. Finally, reviewing PCI DSS provides an overview of the roles technical standards play in organisations.

CHAPTER 3

RESEARCH METHODOLOGY

3.0 INTRODUCTION

Chapter 2 reviewed findings on information security standards and guidelines. The common consensus among information security studies is that information security has multi-dimensions. Technical solutions alone are not enough to manage the status of information security. Information security requires holistic approaches to address all dimensions and critical success factors for protection. Establishing effective information security has challenges or factors that are crucial to its success, and without addressing those factors, the chances for effective information security is minimal. Implementing information security standards, like the ISO 27001, allows organisations to establish effective information security in a systematic, and holistic manner addressing using internationally accepted best practices.

Studies have established a relationship between standards like ISO 27001, and the resolution of holistic approaches, ad-hoc approaches and information security effectiveness. Consequently, this research has two objectives:

- Study the current state of information security in key organisations in Tonga
- Study the impacts of Implementing ISO 27001 to determine if it is the best approach for organisations in Tonga to protect their information assets.

Section 3.1 discusses the research design that guides this study, and Section 3.2 the formulation of a research model that provides the foundation for study. The discussion focuses on research methodologies in section 3.3, together with studies that demonstrated those methodologies. Also appropriate methods are identified for use. In section 3.4, the focus is on data requirements for the study. The chapter finishes with a discussion of research limitations and a conclusion in sections 3.5 and 3.6, respectively.

3.1 RESEARCH DESIGN

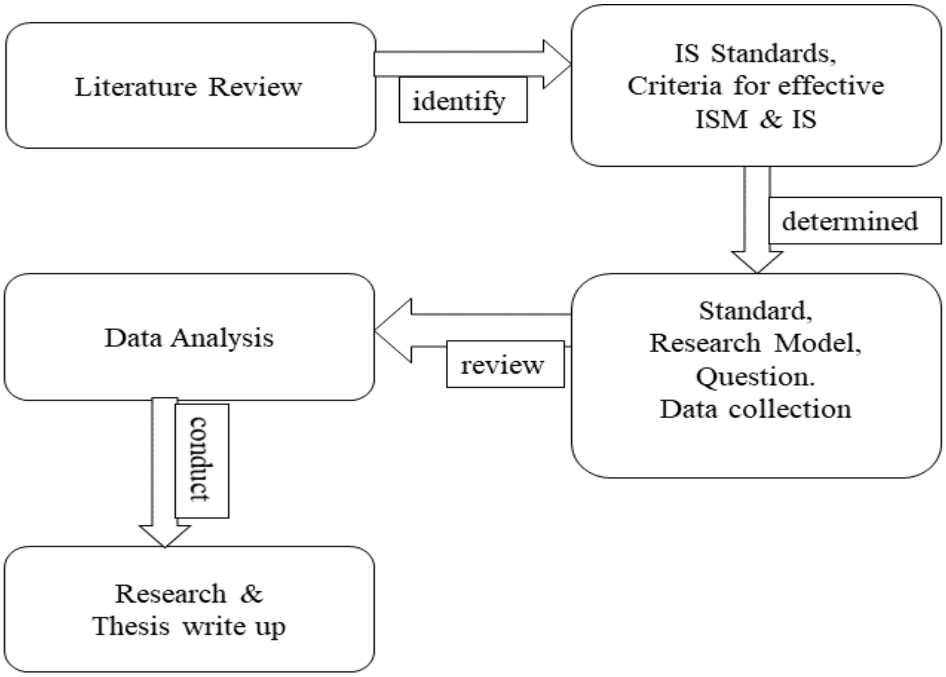


Figure 3.1: Research Plan.

This section discusses the plan summarised in figure 3.1, and the processes summarised in figure 3.2. According to the plan in figure 3.1, the first step is conducting a thorough review of information security studies on establishing effective information security management (ISM) and effective information security. Specifically, the criteria for establishing effective ISM and information security are located. Also the challenges, and the roles information security standards play in organisations to overcome information security challenges are described to develop an effective ISM and hence, effective information security.

Based on the literature review, the researcher selects the standard to focus on, develops a research model, questions and determines what data to collect, how to collect it, and from whom. Furthermore, based on reviewing the research models, questions and data, the researcher determined the most effective data analysis methods and processes for the study. Finally, the researcher carries out the study, culminating in the writing and submission of a thesis that documents the processes and findings of the study.

The research processes consist of six distinct phases, and Figure 3.2 shows the complete research processes. It is important to note that while the diagram provides an accurate depiction of the overall research processes. The phase order of execution may not always be according to the order depicted. The idea is that each phase is well defined, logical, and iterative to enable continuous improvement so that the whole process is responsive to change in response to changes in the research objectives, data, and findings from the literature review.

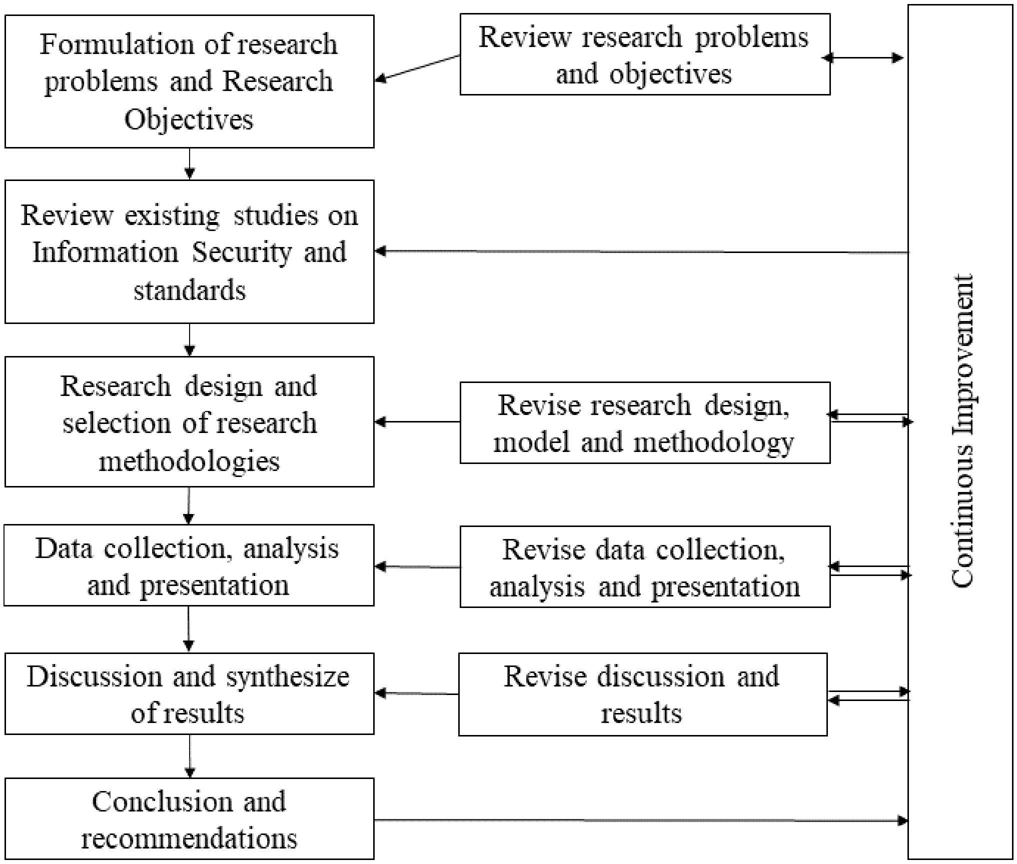

Formulation of research problems and Research Objectives
Review research problems and objectives
Review existing studies on Information Security and standards
Research design and selection of research methodologies
Revise research design, model and methodology
Data collection, analysis and presentation
Revise data collection, analysis and presentation
Discussion and synthesize of results
Revise discussion and results
Conclusion and recommendations
Continuous Improvement

Figure 3.2: Research Processes

The first phase involves the formulation of research problems and objectives. In phase two, the focus is on reviewing existing studies on information security standards, especially the ISO 27000 family of standards and the roles it plays in developing an organisation information security management system (ISMS). In phase 3, the outcome of the literature review facilitates the establishment of research processes and methodologies, as well as determining the data collection process and preparing the data collection tool. Phase 4 is the data processing phase, where the data is organised, analysed and presented ready for discussion and formulation of results in phase 5. Finally, in phase 6, the study presents the findings together with the recommendations for best practice and further research.

3.2 Research Model

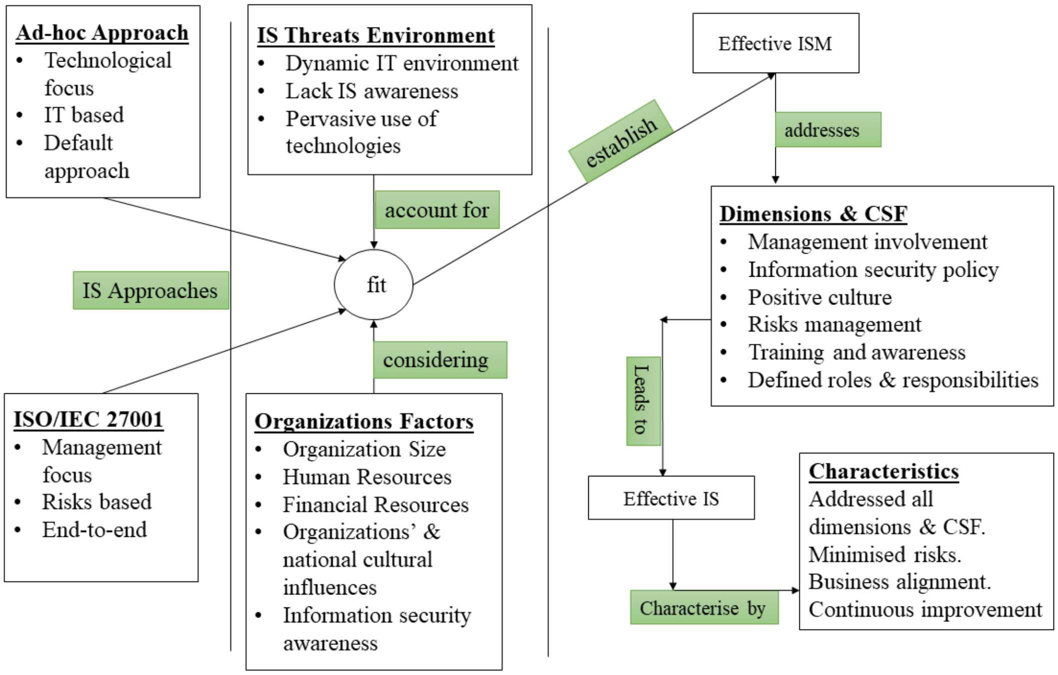


Figure 3.3: Research Model

The researcher formulated the research model in Figure 3.3, based on the study objective and findings from studies reviewed in chapter two. Table 3.1 summarises some of the findings from studies reviewed in chapter two that are relevant to the model design.

Table 3.1: Studies findings summary

Studies' Findings	References
Information security requires a holistic approach to be effective because • Ad-hoc approaches are not enough, given the dynamic nature of technologies and information security threats.	(Bunker, 2012; Da Veiga et al., 2007; Eloff & Eloff, 2003a; Freeman, 2007; Gerber & von Solms, 2005; Soomro et al., 2016; Spremić, 2013; Stoll & Breu, 2012)

• Purely technological solutions failed. • Information security is multi-dimensional	
Information security management is risks management	(Blakley et al., 2001; Campbell, 2016; Gerber & von Solms, 2005; Humphreys, 2008)
Information security frameworks and standard like the ISO 27001 standard, provides a holistic approach to Information security	(Al-Ahmad & Mohammad, 2013; Fal', 2010; Kajava et al., 2006; Kwok & Longley, 1997; Nasser & Nasser, 2017; R. Von Solms, 1999)
Effective information security requires effective, continuously improve information security management	(Chang & Ho, 2006; Humphreys, 2016; Livshitz et al., 2016; Petri et al., 2010; Zammani & Razali, 2016)
Effective information security is one that aligns with business requirements and objectives	(Johnson, 2014; Lidster & Rahman, 2018; Soomro et al., 2016; Tu et al., 2014)
Effective information security minimizes risks from all dimensions of information security.	(Da Veiga & Eloff, 2010; Humphreys, 2008; Tashi & Ghernaouti-Hélie, 2007; R. Von Solms, 1999)

From the literature review alone, one could argue that Tonga organisations information security would benefit (i.e. made more effective) from Implementing the ISO 27001 standard. However, given diverse factors that influence information security, depicted in Figure 3.3, a more appropriate response would be to theorize that implementing ISO 27001 is the best way for Tonga organisations to implement effective information security, which leads to this study's main research question.

> Is the holistic approach provided by ISO 27001 the best approach for Tonga organisations, given their unique organisational factors and threats environment, to establish effective information security?

To understand the question above from a Tonga organisational perspective, there are several sub questions: A Holistic approach compares to what other approaches? What is a holistic approach? Why is the holistic approach better? How does ISO 27001 utilise a holistic approach, and what is effective information security?

In summary, according to studies in Table 3.1, there are two types of information security approaches: ad-hoc which Information Technology (IT)-based and technological focused, and holistic which management based and focuses on systematic addressing of all dimensions and critical success factors (CSF) for information security. The studies also show that information security is about minimizing risks to organisation information assets. Consequently, the best approach is the one that is more effective in minimizing risks. Therefore, by definition, holistic approaches, which address risks from all dimensions and CSF of information security, should be more effective than ones which focus on a single dimension of information security.

Furthermore, studies also show that information security standards like ISO 27001, employ a holistic approach for addressing all dimensions and factors of information security. In theory it is an effective framework for managing organisation information security. In practice, however, studies have shown that factors like lack of financial and human resources, and others (unique to each organisation, i.e. organisational factors) can affect the organisational, especially small and medium enterprises (SMEs), ability to effectively implement ISO 27001. Based on the study findings summarised above: (a) Organisations' information security that is IT-based and technological focused, are by default, using ad-hoc approaches. (b) Analysing the impact of implementing ISO 27001 by comparing Tonga organisations' information security to ISO 27001 requirements, is, in fact, comparing ad-hoc and holistic approaches.

Therefore, the study can answer the main research question by investigating and answering a second research question about the impacts of implementing ISO 27001. Specifically,

> What are the impacts of implementing ISO 27001 on Tonga organisations information security management and information security?

The keyword in the question above is "impact", which is defined as "a marked effect or influence". While impacts can be either negative or positive, the study is only interested in the positive impact of implementing the ISO 27001. A positive impact means Tonga organisations are able to protect (by minimising risks to) their information assets effectively. Therefore, based on the second research question above, the research formulates three main hypotheses for the study: one control hypothesis, H0, and two alternative hypotheses, H1 and H2.

> H0: Implementing ISO 27001 is not the right approach for Tonga organisations given their organisational factors and dynamic threats environment.

The alternative hypothesises are:

> H1: Implementing ISO 27001, given their unique organisational factors and dynamic threats environment, positively impacts Tonga organisations ability to develop an effective ISM.
>
> H2: Implementing ISO 27001 and thereby establishing effective ISM, positively impacts Tonga organisations ability to establish effective information security.

As summarised in Table 3.1, effective information security management (system) is one that employs a holistic approach to address different dimensions of information security. Specifically, one can determine the effectiveness of organisations' ISM by examining how well they address different dimensions and CSF of information security. Therefore, since H1 is about effective ISM, it can be broken down for testing of each dimension and CSF of information security which effective (holistic) ISM should address. Therefore individual components of H1 are:

> H1a: Implementing ISO 27001 positively influence Tonga organisations' top management involvement in information security.
>
> H1b: Implementing ISO 27001 motivates Tonga organisations to establish a comprehensive information security policy.
>
> H1c: Implementing ISO 27001 improves Tonga organisations' information security awareness.
>
> H1d: Implementing ISO 27001 improves Tonga organisations' information security culture.
>
> H1e: Implementing ISO 27001 positively impacts Tonga organisations' ability to establish effective risks management.

H1f: Implementing ISO 27001 improves Tonga organisations' information security resources.

H1g: Implementing ISO 27001 motivates Tonga organisations to establish effective information security governance.

Just as H1 breaks down according to different dimensions and CSF of information security, H2 can also be broken down according to different characteristics of information security as depicted in the model in Figure 3.2 and studies summarised in Table 3.1.

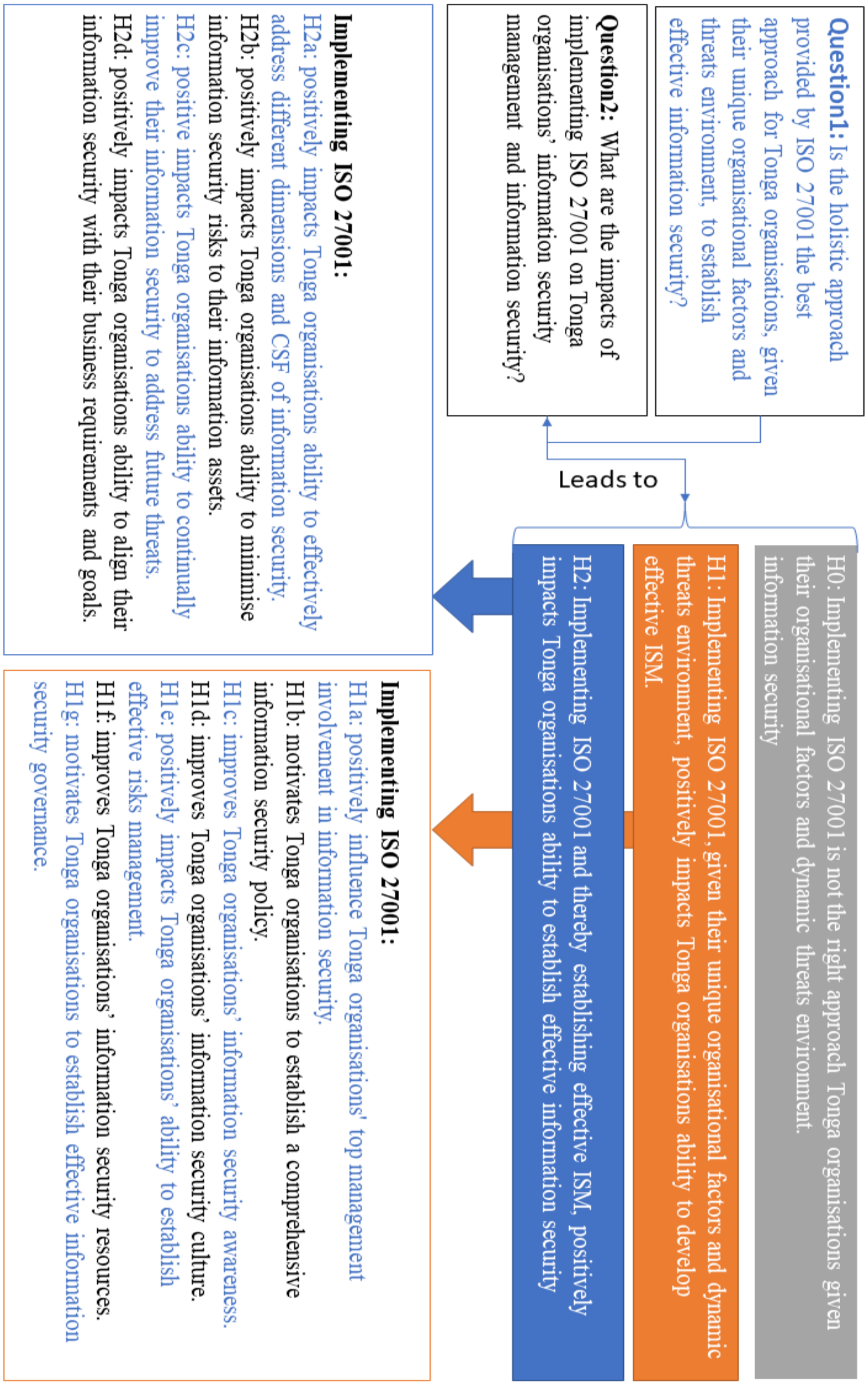
H2a: Implementing ISO 27001 positively impacts Tonga organisations ability to effectively address different dimensions and CSF of information security.

H2b: Implementing ISO 27001 positively impacts Tonga organisations ability to minimise information security risks to their information assets.

H2c: Implementing ISO 27001 positive impacts Tonga organisations ability to continually improve their information security to address future threats.

H2d: Implementing ISO 27001 positively impacts Tonga organisations ability to align their information security with their business requirements and goals.

For an overview of how the study's questions and hypotheses are related, please refer to figure 3.4, which provides a visual representation of the research questions and hypotheses discussed above.



Question1: Is the holistic approach provided by ISO 27001 the best approach for Tonga organisations, given their unique organisational factors and threats environment, to establish effective information security?

Question2: What are the impacts of implementing ISO 27001 on Tonga organisations' information security management and information security?

H0: Implementing ISO 27001 is not the right approach Tonga organisations given their organisational factors and dynamic threats environment. information security

H1: Implementing ISO 27001, given their unique organisational factors and dynamic threats environment, positively impacts Tonga organisations ability to develop effective ISM.

H2: Implementing ISO 27001 and thereby establishing effective ISM, positively impacts Tonga organisations ability to establish effective information security

Implementing ISO 27001:
H1a: positively influence Tonga organisations' top management involvement in information security.
H1b: motivates Tonga organisations to establish a comprehensive information security policy.
H1c: improves Tonga organisations' information security awareness.
H1d: improves Tonga organisations' information security culture.
H1e: positively impacts Tonga organisations' ability to establish effective risks management.
H1f: improves Tonga organisations' information security resources.
H1g: motivates Tonga organisations to establish effective information security governance.

Implementing ISO 27001:
H2a: positively impacts Tonga organisations ability to effectively address different dimensions and CSF of information security.
H2b: positively impacts Tonga organisations ability to minimise information security risks to their information assets.
H2c: positive impacts Tonga organisations ability to continually improve their information security to address future threats.
H2d: positively impacts Tonga organisations ability to align their information security with their business requirements and goals.

Figure 3.4: Research Questions and Hypothesises

3.3 RESEARCH METHOD

The research model and hypothesises discussed in the preceding section are important because they provide three key information points. 1. What to test to achieve this study objective? 2. What kind of data the tests required? 3. What is the outcome of those test, i.e. what the study hopes to find. That information, with the different methodologies discussed in section 3.3.1 and examples from information security studies discussed in section 3.3.2, allowed the researcher to select the research method for the study in section 3.3.3.

3.3.1 RESEARCH METHODS

Establishing a research methodology is critical to successes because the quality of research and its outcome; i.e. whether it yields meaningful results, largely depends on it. A clear and well-defined methodology enables others to follow the research logic, making it easy to assess the validity and trustworthiness of the research results (van Niekerk & von Solms, 2010). Research approaches fall into three main types, qualitative, quantitative or mixed. Each research type employs a different type of research method according to the research objectives.

Qualitative research mostly focuses on identifying relationships between variables in the research question by attempting to answer "why?" and "how?" questions (Walker, 1997). When it is exploratory, suitable research methods include case studies or action research methodologies like grounded theory, ethnography, content analysis, and phenomenological study (Williams, 2011). Other studies have also suggested other qualitative methods or techniques that include triangulation, i.e. combining different methods, sources, investigators or theories together, to "develop a comprehensive understanding of phenomena" (Carter et al., 2014, p. 545)

Among the qualitative methods, grounded theory and case study are the most utilised methods in information security studies. Case studies involve researchers studying an event, activity, process or individual. Case studies focus on the study of a phenomenon in a single organization for a specified period. For example, studies that are studying the current state of an organisation's information security (Williams, 2011). Grounded theory, involves systematic comparison of units of data using a series of structured steps to gradually construct a system of categories which describe an observed phenomenon (Knapp et al., 2006). For instance, if company A suffers many cyberattacks (observed phenomena), based on analysis of interviews and survey of staff; one could gradually build a theoretical model that explains why company A suffers so many cyber-attacks.

Quantitative research, assumes the existence of variables and relationships. It attempts to identify the degree of significances of each variable in a scientific way. Therefore, it focuses mostly on answering "how much?" and "how many?" questions (Walker, 1997). Quantitative research utilises three research methods; descriptive, experimental, and casual comparative research methods.

Descriptive research method examines the situation, as it exists in its current state by identifying "attributes of a particular phenomenon based on an observational basis, or the exploration of the correlation between two or more phenomena" (Williams, 2011, p. 66). For instance, from the reviewed studies above, descriptive research merely analysed what the collected data says about the current state of the studied organisation's information security. Comparative research attempts to examine the cause and effect relationship between the dependent and independent variables. Comparative research are most commonly used in cross-cultural studies to study differences and similarities across societies (Esser & Vliegenthart, 2017).

3.3.2 Review of Studies

This section, based on the methodologies discussed in the preceding section, focuses on reviewing several studies to identify different data collection, research and data analysis methodologies utilised in information security studies. Specifically, this section focuses on reviewing studies that utilise both quantitative and qualitative methodologies, and studies that utilise only quantitative methodologies and studies that utilise only qualitative methodologies.

Studies that utilises both quantitative and qualitative approaches include a study by Khalfan (2004), titled, "Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors". The study demonstrated the use of both quantitative and qualitative methodologies in an information security study. The aim of the study was to analyse and evaluate risks associated with outsourcing services, which many companies use as a cost-cutting measure.

The study uses a triangulation of sources, questionnaire, interview and documents from organisations with experience in outsourcing. They design the questionnaire to gather quantifiable data, hence the exclusive use of closed questions except for two summary questions at the end. The study combines the interview data and documents to provide context for data collected using the questionnaire. By analysing data from three sources, researchers were able to identify, ranked and documented each risk factor associated with outsourcing as well as providing a recommendation on measures to mitigate those factors.

Another study that utilises both quantitative and qualitative methodologies was by Knapp et al. (2006), titled, "Information security: Management's effect on culture and policy". The purpose of the study was to test several hypothesises on the influence of top management support for organisation information security culture and enforcement of policies. The first part of the study utilises a questionnaire with open-ended questions to collect data from 220 certified information security professionals. The responses were analysed using the grounded theory method to extract information, which 12 information security experts evaluated and used to formulate questions for a second questionnaire. The data from the second questionnaire was quantitatively analysed using structural equation modelling (SEM) software.

Both studies reviewed above demonstrated various ways of the utilising both quantitative and qualitative methodologies with triangulation of sources to investigate a phenomenon or phenomena. Both also demonstrated the use of a qualitative method like grounded theory as well as using SEM for statistical analysis.

Studies that demonstrated the use of the only quantitative methodology in information security studies include a study by Yeniman Yildirim et al. (2011). The study aim was to identify factors influencing ISM in SME. To achieve their objectives, the researchers collected data from 97 randomly selected SMEs using a questionnaire consisting of 49 questions divided into several sections, each of which are probable factors influencing information security. A participant responds to each question based on a 5-point Likert scale. The collected data is statistical analysed using SPSS (version 27), a statistical analysis software.

Another study that uses quantitative methodologies was by Dutta et al. (2013), titled, "Risks in enterprise cloud computing: The perspective of IT experts". The purpose of the study was to analysed risks associated with cloud computing. The first part of the study was a comprehensive literature review of risks associated with cloud computing to develop an ontology of cloud computing risks. They create their questionnaire using the identified risks with each identified risk results in four types of questions. Questions consist of a closed question to identify its validity, two 3-point Likert scale questions to identify the risk probability of occurrence and level of impact, and a 5-point Likert scale question to determine its frequency of occurrence. The data collected were statistically analysed to identify for the top 10 critical risks in cloud computing.

Both studies reviewed demonstrated the use of quantitative methodologies in information security studies, specifically the use of a questionnaire with Likert scales and closed questions to collect quantitative data and the use of statistical analysis software like SPSS (version 27).

Studies that demonstrated the uses of only qualitative approaches in information security studies include a study by Karabacak et al. (2016), titled, "A vulnerability-driven cybersecurity maturity model for measuring national critical infrastructure protection preparedness". As the title implied, the purpose of the study was to build a maturity model of root causes of Turkey's national critical infrastructure vulnerability.

They based their study on the result of an earlier study, which concluded that critical infrastructure assets in Turkey are vulnerable; however, it did not identify why. To build their model, they utilised data from an earlier study together with data from nine semi-structured interviews of mid-level managers and employees from the departments responsible for the critical infrastructure assets. They coded their data and analysed using grounded theory methodology to identify the root causes of the vulnerability. After they identified the root causes, they conducted a Delphi survey of six subject matter experts to identify criteria and weight for each root cause. The outcome was a maturity model with root causes as maturity levels; each maturity level has criteria with an assigned weight according to its degree of influence on the root cause.

Another study that utilises only qualitative methods was by Albrechtsen and Hovden (2009). The purpose of the study was to identify, analyse and discuss information security digital divide between managers and users and its influence on their perspective on information security risks. They collected the data for their study by interviewing managers and users from different organisations, of their experience of information security practices in their respective organisations. After collecting the data, they analysed it to identify similarity and differences between managers and users' experiences and therefore, their perspective of information security risks. The researcher conducted a qualitative comparative analysis of users and managers responses.

Both studies demonstrated the use of qualitative methodologies to study an information security phenomenon. Specifically, they demonstrated the use of a Delphi survey as a data-collecting instrument, expert opinions as data sources, and comparative analysis as data analysis methodology.

3.3.3 Selected Methods

From the studies reviewed above and in chapter 2, it is observed that quantitative research with descriptive and or comparative methods are common among information security standards related studies. It is understandable since in most cases, information security studies involved investigating a phenomenon or phenomena that involved multiple dependent and independent variables. This study is no different in that regard since effective information security is dependent on other factors. However, limitations of time mean the researcher cannot collect the relevant data for such a study.

This study intends to conduct gap analysis of Tonga organisation information security against ISO 27001 requirements. However, due to a limited amount of data collected, this study will utilise both quantitative and qualitative analysis to identify and ascribe meaning to those gaps in relations to the relationships between information security approaches, effective ISM, and effective information security depicted in the model in section 3.2. The data will be coded first in a format suitable for statistical analysis using SPSS (version 27) and then be coded again for qualitatively analysis using NVivo (release 1.0). The outcomes of both the statistical and qualitative analysis will provide a clear picture of gaps in organisation information security against the requirements ISO 27001.

3.4 Data Requirements

This study needs to collect suitable data during the data collection phase of the research process to ensure accurate testing of the study's hypotheses. The data needed for this study is the current state of Tonga organization information security. Subsequently, the study collected feedback from Information Technology (IT) experts currently working in different organisations in Tonga using a response guide on the state of their organisations' information security (Note: AUTEC ethics approval for expert feedback in Appendix A). The response guide consists of guiding questions and guidelines on (1) topics the experts should talk about and (2) advice on what they should include or exclude in their response. The topics discussed include information security in general, information security awareness, information security threats and attacks, incidents response and forensics, information security resources and culture.

The rest of the section discusses the experts who participated in the study in section 3.4.1, followed by a discussion of the data collection methods in section 3.4.2, data processing in section 3.4.3, and data analysis in section 3.4.4.

3.4.1 Expert Participants

The Oxford dictionary defines an expert as "a person having a high level of knowledge or skill in a particular subject". The expert selected for this study is IT professionals who have a high level of knowledge of their organization IT environment and information security. Qualifications for experts include many years of work experience in their organization and have intimate knowledge of the Information and Communications Technology (ICT) environment in Tonga. They also must work in a key organisation in Tonga like telecommunications, financial or government department, and finally, they have been involved in a major ICT project in Tonga. For instance, telecommunications projects, e-government projects, or a large project specific to their organisation.

While it was not a condition, all participants selected for the study held senior technical or management positions in their respective organisation and therefore are familiar with their organisations' IT infrastructures, operation and information security processes as well as the ICT environment in Tonga.

3.4.2 Data Collection Methods

Due to travel restrictions, the study relies on collected expert opinions by providing a response guidance tool consisting of guiding questions to direct the experts' responses. As mentioned above, topics cover different aspects of information security like information security awareness, information security threats and attacks, national and organizational culture influences and other information security-related topics. Each expert was provided with a summary of the ISO 27001 key point summary to guide their responses.

The guiding questions used in the response outline are both questions and guidelines to direct the expert on the appropriate information he/she should provide. For example, "After reading the ISO 27001 key point summary, has the organisation suffered any of information security attacks described? If yes, please provide a list with brief details of attack and cause (human error, technology failed, hacker, etc.) in accordance with Appendix A of ISO 27001. Please don't provide information that can be traced to a particular organisation". In total, there were two response guides; the first one using Microsoft Excel covering topics like management involvement, information security processes, forensics, and threats and attacks. The second one sent as a plain email covers information security awareness and culture.

3.4.3 Data Processing Methods

To start the data processing process, the researcher compiled all the expert responses into a single Excel file with one column containing the guiding questions, and subsequent columns contained the experts' feedback. The second stage is coding the experts' feedback for quantitative and qualitative analysis.

Firstly, the researcher coded responses that contain clear cut positive or negative responses with no extra information using a two-point Likert scale. The scale consists of 0 for No and 1 for Yes. For example, a response like "we have an information security plan, we update it regularly." is coded as ('information security plan', 1). On the other hand, a response like "we do not have an information security plan", is coded as ('information security plan', 0).

Secondly, responses that contain positive or negative answers but with qualifiers (conditional responses) were coded using a five-point Likert scale. The scale includes 1 for "absolute no", 2 "conditional no", 3 for "not sure", 4 for "conditional yes" and 5 for "absolute yes". For example, a response like "we have an information security plan, but it only covers security for X department" will be coded as ('information security plan', 4).

The reasons for having two Likert scales is to extract as much quantitative statistics as possible from the experts' feedback. The result of the coding process was stored in multiple Excel files with each file containing data regarding an aspect of organisation information security. For instance, awareness, policy, culture and resources. Each file contains a breakdown of expert responses regarding that particular topic. The leftmost column contains sub-topics. For example, the resources and assets file would have rows containing "have certified staff", "have information security staff", and others on its leftmost column. For quantitative analysis, the rest of the columns contained numbers representing the Likert scale of each expert's feedback on that particular topic. For qualitative analysis, the rest of the columns contain a portion of expert responses that discussed that particular topic.

Once the coding is done, the files with numbers are imported into SPSS (version 27) for quantitative analysis, while the files with written feedback are imported into NVivo (release 1.0) for qualitative analysis. The research will then compile the outcomes of both quantitative and qualitative analysis and present the results in the next chapter.

3.4.4 Data Analysis Methods

The preceding sections discuss the data collection and processing methods. Specifically, the data processing stage involves coding all expert responses and importing them to SPSS (version 27) and NVivo (release 1.0). This section discusses the research data analysis processes.

Figure 3.5 summarises the study data analysis processes. As the diagram shows, data analysis follows data processing which is discussed in the preceding section. The data analysis process is divided into two phases—first, the qualitative and quantitative analysis of expert feedback. Second, analysing the outcomes of the first phase against ISO 27001 requirements.

The quantitative analysis on the first phase involved calculating the ratio of positive to negative responses regarding a particular topic as well as calculating the number of times a concept appears in the expert feedback, expressed in percentages. The qualitative analysis, on the other hand, is much more involved. It serves two purposes: explain the why, how and what of the positive and negative answers and analyse responses that cannot be quantified clearly. For instance, expert feedback about the culture were hard to quantify, so it was mostly analysed qualitatively. The totality of both the quantitative and qualitative analysis in chapter 4, provides a complete picture of how Tonga organizations' information security addresses each dimension or CSF of information security for an accurate comparative analysis against the ISO 27001 requirements.

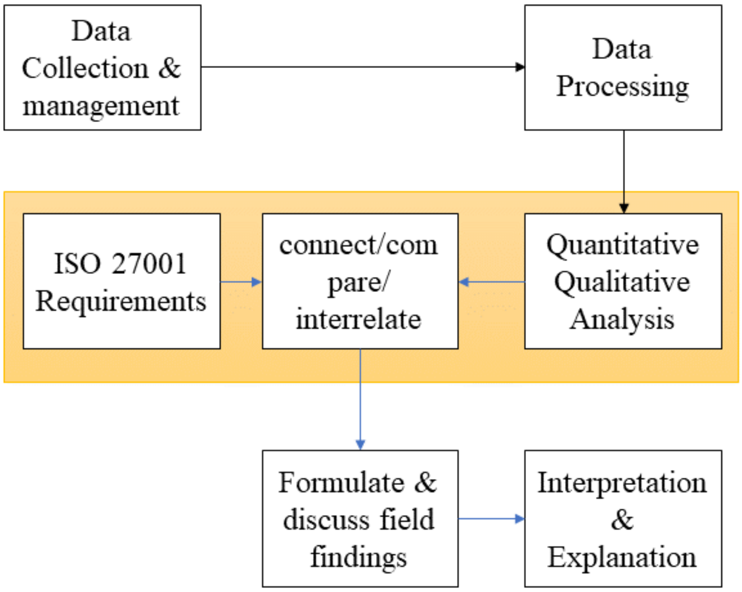

Data Collection & management
Data Processing
ISO 27001 Requirements
connect/compare/ interrelate
Quantitative Qualitative Analysis
Formulate & discuss field findings
Interpretation & Explanation

Figure 3.5: Data Analysis Processes

The second phase involved analysing findings from both quantitative and qualitative analysis against the ISO 27001 requirements. The gap analysis in chapter 5, identifies the gaps between Tonga organisations' information security and ISO 27001 requirements. The identified gaps, in turn, identified the impacts of implementing ISO 27001 on Tonga organisations' information security management and information security. The researcher then uses the identified impacts to test the study's hypotheses in chapter 6.

3.5 Limitations

This study aimed to examine the viability and applicability of ISO 27001 as a solution for organisations in Tonga to protect their information assets. Time constraints and circumstances beyond our control (COVID-19 lockdowns) meant that there were limitations on the data collection method, which also affect the amount of data collected.

The plan was to collect feedback from IT experts from different organisations in Tonga regarding the state of their organisations' information security. Unfortunately, due to travel restrictions, the researcher could not collect the experts' feedback in person. Unfortunately, due to time limitations, the researcher was left with limited alternatives. The only option was to collect expert feedback remotely using a response guide, which consists of guided questions with guidelines to guide experts on their feedback regarding different aspects (areas) of their organisations' information security that are related to the ISO 27001 key points.

While using a response guide to collect feedback should work in theory, in Tonga, it is always better to talk to people and collect their feedback in person. Tongan people relaxed attitude towards life in general means people would not always be willing to spending time responding to issues that they may have little or no interest in. Fortunately, through collaboration others were willing to help by following up with participants in person. However, the lack of in-person contact still put significant constraints on the number of responses received.

3.6 SUMMARY

This chapter discusses different the methods applied to complete the study. The research design section discusses the overall plan, design and processes involved in conducting the study. The design emphasizes iterative processes to deal with changes from other processes. For instance, changes to the research question(s) and or hypotheses would, in most cases, require re-examining data collection tools, and research methods and may also involve further literature reviewing.

The objective of this study to investigate whether implementing the ISO/27001 standard is the best approach for Tonga organisations to establish effective information security. To fulfil the study objective, the researcher developed a research model based on the literature review in chapter two. The research model depicts the relationship between information security approaches, effective ISM, effective information security, and factors that can impact those relationships, according to the reviewed studies.

The research model facilitates the development of research questions and hypotheses to help the study achieve its objective. The research questions and hypothesis determined the type of data needed by the study as well as how types of data processing and analysis are most appropriate for testing the hypotheses and thereby answering the research questions.

Finally, a discussion of data requirements for the study and constraints that may affect the data collection, processing and analysis processes and subsequently, the outcome of the study. The data collection utilises response guidance to collect expert feedback from Tonga organisation information security. The feedback are processed and analysed, and the result used for gap analysis against the ISO 27001 requirements. The study uses the identified gaps to test its hypotheses and subsequently answer the research questions.

CHAPTER 4

RESEARCH FINDINGS

4.0 INTRODUCTION

This chapter covers the "formulate and discuss field findings" phase of the data analysis model in the preceding chapter. The model summarises findings on information security management (ISM) and effective information security and different factors that influence effective information security. Understanding those relationships allows the researcher to examine how those factors and relationships would play out within the context of Tongan organisational information security environments. The model provides an overview of information security approaches for Tonga organisations information security environments and organisational factors. It also shows the influence on effective ISM and therefore, effective information security.

The traditional approach to information security was to treat it as an Information Technology (IT) issue and therefore it was handled exclusively by the IT department which in turn relied entirely on technological solutions like firewall, anti-virus, anti-malware, anti-spam, anomaly detection software, and others. Studies have long argued that the ad-hoc approach has failed information security because it is multi-dimensional. For instance, a firewall can protect information assets from outsider threats, but it cannot protect the same information assets from an employee (human factor dimension). Specifically, purely technological solutions have failed; therefore, a new approach is needed (Arbanas & Žajdela Hrustek, 2019; Bunker, 2012; Posthumus & Von Solms, 2004; Singh et al., 2014).

Studies also argued that information security needed a holistic approach that provides end-to-end information security which addresses all dimensions of the information security environment. Establishing effective information security requires the establishment of effective ISM. Information security standards which contain internationally accepted information security best practices give a common framework i.e. standardised ISM framework, which organisations can adapt to establish their own information security management system (ISMS), tailored according to their organisation's needs. ISO 27001 and the ISO 27000 family of standards is one of well-known and most adopted information security standard available today (BSI, 2017a; Eloff & Eloff, 2003b; Humphreys, 2011; Rao & Nayak, 2014; R. Von Solms, 1999).

For Tonga, the question is whether Implementing ISO 27001 is the best approach for organisations to protect their information assets, given their unique organisational factors and information security threat environment. To identify the impact of implementing ISO 27001; one needs to examine Tonga organisations current information security practices and how they handle different dimensions and the critical success factors (CSF) of information security. For instance, management involvement, information security policy, positive information security culture, risk management, training and awareness, defined roles and responsibilities, and continuous improvement (Arbanas & Žajdela Hrustek, 2019; Chang & Ho, 2006; Kazemi et al., 2012; Singh et al., 2014; Tu et al., 2014)

This chapter presents the result of the analysis of expert responses regarding different aspects of their organisation information security and how they address different dimensions and the CSF of information security. The rest of the chapter consists of a brief discussion of the expert responses in section 4.1. A brief discussion of concept diagrams in section 4.2 and code tables in section 4.3. Finally, section 4.4 presents the field findings followed by a summary of the findings in section 4.5.

4.1 EXPERTS RESPONSES

The researcher received a total of 7 responses in all from IT experts in Tonga. The number of participants seems low, but since Tonga is a small country, they represent most of the largest (in term of the number of employees and or information assets) companies and government departments in the country. The participants included two female and five males which is much better than the female to male ratio of IT professionals in Tonga. Information and Communication Technology (ICT) in Tonga is still a male-dominated profession.

4.2 Concept Diagrams

A concept diagram depicts the relationship between different concepts (Eppler, 2006). Concept diagrams are used in section 4.3 to depict relationships between different concepts (codes) extracted from the expert responses regarding a particular topic. For instance, figure 4.1 depicts codes extracted regarding "information security policy". It means that in regard to "information security policy", some experts' responded that they have "no policy". Experts who said they have no policy also mentioned "but, they are in draft" or they have an "IT policy".

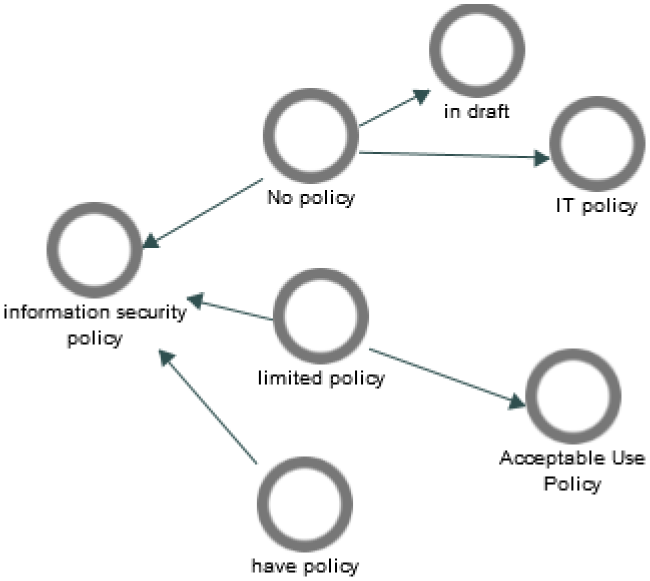


Figure 4.1: A concept diagram

4.3 Codes Tables

The codes tables used in the findings in section 4.4, contained codes which were used to construct concept diagrams discussed in the preceding section, 4.2. Combining both concept diagrams and code tables provides detailed information on the expert responses regarding a particular topic, i.e. aspects of Tonga organisation information security.

Table 4.1: A codes table

Parent Name	Topics/Codes	Aggregate	References
Codes\\Policy	information security policy	Yes	14
\\information security policy	have policy	No	2

	limited policy	No	1
	No policy	No	4
\\information security policy\limited policy	Acceptable Use Policy	No	1
\\information security policy\No policy	in draft	No	1
	IT policy	No	1

For instance, Table 4.1 listed all the codes that are used to build the concept diagram in Figure 4.1. The column "Parent Name" contains the topic and root codes. The "aggregate" column indicates if references include child references. The column "references" together with "aggregate == no" means how many expert responses contained the given code. With "aggregate == yes", means references equal the references of the root code plus references of child codes. Specifically, child references are mostly just duplications of root code references. Therefore, the references of codes with the aggregate column set to yes do not always specify the number of expert responses (in which the code was found) since some of those references are more likely counted more than one time.

For example, on table 4.1, the topic is "information security policy", which has three root codes, "have policy", "limited policy" and "no policy". The code "have policy" was found in two responses. The code "limited policy" was found in one response. The code "no policy" was found in four expert responses. Code "no policy", also has two child codes (last two rows), "in draft" and "IT policy", which were found in two separate responses (one reference each). If the aggregate column of code "no policy" was set to yes, its number of references would be six instead of four, i.e. four references for "no policy" plus two child references, one for "in draft" and one for "IT policy".

4.4 Field Findings

This section reports the study findings on how Tonga organisations address various dimensions and critical success factors (CSF) of information security. The findings include quantitative analysis of expert responses using SPSS (version 27) and qualitative analysis using NVivo (release 1.0). The outcomes of the qualitative analysis are summarised using a concept diagram, see section 4.2, together with a list of its corresponding extracted codes. The list of extracted codes also includes the number of references (how many expert responses contained the code) and flags to indicate whether the number is an aggregate or not. See section 4.3 above for more details. Section 4.4.1 to 4.4.8 presents the findings from Tonga organisation information security according to different dimensions and factors of information security. Section 4.4.9 provides an overview of all the findings in the context of an information security management (ISM), together with analysis of Tonga organisations information security plan and internal audit activities.

4.4.1 Awareness of Information Security and Standards

The findings in this section comprise of statistics and qualitative analysis of experts' responses regarding Tonga organisations awareness of information security in general and of information security standards. Table 4.2 summarises the statistics extracted from expert responses regarding the subject.

Table 4.2: Information security & standards awareness Statistics

Topics	No	Yes
Awareness of IS standards	57.1%	42.9%
Awareness of ISO 27001	85.7%	14.3%
Attended ISO 27001 or information security training	57.1%	42.9%
Implemented an information security standard	100.0%	0.0%
Interested in implementing an information security standard	0.0%	100.0%
Is information security important to the organisation?	0.0%	100.0%

A vital factor affecting the effectiveness of an organisations' information security is their awareness of information security threats, consequences and available solutions provided by information security standards. Consequently, one area experts provided feedback on was the organisation overall awareness of information security and standards, especially for Information Technology (IT) department and management. According to the statistics in table 4.2, while almost half (42.9%) of the experts are aware of information security standards and attended information security training (42.9%), only 14% are aware of ISO 27001. Furthermore, all experts agree that information security is important to their organisations and their organisations want to implement information security standards; however, none of the organisations has any prior experience in implementing one.

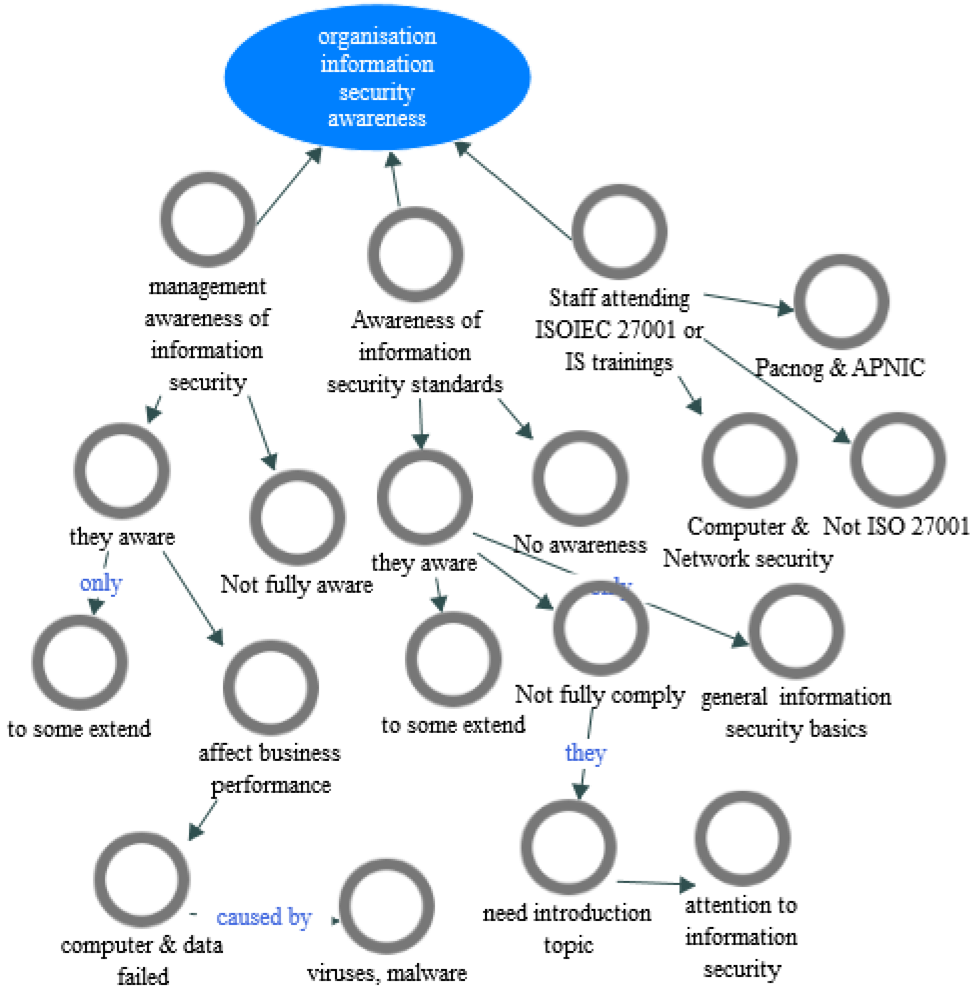

organisation information security awareness
management awareness of information security
Awareness of information security standards
Staff attending ISOIEC 27001 or IS trainings
Pacnog & APNIC
they aware
only
to some extend
Not fully aware
affect business performance
computer & data failed
caused by
viruses, malware
they aware
to some extend
No awareness
only
Not fully comply
they
need introduction topic
attention to information security
Computer & Network security
Not ISO 27001
general information security basics

Figure 4.2: Management & IT awareness qualitative analysis

Derived from codes in Table 4.3

According to the qualitative analysis depicted in Figure 4.2, the experts overwhelmingly agree (see Table 4.3 below, the code “they aware” has five non-aggregate references, i.e. five experts’ responses) that top management is aware of information security issues in their respective organisation. However, further analysis of their responses found, that while top management is aware of information security issues, it is only to "some extend". As one expert noted, they are aware that it could affect the organisations' performance due to computer failure and data corruption caused by "malware and viruses". However, they are not "fully aware" of information security threats and its implications; otherwise, they would pay more "attention to information security".

Moreover, IT department awareness of information security is limited to technical issues as illustrated by the training they attended. The experts indicated their staff attended PACNOG (PacNOG, n.d.) and APNIC training (APNIC, n.d.), which are mostly focus on "computer and network security" and not on ISM. The findings account for the low awareness of ISO 27001, despite the fact it is one of the most adopted information security standards today.

Analysis of codes in Table 4.3 makes sense of the analysis above. For instance, row number four, the topic "awareness of information security standards", there are two root codes, "awareness" and "no awareness". Four experts (57.1% in table 4.2 above) stated that their organisations have "no awareness" of information security standards, while three (42.9%) stated they are aware of information security standards. Out of those three experts, one expert added management were aware "to some extend", one expert said "not fully comply", and one expert said "general information security" basics.

Table 4.3: Information security & standards awareness extracted codes

Parent Name	Topics\Codes	Aggregate	References
Codes\\Mgmt-IT-Awareness	Staff attending ISOIEC 27001 or IS trainings	Yes	13
	management awareness of information security	Yes	6
	Awareness of information security standards	Yes	14
\\Awareness of information security standards	No awareness	No	4
	they aware	Yes	3
\\Awareness of information security standards\they aware	general information security basics	No	1
	Not fully comply	No	1
\\Awareness of information security standards\they aware	to some extend	No	1
\\management awareness of information security	Not fully aware	No	1
	they aware	No	5
\\management awareness of information security\Not fully aware	need introduction topic	No	1

\\management awareness of information security\Not fully aware\need introduction topic	attention to information security	No	1
\\management awareness of information security\they aware	affect business performance	No	1
	to some extend	No	1
\\management awareness of information security\they aware\affect business performance	computer & data failed	No	1
\\management awareness of information security\they aware\affect business performance\computer & data failed	viruses, malware	No	1
\\Staff attending ISOIEC 27001 or IS trainings	Computer & Network security	No	3
	Not ISO 27001	No	1
	PACNOG & APNIC	No	2

In other words, while experts said their top management is aware of information security standards, they also qualify their answers with phrases like “to some extend”, “not fully aware”, and “information security basics”. They qualify their assertion that their top management is aware of information security standards or information security in general.

4.4.2 Top Management Involvement

This section presents the findings extracted from expert feedback on whether their organisations’ top management is involved in their information security and if they are involved, what is the extent of the involvement.

Figure 4.3 shows a conceptual diagram of the codes extracted from expert feedback regarding management involvement in their organisation information security. As noted by studies, management involvement is essential not only because ISM needed resources which only top management can authorise, they also influence organisation information culture (Alnatheer, 2015), and enforcement of information security policies (Knapp et al., 2006).

According to responses received, 71.4% of the experts said their organisations’ top management is involved in information security. The high number of involvement is good news. However, according to the qualitative analysis of experts’ responses in figure 4.3, management involvement extends to only “approving budget, materials” and projects or only involved when there is a “security problem”. Some experts also indicated that top management are only involved in "technical implementation" of projects or if it is something that is of interest to them personally, i.e. "own interest".

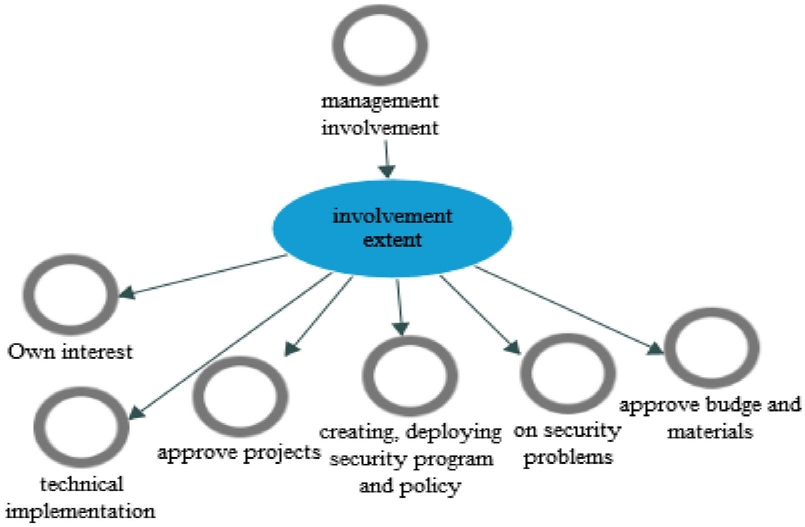


Figure 4.3: Analysis of responses about management involvement in IS Based on codes in Table 4.4

Analysis of the codes in Table 4.4, reveals that on the topic of "management involvement' in information security. Out of seven responses, each expert mentions something different like "approve budget and materials", "approve projects", "creating, deploying security program and policy", "on security problems", "Own interest" and "technical implementation". In other words, the extent of management involvement in information security differs greatly among Tonga organisations.

Table 4.4: Management Involvement extracted codes

Parent Name	Topics/Codes	Aggregate	References
Codes\\MGMT	management involvement	Yes	13
\\management involvement	approve budge and materials	No	1
	approve projects	No	1
	creating, deploying security program and policy	No	1
	on security problems	No	1
	Own interest	No	1
	technical implementation	No	1

4.4.3 Information Security Policy

This section discusses findings based on expert feedback and a previous study regarding Tonga organisations' information security policy or the lack thereof. According to a quantitative analysis of expert responses, 57.1% said their organisations have an information security policy. That result is in line with a survey conducted in 2016 by Laulaupea'alu and Keegan (2019) in which they found that over half of the organisations they surveyed said they have an information security policy. While it is a good sign that the majority of organisations have an information security policy, a qualitative analysis of the responses in Figure 4.4 reveals a different picture. While experts agree they have an information security policy, one response added that it is an "IT policy" while another added that it is an "acceptable use" policy. As noted in chapter 3, section 3.4.1, these are key companies and government departments. The discrepancy in expert responses is supported by findings in section 4.4.1, which indicates a lack of general awareness of information security and standards among organisations in Tonga, even by experienced IT professionals.

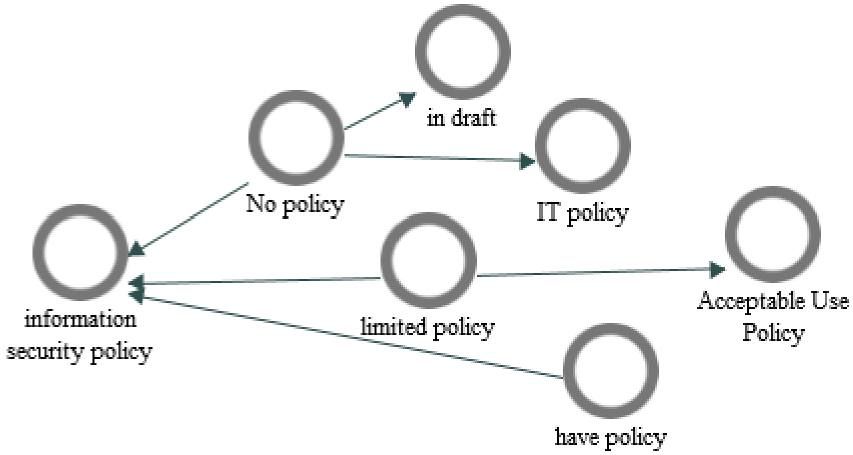


Figure 4.4: Analysis of responses about IS policy

Based on codes in Table 4.5

Table 4.5: Information security policy extracted codes

Parent Name	Codes	Aggregate	Number of References
Codes\\Policy	information security policy	Yes	14
\\information security policy	have policy	No	2

	limited policy	No	1
	No policy	No	4
\\information security policy\limited policy	Acceptable Use Policy	No	1
\\information security policy\No policy	in draft	No	1
	IT policy	No	1

The codes in Table 4.5 support the findings depicted in Figure 4.4. The code "have policy" in the second row has two references, i.e. found in two responses. The code "limited policy" and "no policy" account of remainder of the experts, i.e. five experts or 71.4% of the organisations. In other words, the number of organisations in Tonga with an information security policy is very low. Given these are key organisations, and they employed some of the most experienced IT people, it has implications for the other organisations not participating in the study.

4.4.4 Resources and Assets

This section presents the findings for Tonga organisation information security resources and assets. Table 4.6 summarises responses related to organisation human resources and budget. It is interesting to note that the majority (57.1%) of the organisations have a budget and only 14.3% of organisations have no information security budget. In the qualitative analysis in Figure 4.5, one participant indicated that while they do have a budget, it is "not mandatory" for them to spend it. Another participant also indicated that their security budget is only for staff salaries and not for operation and support of an information security program.

Table 4.6: Resources statistical analysis

Topics	Absolute No	Conditional No	Not sure	Conditional Yes	Absolute Yes
IS Budget	14.3%	28.6%	0.0%	57.1%	0.0%
IR & Forensics Staff	71.4%	14.3%	0.0%	14.3%	0.0%
Dedicated IS staff	57.1%	0.0%	0.0%	14.3%	28.6%
IS certified staff	85.7%	0.0%	14.3%	0.0%	0.0%
Importance of skilled IS staff	14.3%	0.0%	14.3%	0.0%	71.4%

For information security staff, 14.3% of organisations have established an "IS section" with dedicated information security staff, i.e. initiated some formal information security governance structure. Analysis shown in Figure 4.5 indicates that while many of the organisations do not have dedicated information security staff, they do have an "IT section". Some participants indicated the reason for the lack of dedicated information security staff is because of "lack of awareness". In contrast, others stated that having certified information security staff is "not important" to the organisation.

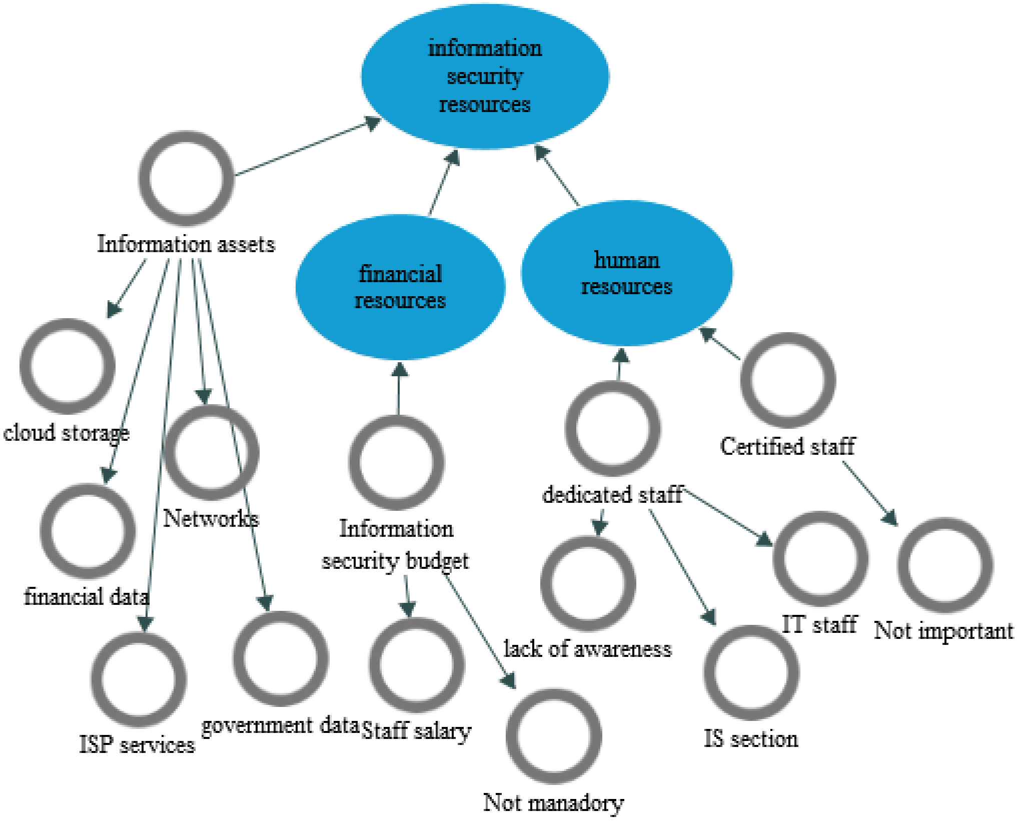


Figure 4.5: Analysis of responses about resources and assets

Based on codes in Table 4.7

The lack of financial, human resources and organisational structure in organisations in Tonga, agrees with findings by Laulaupea'alu and Keegan (2019), based on a survey of Tonga organisation vulnerabilities, conducted in 2016. In their study, concerning information security funding, they stated that "Some large organisations are not allocating funds in their budget to purchase antivirus software for protection" (p. 189). Concerning skilled staff, they stated that "The results of the survey showed that 25 % of the organisations in Tonga hire a specialist as a member of staff to mitigate threats to organisation's data" (p. 190), which is in line with the data from this survey.

The information security resources allocated by Tonga organisations do not seem to be proportionate to the information assets organisations they are looking after. For instance, according to the analysis in Figure 4.5, some of the organisations involved in this study look after “financial data”, “government data”, “ISP services” and cloud-based data (“cloud storage”). Specifically, the assets the experts mentioned are critical information assets which should be a top priority for organisations to protect.

The analysis of the codes in Table 4.7, while do not necessarily provide new findings, it does support the analysis in Figure 4.5. For instance, with regard to “certified staff”, only one expert (1 reference) has something more to say about it, “not important”. The rest just answer “no”, hence no codes were derived from their responses. In regard to having dedicated staff, two experts said they have “IT staff” and others are explained above. In regards to information assets, it is interesting that two mentioned “financial data” and two mentioned “government data”. The experts mentioned some very critical financial and government information assets; however, they were not included for non-disclosure reasons.

Table 4.7: Resources and assets codes

Parent Name	Name	Aggregate	Number of Coding References
Codes\\Resources	Certified staff	Yes	8
	dedicated staff	Yes	11
	Information assets	Yes	18
	Information security budget	Yes	9
\\Certified staff	Not important	No	1
\\dedicated staff	lack of awareness	No	1
	IT staff	No	2
	IS section	No	1
\\Information assets	cloud storage	No	1
	financial data	No	2
	government data	No	2
	ISP services	No	1
	Networks	No	5
\\Information security budget	Not mandatory	No	1
	Staff salary	No	1

4.4.5 Information Security Awareness

The findings in this section deal with organisation internal information security awareness. Specifically, are non-IT staff or are the organisations aware of information security issues and addressing those issues. Table 4.8 summarises expert responses regarding information security awareness training and end-to-end information security awareness. According to their responses, only 42.9 % of organisations have non-IT departments that are aware of information security-related issues.

Table 4.8: Information security awareness statistics

	Absolute No	Conditional No	Not sure	Conditional Yes	Absolute Yes
Other departments awareness	28.6%	0.0%	28.6%	42.9%	0.0%
awareness training	85.7%	0.0%	0.0%	14.3%	0.0%

42.9% of non-IT department information security awareness is limited to when the IT department informed them of “malicious email and software”, according to the qualitative analysis of expert responses in Figure 4.6. The other organisations have “little awareness”, consider it “not important” or have no awareness at all, i.e. “only IT” are aware of and are dealing with information security-related issues.

Another important aspect of organisation information security awareness is their information security awareness training or lack thereof. According to Table 4.8, 85.7% of organisations have no awareness training at all. The lack of awareness training is related to the IT department and top management lack of awareness of information security issues and standards as detailed in the findings in section 4.4.1.

The detailed analysis of codes in Table 4.9, do not provide any new findings, but rather elaborates and supports the findings above. For instance, six experts (85.7%) indicated “no awareness”. Interestingly, out of those six, one expert indicated they do have a training budget which they often spend on other areas. Furthermore, other interesting points not discussed above, including two experts (28.6% of organisations) indicated that non-IT staff only know about information security when they informed.

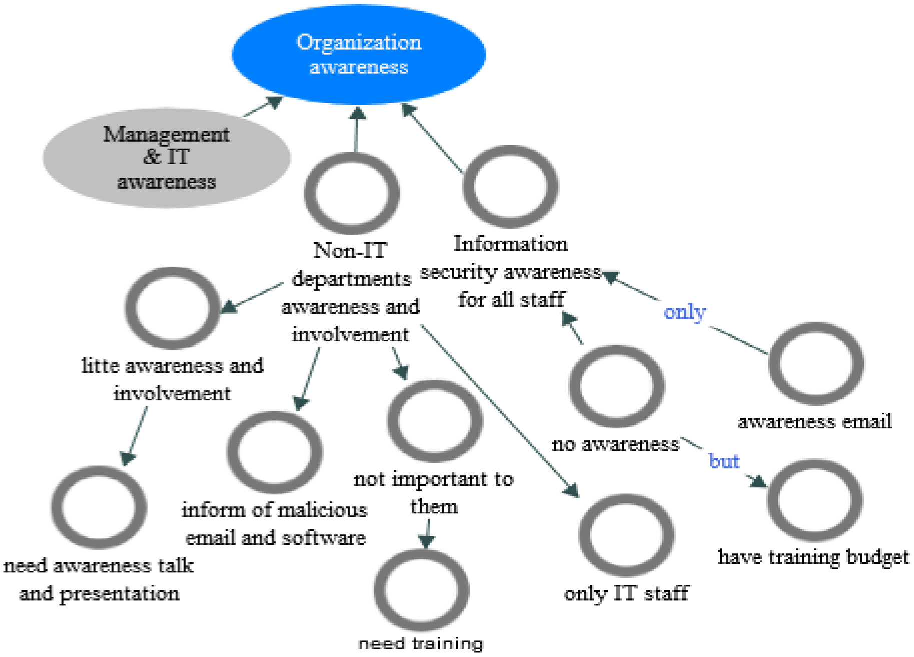

Organization awareness
Management & IT awareness
Non-IT departments awareness and involvement
Information security awareness for all staff
only
litte awareness and involvement
awareness email
not important to them
no awareness
but
inform of malicious email and software
need awareness talk and presentation
have training budget
only IT staff
need training

Figure 4.6: Analysis of responses about IS awareness

Based on codes in Table 4.9

In other words, for those organisations, non-IT staff are in the dark on information security most of the time except when IT decides to inform them of selected information security issues.

Table 4.9: Information security awareness extracted codes

Parent Name	Topic/Codes	Aggregate	References
Codes\\IS awareness	Information security awareness for all staff	Yes	14
	Non-IT departments awareness and involvement	Yes	12
\\Information security awareness for all staff	awareness email	No	1
	no awareness	No	6
\\Information security awareness for all staff\no awareness	have training budget	No	1
\\Non-IT departments awareness and involvement	not important to them	No	1
	only IT staff	No	1
	little awareness and involvement	No	1
	inform of malicious email and software	No	2
\\Non-IT departments awareness and involvement\little awareness and involvement	need awareness talk and presentation	No	1
\\Non-IT departments awareness and involvement\not important to them	need training	No	1

4.4.6 INFORMATION SECURITY CULTURE

Cultivating and promotion of positive information security culture is critical since human behaviour has significant risks to organisation information assets (Alnatheer, 2015; Choi et al., 2018; Mahfuth et al., 2017). Consequently, the experts were requested to provide feedback on the influence of organisation culture on information security culture, and what actions their organisations are taking to address any information security issues that arise due to influence of cultures on information security. Figure 4.7 presents a summary of the findings based on the responses.

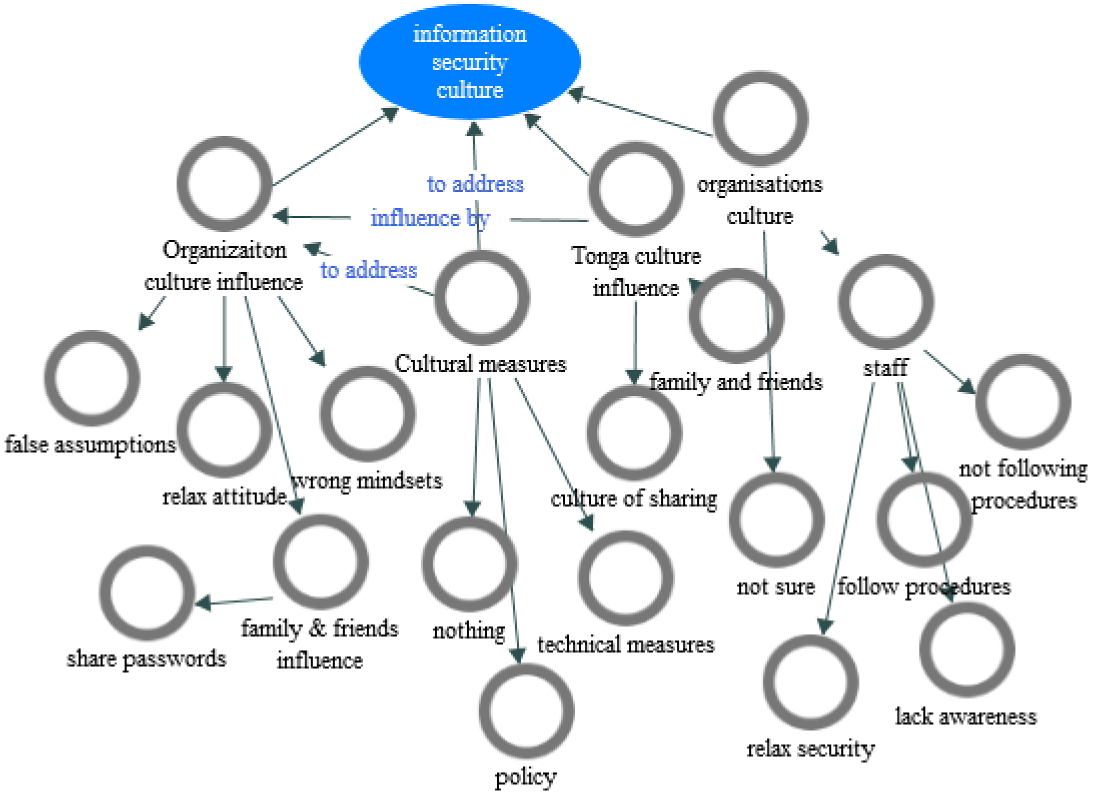


Figure 4.7: Analysis of responses about culture

Based on codes in Table 4.10

According to the feedback received, the Tongan biggest cultural influences are "family and friends" and "sharing". As one expert put it, "Tongan culture, upbringing in a Tongan environment and our Tongan values affect information security. (We are) living in a Tongan environment, (a) big household full of extended family, sharing confidential information, sharing password info, etc."

In a sentiment echoed by Semisi et al. (2015), he stated that the three principal cultural characteristics of Tongan people are 1. Their "desire to build and enhanced relationship" (p. 6) every chance they get. 2. Basing "their identity with extended family and community" (p. 6) rather than the individual. 3. "Focus on the present or the immediate event" (p. 6) and not on less immediate events, and needs. Specifically, a Tongan by nature finds it harder to deny requests by friends and families, even if those requests affect organisations' information security.

According to Figure 4.7, Tongan organisation cultures are directly influenced by Tongan culture. For instance, participants agree that not only family and friends influence an organisations' culture, but that staff are relatives and tend to share passwords and other information. Also, relatives can come into the organisation, and staff usually let them use the Wi-Fi. Moreover, peoples "relax attitude" leads to "false assumption"; like thinking that Tonga is a "small nation and everything is secure, no one wants to steal any information from us". The codes in table 4.10 indicated that two experts stated that their staff do not follow security procedures, and two indicated staff have a low awareness of security procedures. Moreover, one expert indicated security in their organisation, especially information security, is very relaxed, therefore there are no set procedures for their staff to follow. Only one expert indicated their staff follow the organisation's security procedures. One expert was "not sure" of their organisation's information security culture.

Table 4.10: Culture extracted codes

Parent Name	Topics/Codes	Aggregate	References
Codes\\culture	Cultural measures	Yes	8
	Organisation culture influences	Yes	9
	Tonga culture influences	Yes	8
	Organisation culture	yes	14
\\Cultural measures	Nothing	No	1
	Policy	No	2
	technical measures	No	1
\\Organisation culture influences	false assumptions	No	1
	family & friends influence	No	2
	relax attitude	No	1

	wrong mindset	No	1
\\Organisation culture influences\\ family & friends influence	share passwords	No	2
\\Tonga culture influences	lack of knowledge and awareness	No	1
	culture of sharing	No	2
	family and friends	No	1
\\Organisation culture	Not sure	No	1
	Staff	No	6
\\Organisation culture\\staff	relax security	No	1
	lack awareness	No	2
	follow procedures	No	1
	not follow procedures	No	2

4.4.7 Information Security Risk Management

This section presents findings on Tonga organisations' information security management. The response guide directed experts to provide feedback on what think are the information security threats to their organisations, whether they have experienced any information security attacks, and whether they have done any risk assessment of their information assets. Discussions of their responses are in the sections below. Section 4.4.7.1 discusses the findings on organisation information security threats and attacks, and section 4.4.7.2 discuss the findings on organisation risk management practices.

4.4.7.1 Organisations threats and attacks profile

Table 4.11 provides statistics of experts' quantifiable responses regarding information security threats, attacks, and risks assessments. According to data, 42.9% of organisations experienced information security attacks while 85.7% said they have plans to counter such attacks in the future. The percentages do not add up; however, some experts declined to discuss the attacks. Specifically, more organisations experienced information security attacks than 42.9% who indicated it. This was expected as experts were instructed not to talk about information if they violated their companies' policies or it can be used to identify their organisation.

A qualitative analysis of expert responses in Figure 4.8 indicated that for organisations which experienced attacks; they experienced two types of attacks, social engineering and hacking attacks.

Table 4.11: Threats and attacks

	Absolute No	Conditional No	Not sure	Conditional Yes	Absolute Yes
Any IS Attacks?	0.0%	14.3%	28.6%	42.9%	14.3%
Plan to prevent attacks	14.3%	0.0%	0.0%	85.7%	0.0%

The rest of what they described as attacks were either factors like “no license, human error”, that facilitate attacks or consequences of attacks like “corrupt data” which was made worse by having “no backup”. According to participants, security threats include “social hacking“, “spam”, “virus”, “network security threats”, and “technology failed”. The mentioned threats are human factors threats, i.e. mostly facilitating by human actions or behaviour due to lack of information security awareness, carelessness, or malicious.

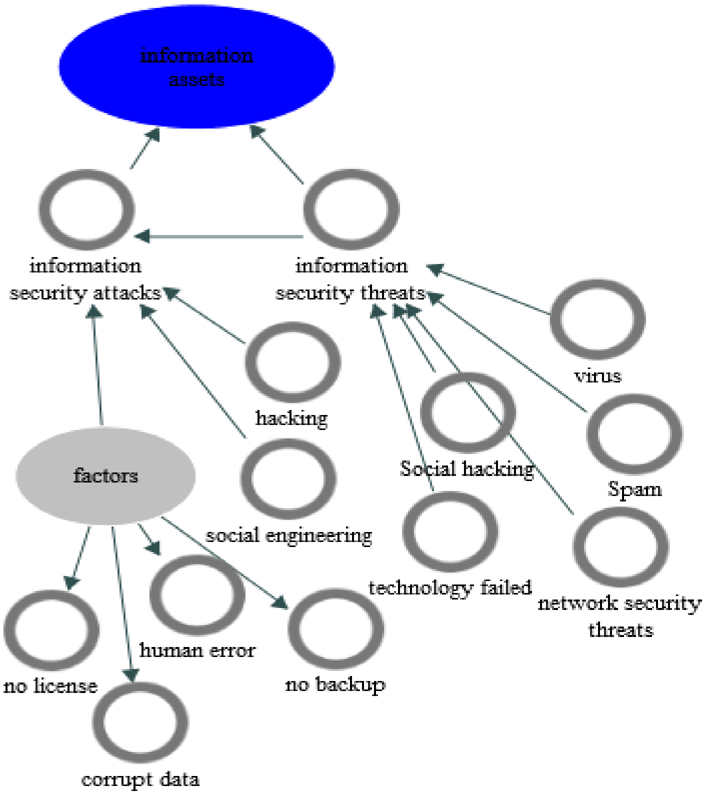


Figure 4.8: Analysis of responses about IS threats & attacks
Based on codes in Table 4.12

While the analysis of codes in Table 4.12 does not reveal any new findings it helps to interpret Figure 4.8. For instance, on the topic of "information security attacks", three participants mentioned "human error", i.e. 42.9% while two participants mentioned "hacking" or 28.6%. On the topic of "information security threats", the most common is "spams" with 57.1%, i.e. mentioned four participants, while "virus" was mentioned by two participants. As noted in chapter 3, these are key organisations and for two of them to be hacked (potentially more than two since the others did not want to talk about it) is a serious problem for Tonga organisations. The findings above are supported by Laulaupea'alu and Keegan (2019), based on a survey by one of the authors in 2016. They found similar types of information security threats and attacks. For instance, according to their findings, 27% of organisations had malicious software attacks, 26% had problems with spams, six percent had unauthorised access, five percent were victims of social engineering attacks, and three percent were victims of ransomware attacks.

Table 4.12: Threats & attacks extracted codes

Parent Name	Topics/Codes	Aggregate	References
Codes\\threats	information security attacks	Yes	16
	information security threats	Yes	16
\\information security attacks	no license	No	1
	no backup	No	1
	social engineering	No	1
	Hacking	No	2
	corrupt data	No	1
	human error	No	3
\\information security threats	Spam	No	4
	technology failed	No	1
	network security threats	No	1
	Social hacking	No	1
	virus	No	2

4.4.7.2 RISKS ASSESSMENTS

Information security is about minimising information security risks, making risk management a critical component of any ISMS. Table 4.13 provides expert responses regarding risk assessments and whether they think their information assets are secure.

Table 4.13: Risks assessments

	Absolute No	Conditional No	Not sure	Conditional Yes	Absolute Yes
Are Information assets secure?	0.0%	14.3%	42.9%	42.9%	0.0%
Any risk assessments?	42.9%	0.0%	0.0%	57.1%	0.0%

According to the experts' feedback, 42.9% of organisations conduct no risk assessment, while 57.1% did. Despite the 57.1% of organisations conducting risks assessments, 42.9% are not sure, and another 42.9% said yes but are still unsure if their information assets are secure.

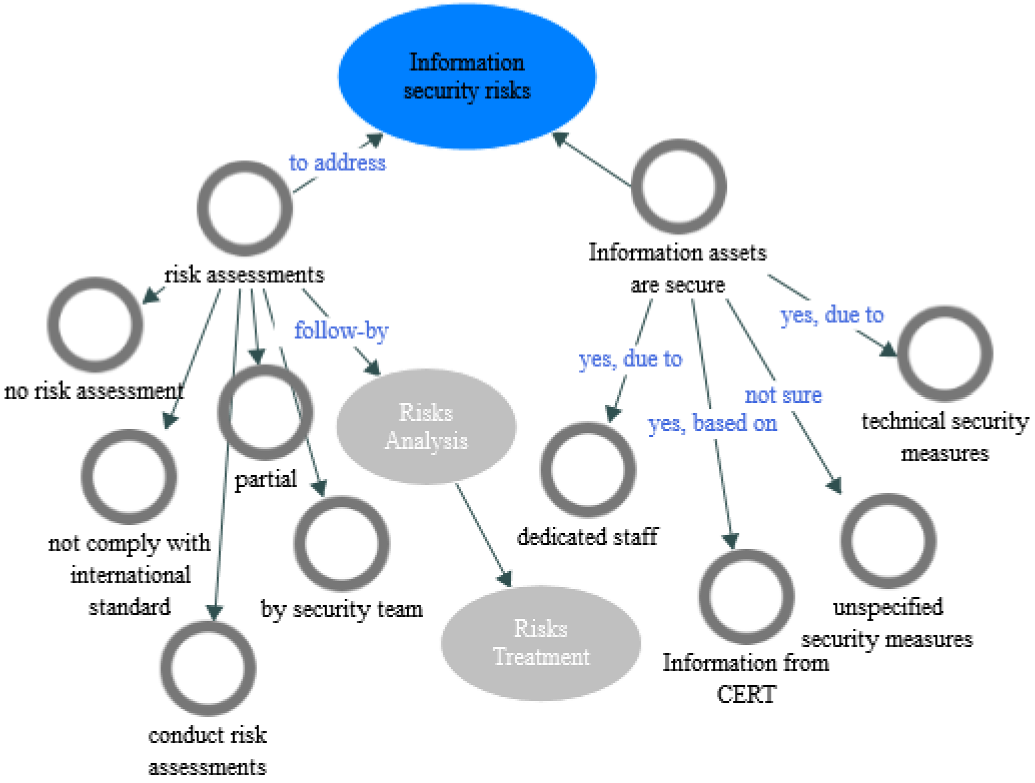


Figure 4.9: Analysis of responses about risks assessments

Based on codes in Table 4.14

Furthermore, according to Figure 4.9, the participant who responded that they do conduct risks assessments, added they have a "security team" who conducts "active risks" assessment whilst others indicated it was only a "partial" risk assessment. One participant stated they do conduct risks assessments and did not comply with the international standard. They did not elaborate on which international standard. In other words, there is no mentioned of any well-defined program and processes involved despite requesting they provide as much information as possible. It is also interesting that one expert mentioned "not comply" with international standards despite organisations (include the experts) lacking information on security standards awareness according to the findings in 4.4.1. One could assume that the expert uses the phrase perhaps not literally but to indicate the state and quality of their risks assessments.

As noted in 4.3, Table 4.14 contained codes use to construct 4.9. Analysis of the codes reveals interesting information. When requested to give feedback on security of their information assets, three experts (42.9%) discussed "technical security measures". In other words, many of the experts and subsequently, organisations in Tonga still consider information security as primarily, a technological problem that could be solved by technological means.

Table 4.14: Risk assessment extracted codes

Parent Name	Topic/Codes	Aggregate	References
Codes\\Risks	Information assets are secure	Yes	13
	risk assessments	Yes	14
\\Information assets are secure	Information from CERT	No	1
	dedicated staff	No	1
	technical security measures	No	3
	unspecified security measures	No	1
\\risk assessments	Partial	No	1
	not comply with international standard	No	1
	conduct risk assessments	No	1
	by security team	No	1
	no risk assessment	No	3

4.4.8 Incidents Responses and Forensics

This section presents findings on organisation Incident response and forensics activities according to feedback from the IT experts. Table 4.15 summarises statistics from the quantitative analysis of expert responses.

Table 4.15: Incident responses and forensics stats

	Absolute No	Conditional No	Not sure	Conditional Yes	Absolute Yes
IR & forensics plan	71.4%	0.0%	0.0%	14.3%	14.3%

IR & Forensics Staff	71.4%	14.3%	0.0%	14.3%	0.0%
IR & forensics important?	0.0%	0.0%	14.3%	0.0%	85.7%

According to experts, 71.1% have no incident response or forensics plans, 71.4% has no skilled staff; however, 85.7% of organisations do consider incidents response and forensics important. Specifically, expert responses to the importance of incident response and forensics for their organisations do not correspond to organisations' incident response and forensics activities.

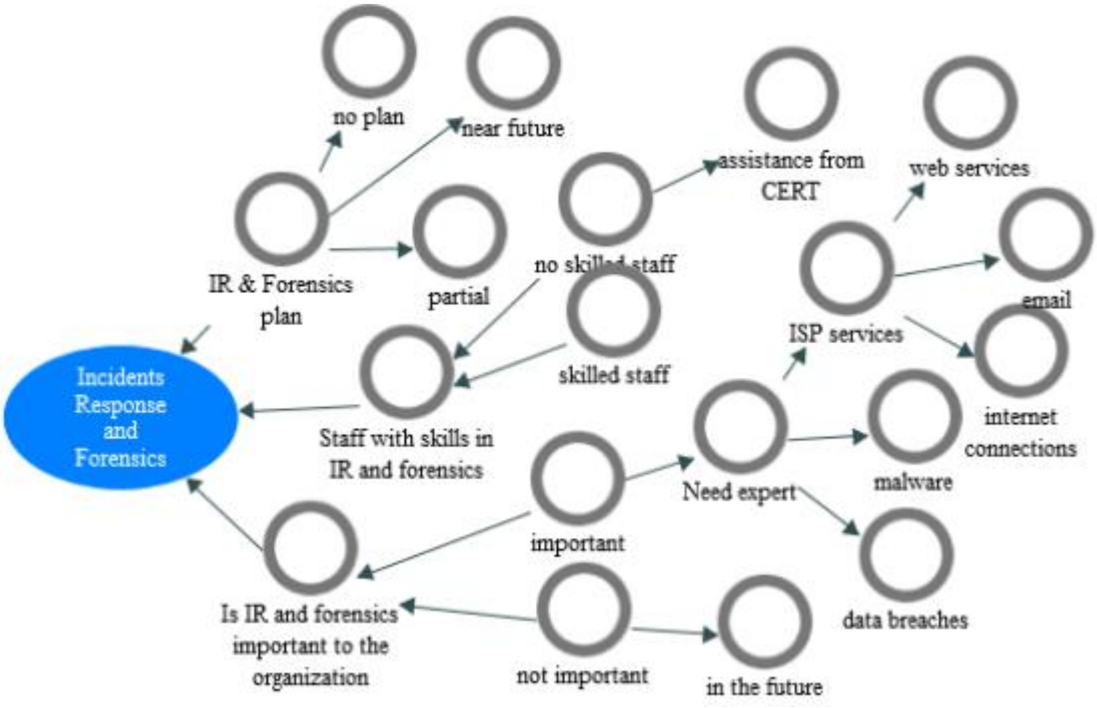


Figure 4.10: Analysis of responses about Incidents responses and forensics Base on codes in Table 4.16

The qualitative analysis in Figure 4.10, reveals that of among organisations who did have a plan, one (one reference, see table 4.16) is only a "partial" plan. For organisations who do not have any plan, one organisation plans to establish incident response and forensics plan in the "near future

Furthermore, according to the codes in Table 4.16, "no plan" has four references and "near future" has one reference, meaning five experts implied they have no incident response and forensics program, while two implied yes. However, one of that yes is "partial" which is considered as yes or no. Therefore, 85.7% of Tonga organisations' have no incident response and forensics plans. In other words, Tonga organisations lack any incidents response and forensics plan. Instead, one expert mentioned they rely on "assistance from CERT" Tonga.

Despite the statistics above, one (one reference, see table 4.16) organisation mentioned that they do "need expert" to deal with incidents like "malware" and "data breaches". The expert goes on to mention that for information security incidents occurring within their internal network and (Internet Service Provider) ISP services, they have technical capabilities. The organisation provides "web services", "email" and "internet connections" to their customers. In contrast, one expert responded that incidents response and forensics is "not important" to their organisation now but maybe "in the future".

Table 4.16: Incidents response & forensics extracted codes

Parent Name	Topics/Codes	Aggregate	References
Codes\\ISIR	Staff with skills in IR and forensics	Yes	14
	IR & Forensics plan	Yes	14
	Is IR and forensics important to the organization	Yes	14
\\IR & Forensics plan	near future	No	1
	no plan	No	4
	Partial	No	1
\\Is IR and forensics important to the organization	Important	No	6
	not important	No	1
\\Is IR and forensics important to the organization\important	Need expert	No	1
\\Is IR and forensics important to the organization\important\Need expert	data breaches	No	1
	ISP services	No	1
	Malware	No	1
\\Is IR and forensics important to the organization\important\Need expert\ISP services	Email	No	1
	internet connections	No	1
	web services	No	1
\\Is IR and forensics important to the organization\not important	in the future	No	1
\\Staff with skills in IR and forensics	no skilled staff	No	6
	skilled staff	No	1
\\Staff with skills in IR and forensics\no skilled staff	assistance from CERT	No	1

4.4.9 INFORMATION SECURITY PROCESSES

Establishing effective information security management (ISM) is the first step in establishing effective information security. Organisations must not only establish an ISM but must continually monitor, assess and improve it to remain effective. Table 4.17 summarises the statistics on Tonga organisations information security plan and internal auditing.

Table 4.17: Information security plan & internal auditing stats

	Absolute No	Conditional No	Not sure	Conditional Yes	Absolute Yes
Information security Plan	57.1%	0.0%	0.0%	42.9%	0.0%
Internal audit	57.1%	0.0%	0.0%	0.0%	42.9%

Figure 4.11 depicts the relationship between different concepts (codes) extracted from expert responses regarding organisation information security plan and internal auditing processes. According to Table 4.17, 57.1% of organisations have no information security plan, while only 42.9% of organisations conduct internal audits. A qualitative analysis of figure 4.11 shows that while 42.9% of (or three out of seven) organisations do conduct internal auditing, only one (see table 4.18, the code "active auditing" has one reference) have an active internal auditing program. One (see table 4.18, the code "not comply with international standard" has one reference) other organisation conducts internal auditing but not according to international standard. If one were to remove the organisation that conducts auditing but not according to international standards, it means 71.4% of organisations have no proper auditing program.

Furthermore, according to figure 4.11, on the topic of information security plans, one (see table 4.18, the code "dedicated staff" has one reference) organisation has dedicated information security staff, looking after their information security which is according to their plan. The rest of the experts, instead of talking about their information security plan, they discussed actions taken by their organisations to address information security threats. For instance, installing "anti-virus", conducting information security "awareness", "backup daily to cloud" and "firewall upgrade".

In other words, then 85.7% of Tonga organisations have no information security plan. In addition internal auditing activities and information security plans, Figure 4.11 also shows the state of various crucial components of information security, according to the findings discussed in section 4.4.1 to 4.4.8, regarding required information security.

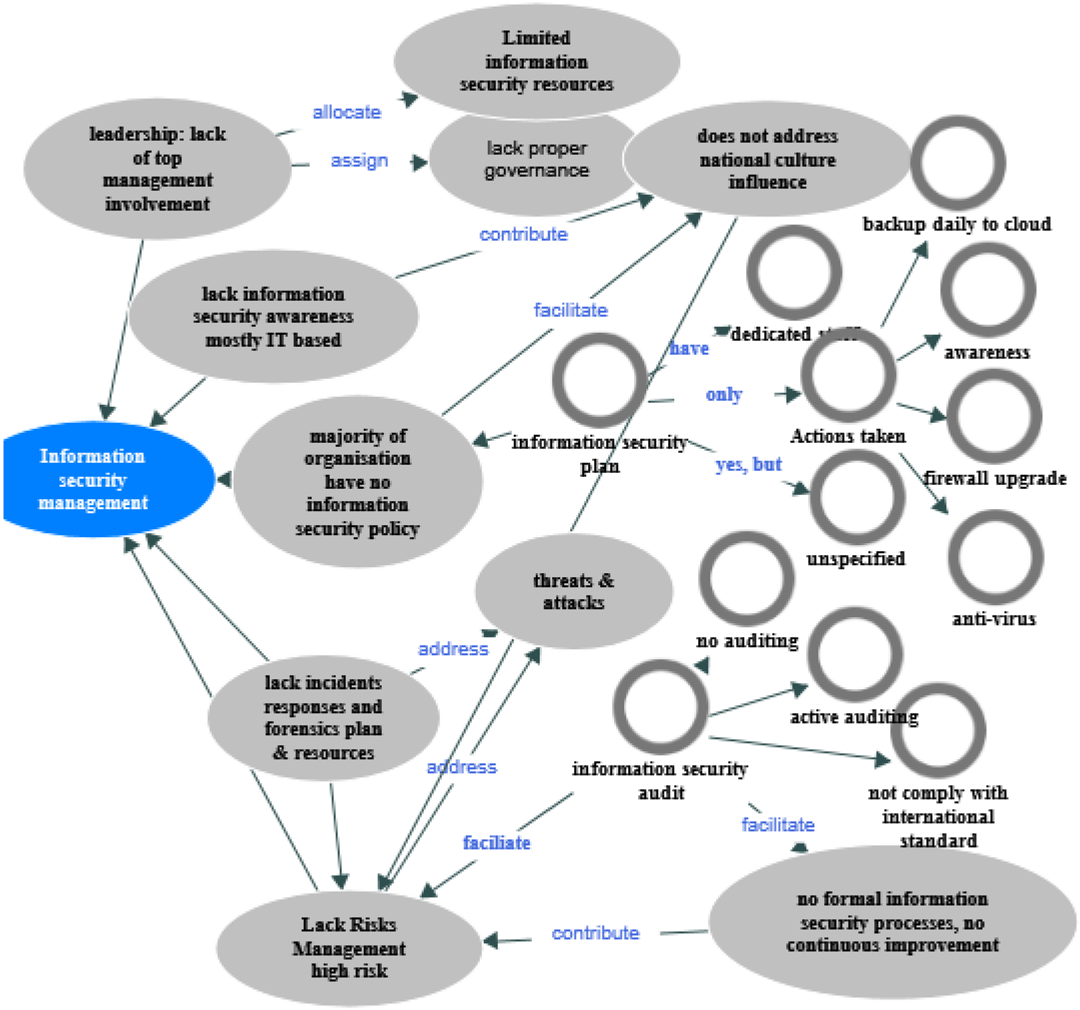

Limited information security resources
allocate
leadership: lack of top management involvement
assign
lack proper governance
does not address national culture influence
backup daily to cloud
contribute
lack information security awareness mostly IT based
facilitate
dedicated staff
have
awareness
only
Information security management
majority of organisation have no information security policy
information security plan
Actions taken
yes, but
firewall upgrade
unspecified
threats & attacks
anti-virus
no auditing
address
active auditing
lack incidents responses and forensics plan & resources
address
information security audit
not comply with international standard
facilitate
faciliate
Lack Risks Management high risk
contribute
no formal information security processes, no continuous improvement

Figure 4.11: Overview ISM processes

Analysis of responses about IS plan and internal audits

Based on codes in Table 4.18

Figure 4.11 provides a visual overview of all the findings discussed in this chapter. Tonga organisations information security are mostly IT-based, and lacked well defined and planned processes. Without well planned, and well-defined processes, organisations cannot monitor, assess, and measure their information security so they can improve and adapt it according to changes in the organisation requirements and objectives or according to changes in the organisation threat environment.

Table 4.18: Auditing & Information security plan extracted codes

Parent Name	Topics/Codes	Aggregate	References
Codes\\IS process	information security audit	Yes	13
	information security plan	Yes	13
\\information security audit	active auditing	No	1
	no auditing	No	4
	not comply with international standard	No	1
\\information security plan	dedicated staff	No	1
	unspecified	No	1
	Actions taken	No	4
\\information security plan\Actions taken	backup daily to cloud	No	1
	firewall upgrade	No	2
	anti-virus	No	2
	awareness	No	1

4.5 Summary

This chapter discussed the findings regarding Tonga organisation information security based on feedback from IT experts in Tonga. In total, seven IT experts from different organisations in Tonga were kind enough to participate in this study. The response guide provided to guide expert feedback contains the topics according to the research scope of information security. All responses were both quantitative and qualitative analysed using SPSS (version 27) and NVivo (release 1.0) respectively, and the output combined and presented in chapter 4, section 4.4.

The findings in section 4.4 are according to the topics in the response guide provided to the experts. Section 4.4.1 contains the findings regarding organisation general awareness of information security and information security standards. It is obvious from those findings alone that Tonga organisations in general lacked sufficient information security awareness. Section 4.4.2 to 4.4.8 presented findings regarding each dimension and CSFs of information security.

The findings confirmed that Tonga organisation information security is mostly ad-hoc in nature. Tonga organisations information security lacks management involvement, and many do not have any information security policy. Judging by the limited resources, information security awareness programs, incidents response and forensics programs, risk management programs, and information security plans, information security is not a high priority.

Finally, the findings and overview in section 4.4.9 indicated that Tonga organisations are not close to establishing an effective ISM. Without effective ISM, most organisations are not sure whether their information assets are secure or not. Tonga organisations also lack information security plans and internal audits. Like risk management, internal audit is vital to the success and effectiveness of any information security. These things are not only useful in planning, but also in operating and assessing information security process performance and effectiveness.

CHAPTER 5

ANALYSIS

5.0 INTRODUCTION

The main research question of this study is “Is the holistic approach provided by ISO 27001 the best approach for Tonga organisations, given their unique organisational factors and threat environments, to establish effective information security?” As discussed in section 3.2, the question can be answered by studying the impacts of implementing ISO 27001 on Tonga organisation information security. Consequently, the first step is to collect data from Tonga organisations regarding their information security. Chapter 3 discusses the data collection and analysis and the findings are presented in Chapter 4.4.

As noted in chapter 3, implementing ISO 27001 has three outcomes, mirrored by the three hypotheses discussed. The first outcome, organisations in Tonga failed to implement ISO 27001 due to organisational factors. The second outcome, Tonga organisations implement an effective information security management system. The third outcome, Tonga organisations establish effective information security to protect their information assets.

Consequently, the analysis in this chapter follows the three listed outcomes. Section 5.1 analyses the dimensions and critical success factors (CSF) of information security management (ISM), 5.2 analyses characteristics of effective information, 5.3 focuses on the alternative outcomes, and section 5.4 provides a summary of the analysis.

5.1 ANALYSIS OF EFFECTIVE ISM

This section presents a gap analysis of Tonga organisation information security against ISO 27001 requirements. Specifically, the analysis compares organisations’ existing information security with an ISO 27001 based information security. The different dimensions and CSF of information security are addressed. The sections follow the hypotheses H1a to H1g in chapter 3, specifically, section 5.1.1 to 5.1.9 test hypothesis H1a to H1g, respectively.

5.1.1 Management Involvement

The gap analysis in this section focuses on analysing the gaps between Tonga organisation top management involvement in their information security and ISO 27001 requirements. According to the findings in 4.4.2, while 71.4% of the organisations said top management is involved in information security, qualitative analysis of expert responses as shown in figure 4.3, reveals that management involvement in information security is limited.

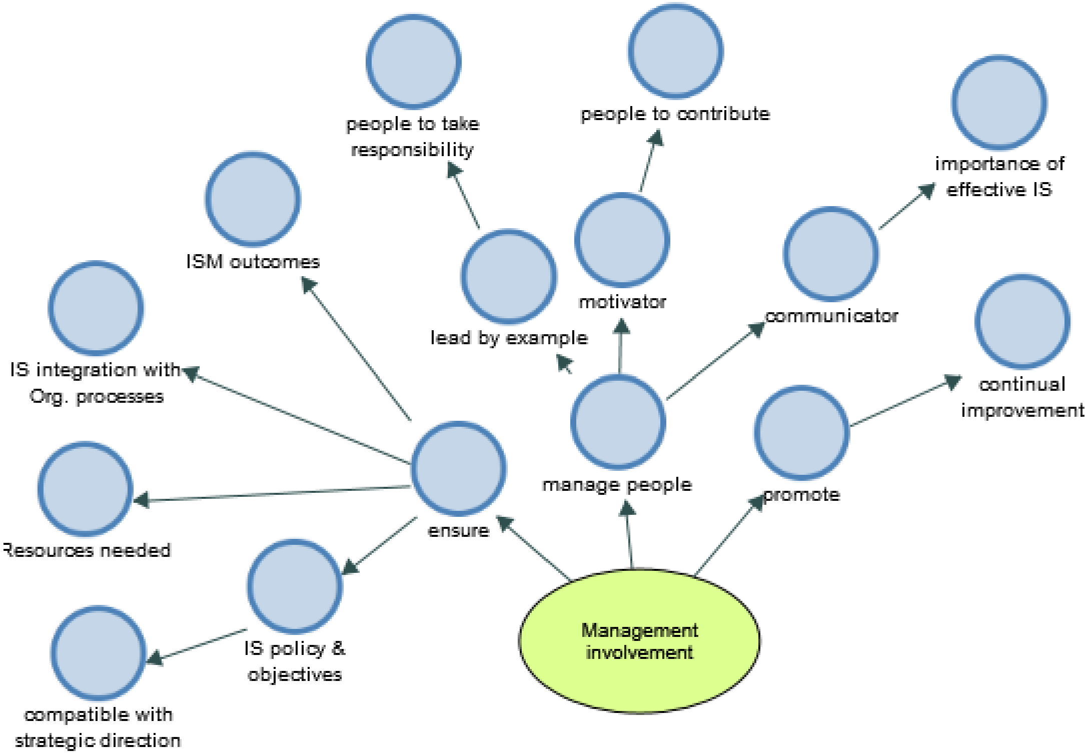


Figure 5.1: ISO 27001 Management Involvement Analysis

Adapted from (BSI, 2017a)

In contrast, Figure 5.1 shows ISO 27001 requirements for management involvement, i.e. leadership requirements. Specifically, according to ISO 27001, the extent of top management involvement in information security goes beyond just approving budgets and projects as in the case of Tonga organisations. Top management responsibilities under ISO 27001 include ensuring organisations develop an information security policy, allocating information security resources, establishing information security governance, and are ultimately responsible for the outcomes of the organisations' information security programs. Furthermore, according to ISO 27001, top management must also promote continual improvement, information security processes, people, and set an example for other leaders to follow when it comes to information security.

Table 5.1 summarises the differences (i.e. gaps) between Tonga organisations' top management involvement and what ISO 27001 requires. Specifically, Tonga organisations top management involvement in their information security has gaps compared to what ISO 27001 requires. Therefore, implementing ISO 27001 will have a significant positive influence on Tonga top management involvement in information security.

Table 5.1: Top management involvement gaps analysis

Tonga organisations' information security based on ad-hoc approaches	Tonga organisations' information security based on ISO 27001
Top management has limited involvement in Information security	Required extensive management involvement
Approve budget	Establish information security policy
Approve projects	Responsible for defining the scope of information security management system (ISMS)
Involve in technical implementation	Responsible for information security outcomes
Involve only on issues that of interest to them	Establish governance structure, assigning roles and responsibilities
	Information security awareness programs
	Allocate information security resources
	Involved in risks management
	Responsible for continual improvement of information security processes

5.1.2 Information Security Policy

According to the findings of 4.4.3, while the majority of the organisations said they have an information security policy, some of them are Information Technology "(IT) policy" or "acceptable use" as depicted by Figure 4.4. Specifically, the majority of

Tonga organisations have no information security policy and do not differentiate between information security policy and "IT policy".

In contrast, according to ISO 27001 section 5.2, organisations management shall; 1. Establish an information policy, which among other requirements must include a commitment to the continuous improvement of the ISM. 2. Organisations must document their information security policy. 3. Organisations must communicate the information security policy to the organisation. 4. The information security policy must be available to other parties.

According to ISO 27003, the information security policy should contain brief statements specifying the intent and focus of the organisations' information security. Organisations' should align their information security objectives, procedures, and activities with their information security policy (BSI, 2017d). In other words, from an ISO 27001 perspective, information security policies are the glue that hold information security processes together, without which everything is disjointed and uncoordinated.

Table 5.2 summarises the different between Tonga organisations and ISO 27001 in term of information security policy. The gaps between what Tonga organisations have and effective information security policy, and what ISO 27001 requires, are significant due to the lack of management involvement as in section 5.1.1 and a lack of awareness according to findings in 4.4.1. Therefore, implementing ISO 27001 will provide the necessary awareness and knowledge by establishing a compulsory security policy requirement, which will motivate Tonga organisations to establish a comprehensive information security policy that will be beneficial to the organisations.

Table 5.2: Information security policy gaps analysis

Tonga organisations' information security based on ad-hoc approaches	Tonga organisations' information security based on ISO 27001
Almost half of organisations have no information security policy	Organisations must develop an information security policy
IT and Acceptable use policies	Top management is responsible for establishing an information security policy
No awareness training, see 5.1.3	Communicate Information security policy to every stakeholder, inside or outside the organisation.

	Organisations must enforce their Information security policy.

5.1.3 Information Security Awareness

According to the findings in section 4.4.1 and 4.4.5, Tonga organisations generally lacked awareness of information security and information security standards. For instance, a complete lack of awareness of ISO 27001, one of the most well-known information security standards today. Furthermore, Tonga organisations also lacked information security awareness training, and very few organisations have any non-IT department that is aware of information security issues and / or is actively involved in information security.

Moreover, according to findings in 4.4.6 on addressing influences of Tongan culture on organisation information security and 4.4.4 on organisation IT staff information security training, suggest that organisation awareness of information security is technological. The participants, with few exceptions, refer to technological solutions when discussing measures they use to address information security issues. According to ISO 27001 section 7.3, "persons doing work under the organisation's control", i.e. employees, contractors, business partners, suppliers, must: 1. Aware of the organisations' information security policy. 2. Aware of how they contribute to the effectiveness of the information security. And, 3. Aware of the consequences of not complying with the organisations' information security policy.

Moreover, according to ISO 27003, organisations must prepare an awareness programme with specific messages depending on the audiences. They must include information security needs and expectations within awareness and training materials on other topics to place information security needs into relevant operational contexts. Organisations should run their awareness program at regular intervals. Staff knowledge and understanding of the awareness message should be verified after each awareness programme done at random intervals (BSI, 2017d).

Table 5.3 below summarises the differences between Tonga organisation current information security awareness practices and what ISO 27001 requires. As evident from the list of ISO 27001 requirements, there is a significant gap between organisational information security awareness and what ISO 27001 requires. ISO 27001 requires establishing of awareness programs, but also organisations must run those awareness programs continuously. Therefore, implementing ISO 27001 will improve Tonga organisation information security awareness.

Table 5.3: Information security awareness gaps analysis

Tonga organisations' information security based on ad-hoc approaches	Tonga organisations' information security based on ISO 27001
Lacks awareness of information security and standards	Organisations must communicate their information security policy to all internal and external stakeholders.
Lacks information security policies	Staff must understand, accept and support the objectives stated in the information security policy
Lacks awareness training	Train staff to know their roles and how they can contribute to the effectiveness of information security
Lacks end-to-end information security awareness, i.e. other departments have limited awareness of information security	Inform staff of the consequences of not complying with organisations' information security policy
Awareness limited to when IT informed them of malicious emails and software	Awareness programme tailor to a particular audience
	Conduct awareness programmes at regular intervals
	Verify staff knowledge, understanding and awareness of information security after each awareness session or random sessions.

5.1.4 Information Security Culture

According to the survey findings, Tongan culture influences organisational culture, which in turn influences the organisations' information security culture. The qualitative analysis depicted by Figure 4.7 in section 4.4.6, shows that Tonga organisations, while aware of Tongan culture influences on information security, the majority do not do anything about it. One cultural factor mentioned by experts is the influence of "family and friends". Specifically, employees tend to share their passwords and other information with family and friends, who sometimes are also co-workers. According to the findings in 4.4.6, the solution provided includes establishing information security policy and technical solutions. The rest either said “do nothing” or did not provide any feedback.

In contrast, according to ISO 27001 requirements 5.1, 5.2 and 7.3, (1) organisations will establish an information security policy and (2) awareness programs to communicate the policy to staff with the support of the organisations' top management. Also, ISO 27001 section 7.4 stated that organisations "shall determine the need for internal and external communications relevant to the information security management system" (BSI, 2017, p. 6). It means, not only organisations must develop information security processes (as part of an Information Security Management System (ISMS)) they must also communicate those processes (objectives, requirements, how it is relevant to them) to both internal and external stakeholders. In other words, ISO 27001 mechanisms for addressing influences of national and organisational cultures on information security, are via its information security policy requirements and information security awareness requirements.

Table 5.4 provides a summary of gap analysis of Tonga organisation activities and ISO 27001 required activities that would contribute to organisations establishing a positive information security culture. The significant gaps between ISO 27001 requirements and Tonga organisation practices mean that implementing ISO 27001 will significantly improve Tonga organisation information security culture.

Table 5.4: information security culture gaps analysis

Tonga organisations’ information security based on ad-hoc approaches	Tonga organisations’ information security based on ISO 27001
Acknowledge the influence of national culture on information security	Organisations must develop an information security policy
Acknowledge the influence of organisations’ culture on information security	Organisations’ stakeholders (employees, partners, suppliers) must be made aware of the policy objective and requirements.
Not addressing the influence information security culture on effectiveness of information security, i.e. “do nothing”	Organisations must establish awareness programme conducted at regular intervals instructing stakeholders on how they contribute to the effectiveness of information security.
	Management must indicate their support of the Information security policy, and stakeholders should be made aware of the consequences of non-compliance.

5.1.5 Information Security Risks Management

The fifth expected outcome of implementing ISO 27001 is that Tonga organisations will improve their risk management. The findings discussed in section 4.4.7 demonstrated the need for effective information risk management due to information security threats and the attacks organisations experienced. According to the analysis in Figure 4.8 and findings by Laulaupea'alu and Keegan (2019), the majority of attacks like social engineering attacks, spam, and viruses are human factor-based attacks which cannot be fully addressed by technological solutions alone. It is therefore important that organisations assess all risks to their information assets to identify appropriate controls to mitigate those risks.

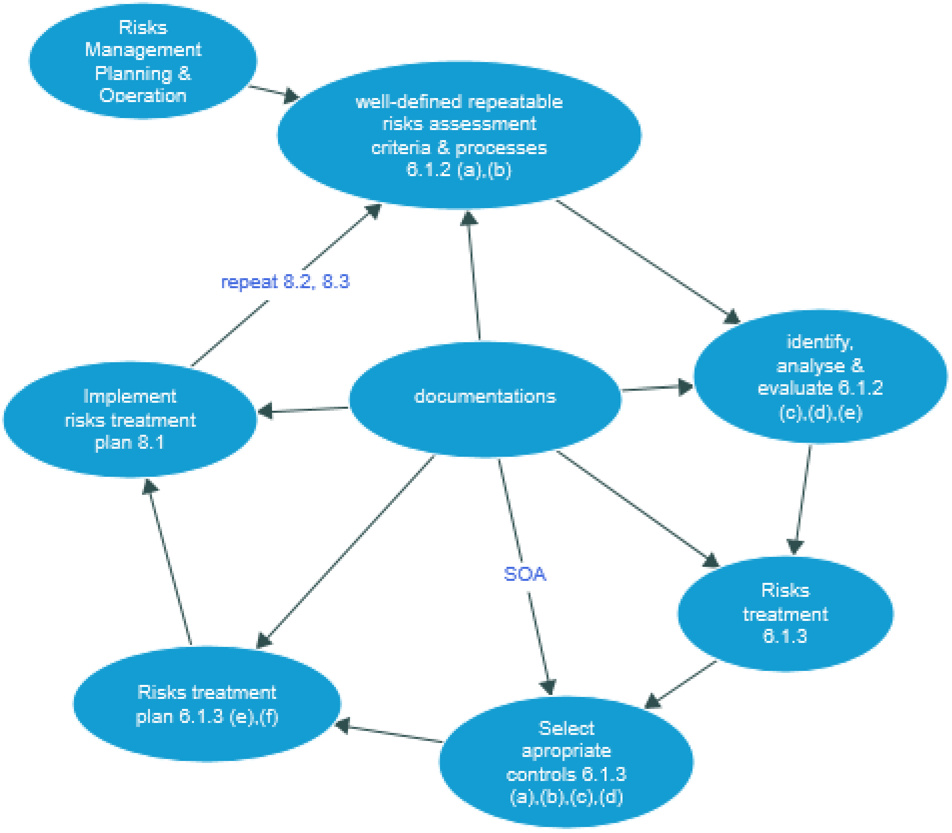

Risks Management Planning & Operation
well-defined repeatable risks assessment criteria & processes 6.1.2 (a),(b)
repeat 8.2, 8.3
Implement risks treatment plan 8.1
documentations
identify, analyse & evaluate 6.1.2 (c),(d),(e)
SOA
Risks treatment 6.1.3
Risks treatment plan 6.1.3 (e),(f)
Select apropriate controls 6.1.3 (a),(b),(c),(d)

Figure 5.2: ISO 27001 risks management requirements (BSI, 2017a)

According to the analysis of expert responses, Tonga organisation risk management processes are either non-existent or ad-hoc at best. A fact illustrated by the high number of experts (42.9%) who are not sure if their organisations' information assets are secure or not. While, according to the statistics in Table 4.13, 57.1% of organisations did not conduct risk assessments of their information assets, only one organisation has an information security team that they said conducted active risk assessments. The ISO 27000 family of standards, reviewed in chapter two, placed heavy emphasis on risk management. Figure 5.2 showed ISO 27001 required risks management activities. Within the ISO 27000 family of standards, ISO 27001 provides the main (risks management) requirements, and ISO 27005 provides guidelines to help organisations plan and implement their risks management programs. ISO 27001 risk management processes include risk assessment, risk analysis and risk treatment, with requirements for conducting risk assessment and treatment during the planning phase (ISO 27001 section 6.1.2 and 6.1.3) and the operation phase (ISO 27001 section 8.2 and 8.3). More importantly, since ISO 27001 emphasises continuous improvement, risk management processes under ISO 27001 are also continuing to keep up changes in organisation requirements, objectives and information security threat environments.

Table 5.5 provides a gap analysis of Tonga organisation risk management practices, and an ISO 27001 based information security management (ISM), risk management practices check. The non-existence of Tonga organisation information security risk management programs means implementing ISO 27001 will have a significant positive impact on the Tonga organisations' ability to establish a comprehensive risk management program.

Table 5.5: Risks management gaps analysis

Tonga organisations' information security based on ad-hoc approaches	Tonga organisations' information security based on ISO 27001
Almost half of the organisations are not sure if their information assets are secure or not.	Organisations must conduct information security risks assessment.
Almost half of the organisations never conducted any information security assessment of their information assets	Organisations must conduct information security risks analysis based on risks assessments.
Only one organisation conducted "active" information security risks assessment.	Organisations must formulate a risks treatment plan based on their risks analysis.
	Organisations must repeat risks management processes at regular intervals

5.1.6 INFORMATION SECURITY RESOURCES

The sixth expected outcome of implementing ISO 27001 is that Tonga organisations will improve information security resources. The statistics in Table 4.6 illustrated Tonga organisations lack of skilled information security staff and financial resources. For instance, the majority (74.1%) of participating organisations have no skilled incident response and forensic staff. In addition, 85.7% do not have certified information security staff, while 57.1% do not have dedicated information security staff. Moreover, 42.9% of organisations do not have an information security budget.

Qualitative analysis of organisation resources depicted by Figure 4.5 in 4.4.4 indicated that the resources Tonga organisations are allocating for information security is not proportionate with the information assets that the participating organisations are looking after. For instance, financial data, ISP services, and government data. One interesting point made by one of the participants is their organisations has an information security budget, but they 'don't need to spend it'.

According to ISO 27001 section 5.1, organisation top management should ensure "that the resources needed for the information security management system are available" (BSI, 2017a, p. 2). Section 7.1 also specified that the "organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system" (BSI, 2017a, p. 5). In other words, organisations must provide staff to direct the activities, time to perform activities, financial resources, and technology, and tools and materials depending on each organisation ISMS needs (BSI, 2017d).

Table 5.6 summarises the gaps analysis in Tonga organisations' information security resources and what ISO 27001 requires. The main point is Tonga organisations will be willing to support an ISO 27001 implementation because it is a proper business project with: 1. legitimate business reasons why they must make information security a priority; 2. Well-defined resources needs; 3. a tangible outcome (security of the organisations' information assets) which organisations can measure. 4. Well-defined processes which organisations can integrate with their internal processes. Therefore, this gives organisations reasons to invest in improving their information security by ensuring it has the necessary resources.

Table 5.6: Information security resources gaps analysis

Tonga organisations' information security based on ad-hoc approaches	Tonga organisations' information security based on ISO 27001
Lacks dedicated and certified information security staff	Organisations must provide resources sufficient to support the implementation and operation of information security management
Tonga organisations do not prioritise information security judging by the resources they provided for information security	Resources include: • Financial resource • Personnel • Facilities, and • Technical infrastructure
Lacks of skilled incidents response and forensics staff	top management should assess resource needs during management reviews and set objectives for continual improvement and monitoring effectiveness of planned activities
Close to half of organisations do not have an information security budget	Offer a proper business project with well-defined plan, resources, and outcomes which the organisations can measure & integrate as part of its business processes

5.1.7 Information Security Governance

According to findings in 4.4.2, first and foremost Tonga organisations lack appropriate top management involvement in information security. Top management involvement is necessary since they are the only one who can assign roles and authorities necessary to properly manage organisations' information security. The data shows that they also lack well-defined information security governance, i.e. lack dedicated information, security staff, according to the findings in 4.2.4 and analysis in 5.1.6. Finally, Tonga organisations lack properly trained information security professionals according to findings in section 4.4.1 and 4.4.4. In other words, Tonga organisations' information security is mostly governed and run by their IT departments according to the findings in chapter 4.

The ISO 27001 and the ISO 27000 family of standards put great emphasis on organisations establishing proper information security governance structures. According to ISO 27001 section 5.3, part of leadership, i.e. top management responsibilities is the establishment of an information security governance structure by allocating authorities, roles and responsibility. According to ISO 27003, “Top management ensures that roles and responsibilities as well as the necessary authorities relevant to information security are assigned and communicated” (BSI, 2017d, p. 9). Furthermore, the ISO 27000 family of standards also come with ISO 27021, which provides guidelines on skills (competencies) needed for each information security role. For instance, relevant leadership skills, communication skills, resources management skills, and risks management skills (BSI, 2017e). The guidelines provided by ISO 27021 allows organisations to identify the exact human and financial resources they need and be able to budget accordingly.

Table 5.7 summarises the gaps between Tonga organisations existing information security governance, or lack thereof and what an ISO 27001 based ISM requires. Specifically, implementing ISO 27001 will improve Tonga organisation information security resources, allowing them to establish effective information security governance.

Table 5.7: ISG gaps analysis

Tonga organisations’ information security based on ad-hoc approaches	Tonga organisations’ information security based on ISO 27001
Lack of top management involvement in information security	Requires extensive top management involvement in information security
Lack of dedicated information security body and information security staff	Requires management to establish an information security governance with assigned roles and responsibilities
Lack of properly trained information security staff	Provide specific guidelines on required competencies (i.e. what skills information security professionals needed to implement ISO 27001 based ISM). Organisations can either trained or hire proper information security staff.
	ISM roles are well defined together with what skills needed for each role

5.1.8 Summary of Analysis of effective ISM

The final expected outcome of implementing ISO 27001, is that it will enable Tonga organisations to effectively manage their information security. The findings in chapter 4 section 4.4.9 show Tonga organisations lack systematic, and organised information security processes. Specifically, figure 4.11 summarises the findings regarding Tonga organisations' information security.

Tonga organisations lack of information security management processes is illustrated by the gaps between Tonga information security practices and ISO 27001 requirements, identified by gap analysis in section 5.1.1 to 5.1.7. The identified gaps mean that implementing ISO 27001 will have significant positive impacts on each of the areas: management involvement, information security policy, awareness, culture, risk management, resources and governance. Each of those areas represents various dimensions or critical success factors of information security. Therefore, implementing ISO 27001 will allow Tonga organisations to effectively address (positive impacts) the areas.

Consequently, since according to studies summarise in table 3.1, effective ISM employs holistic approaches to address various dimensions and critical success factors of information security that minimise risks to organisation information assets. The study can affirm the assertion that by implementing ISO 27001, Tonga organisations will establish effective ISM.

5.2 ANALYSIS OF EFFECTIVE INFORMATION SECURITY

This section focus on gap analysis of factors found in Tonga organisations existing information security and Tonga organisations ISO 27001 based information security, that characterise effective information security. The discussion follows the hypotheses, H2a to H2d in chapter 3.

The characteristics of effective information security according to studies reviewed in chapter two and those summarised in Table 3.1 include: 1. they are addressing different dimensions and critical success factors (CSF) of information security, discussed in section 5.2.1. 2. Minimising information security risks to organisation information assets, discuss in section 5.2.2. 3. Continuously improve information security management (IMS), discussed in section 5.2.3 and 4. Business-aligned information security, in discussion section 5.2.4.

5.2.1 Addressing Dimensions and CSF

One of the characteristics of effective information security and an expected outcome of implementing ISO 27001 is that Tonga organisations information security will be addressing all the dimensions of human factors, cultural factors, and technological factors, for information security. According to multiple studies, top management involvement is one, if not the most important CSF of information security (Arbanas & Žajdela Hrustek, 2019; Choejey et al., 2016; Diesch et al., 2020; Kazemi et al., 2012; Mousavi & Kumar, 2019). It is evident from the analysis in 5.1.1 that implementing ISO 27001 will improve Tonga organisations' top management involvement in information security.

Furthermore, improving top management involvement in information security will have significant positive impacts on other CSF like establishing comprehensive information security policy (see 5.1.2), establishing positive information security culture (see 5.1.4), and improving organisations' information security awareness (see 5.1.3). Addressing the CSF above are critical because they combine to address the human and sociological dimensions of information security.

As noted in the analysis in section 5.1.2 and 5.1.3, implementing ISO 27001 will result in Tonga organisations establishing a comprehensive information security policy and awareness programs. Those programs will, in turn, help Tonga organisations develop a positive information security culture as per analysis in section 5.1.4. Furthermore, according to analysis in 5.1.7, implementing ISO 27001 will improve Tonga organisations information security governance. In other words, according to analysis in section 5.1, implementing ISO 27001 will have significant positive impacts on how Tonga organisations address various dimensions and the CSF of information security.

5.2.2 Minimised Information Security Risks

A crucial expected outcome of implementing ISO 27001 is that Tonga organisations will be able to minimise risks to their information assets. Risks minimisation is a critical aspect of effective information security since it is impossible to eliminate all negative risks (Boyle & Panko, 2015; Taylor, 2015). Specifically, there is no such thing as absolute or comprehensive security. The best organisations can hope for, and the main emphasis of information security is to protect information assets by minimising risks from information security threats.

As noted by studies reviewed in chapter two and summarises in Table 3.1, information security is multidimensional, i.e. it is not purely technological but has other dimensions like human and cultural dimensions. For organisations to effectively protect their information assets, they must identify and address risks from all dimensions and not just threats from technology.

According to the analysis in section 5.1 and 5.2.1, Tonga organisations will be able to implement information security that addresses all dimensions and CSF of information security by implementing ISO 27001. By addressing and minimising risks from different dimensions of information security, Tonga organisations will be improving the effectiveness of their information security.

5.2.3 Continuously Improved Information Security

One of the expected outcomes of implementing ISO 27001 is that it will enable Tonga organisations to continually improve their information security. According to Humphreys (2016), organisations ability to continuously improve their information security is critical because of the "degree of uncertainty regarding information security risks in today's fast-changing business environment means that organisations need to be proactive and adaptive to the risks brought about by such changes" (Humphreys, 2016, p. 179).

Consequently, in order for Tonga organisations to establish effective information security, they must be able to establish an ISM that they can continuously improve. Subsequently, according to the analysis in section 5.1.8, the impact of implementing ISO 27001 is the ability of Tonga organisations to establish effective ISM by implementing ISO 27001. Since continuous improvement is part of ISO 27001 requirements (BSI, 2017a), Tonga organisations will be able to establish an ISM that they can continuously improve to deal with changing technologies and threat environments.

5.2.4 Information security & Business objectives Alignment

The last expected outcome of implementing ISO 27001 is that Tonga organisations will be able to better align their information security with their business requirements and objectives. In other words, information security "should be a business enabler, adding value to the business and minimizing the information security risks to help maximize its business opportunities" (Humphreys, 2016, p. 28). The survey findings discussed in section 4.2.1 noted the lack of awareness both by management and IT, not only of information security standards in general but also specific standards like ISO 27001. The lack of awareness of information security frameworks both by top management and IT staff means organisation information security will lack cohesion due to the lack of organised and documented information security processes. For instance, section 4.2.3 discusses organisation information security policy or lack thereof. The lack of information security awareness is discussed in section 4.2.5. The lack of information security risk management is discussed in section 4.2.7, and lack of information security planning is discussed in section 4.2.9. Without a well-defined information security plan and information security processes; it will be hard for organisation information security to adapt to change and to align with internal and external requirements, and the business objectives.

Implementing ISO27001 means organisations will be establishing an ISM with organised and documented (requirements 7.5) processes with continuous improvement, as discussed in section 5.2.3 above. Accordingly, "The organisation shall continually improve the suitability, adequacy and effectiveness of the information security management system" (BSI, 2017, p. 9). Since ISO 27001 based ISMS processes are well-planned, well-defined and documented, organisations can integrate their ISMS processes with their business processes. Therefore, making it easier for organisations to adapt and align their information security processes and objectives with their business objectives and requirements, continuously.

5.2.5 SUMMARY OF ANALYSIS OF EFFECTIVE INFORMATION SECURITY

According to studies reviewed in chapter 2 and summarises in table 3.1, effective information security is information security that: 1. Employs a holistic approach to address various dimensions and CSFs of information security. 2. Minimised risks to organisations information assets. 3. Continuously improve to remain relevant. 4. Align with organisation business goals and requirements.

The analysis in sections 5.2.1 to 5.2.4 and 5.1, confirmed that by implementing ISO 27001, Tonga organisations would effectively manage their information security, thereby establishing information security that is aligned with their business goals and requirements. This addresses the various dimensions and CSF of information security to minimised risks to their information assets, and continuously improve to remain relevant. Therefore, the study can affirm the assertion that Tonga organisations will establish effective information security by implementing ISO 27001.

5.3 NOT THE RIGHT APPROACH

The control hypothesis of the study state that that implementing ISO 27001 is not the right approach for Tonga organisations to improve their information security, given (because of) their organisational factors and dynamic threat environment. This section will analyse the validity of such an assertion based on the findings in chapter 4 and analysis in sections 5.1 and 5.2. The rest of the section focuses on the analysis of arguments supporting the assertion, section 5.3.1, and analysis of arguments against, section 5.3.2.

5.3.1 ARGUMENT FOR

The finding that Tonga organisations are lacking in information security resources, discussed in 4.4.4, is the one that most likely supports this assertion. The Tonga information security threat environment according to findings in chapter 4, section 4.4.7, is not a factor that will inhibit Tonga organisations from implementing ISO 27001, rather they are reasons why Tonga organisations should implement effective ISM.

Out of the organisational factors identified by studies reviewed in chapter two, lacking resources is one of the more critical factors. According to multiple case studies, many SMEs either failed to or do not intend to implement ISO 27001 because they lack either financial resources or skilled information security staff. For instance, a study like Alshitri and Abanumy (2014) identified a lack of skilled information security professional, or a study by Gillies (2011) which identified lacking financial resources as factors inhibiting the adoption of ISO 27001.

Why are those studies findings relevant? They are relevant because Tonga organisations and government departments are small, and most studies will identify them as SMEs based on the number of staff and revenue. Consequently, it is logical to assume that factors affecting other SMEs will affect Tonga's organisations ability to implement ISO 27001 as well.

5.3.2 ARGUMENT AGAINST

While findings in 5.3.1 are legitimate findings worthy of consideration, they also raise several questions: 1. Do Tonga organisations information security lack resources because organisations generally lack resources? 2. Do Tonga organisations lack information security resources because of priorities?

According to findings in 4.4.4, Tonga organisations do allocate resources for information security. For example, 100% of the organisations have IT staff and most organisations have an information security budget. Furthermore, according to a survey by Laulaupea'alu and Keegan (2019), 25% of organisations have local information security specialists, 19% hired specialists from other organisations and 5% hired overseas specialists.

In other words, from the findings, answers to the questions above are; 1. Tonga organisations do have resources they just do not spend it on information security. 2. Tonga do have access to information security professionals, either locally or from regional countries, that organisations can hire. Instead, what it stands out from the findings in chapter 4, sections 4.4.1 and 4.4.5, is Tonga organisations lack information security awareness. Specifically, Tonga organisations lack awareness of information security and standards and lack management involvement in information security. As a result, information security is not a priority for many organisations.

The most telling of the findings is 4.4.4 in which one organisation mentioned that the organisations have an information security budget, but they 'don't need to spend it'. In other words, organisations do provide provisional budgets in case they need it, but it is not mandatory for IT or information security departments to prepare and submit an implementation plan and ROI analysis for it. Therefore, one cannot argue with any certainty that implementing ISO 27001 will be failed because of lack of resources. If anything, according to 5.1.6, implementing ISO 27001 will improve organisations' information security resources.

5.4 Summary

This chapter discussed gap analysis of the Tonga existing information security against ISO 27001 requirements based on three expected outcomes (of Tonga organisations implementing ISO 27001). The outcomes are: 1. they will establish effective ISM. 2. Establish effective information security. 3. They failed to implement it, i.e. not the right approach because of organisation factors like lack of resources.

The analysis in 5.1 is based on the findings by studies reviewed in chapter two (see Table 3.1) that effective ISM utilises holistic approaches to systematically addresses all dimensions and CSF of information security. Consequently, the analysis of Tonga organisation information security against ISO 27001 requirements focuses on how they address different dimensions and CSF of information security. The analysis concluded that Tonga organisations would establish effective ISM by implementing ISO 27001.

Furthermore, the analysis in 5.2 follows on the analysis in 5.1; however, it focuses on the characteristics of Tonga organisations' information security and ISO 27001 based ISMS that characterise them as effective information security. The characteristics include the ability to minimise risks by addressing all dimensions of information security that are continuously improved, and aligned with organisation business objectives and requirements. The analysis found that Tonga organisations will improve the effectiveness of their information security by implementing ISO 27001. Tonga organisations information security lacks in critical areas like risk management, internal auditing, and management involvement and above all, lacks any systematic, holistic ISM.

According to analysis in 5.3, while there is always a possibility that implementing ISO 27001 will fail due to lacks of resources, but the findings suggested that Tonga organisations problems are not resources but lack of information security awareness. As a result, Tonga organisation information security is still IT and purely technological based. Because Tonga organisations information security processes are ad-hoc and lacking in many areas, implementing ISO 27001 will have significant impact on organisation ISM and effectiveness of their information security in protecting their information assets.

CHAPTER 6

DISCUSSION

6.0 INTRODUCTION

This chapter discusses the findings of Tonga information security from chapter 4 and the gap analysis in chapter 5. The discussion focuses on mapping the findings and gap analysis to hypotheses in chapter 3, to answer this study research questions. Furthermore, chapter 4 presents the findings on Tonga information security together with the gap analysis of the findings against ISO 27001 requirements in chapter 5. This identifies the impacts of implementing ISO 27001 on Tonga organisation information security.

Consequently, this chapter presents no new findings or analysis. Instead, the focus of discussion in section 6.1, is solely on mapping the findings and the gap analysis to hypotheses and summarise the outcomes of the mappings to answer the research questions. The rest of the chapter is as follows. Section 6.2 discusses constraints which may directly or indirectly affect the outcome of this study, and section 6.3 summarises the discussions of this chapter.

6.1 DISCUSSION OF GAP ANALYSIS

This study aims to determine the best approach for Tonga organisations information security by comparing the current state of their information security with information security established and managed by an ISO 27001 based information security management system (ISMS).

Consequently, this section focuses on discussing the outcomes of the gap analysis in chapter 5 in relation to the hypotheses in chapter 3. Therefore, section 6.1.1 focuses on answering the study's second research question, while section 6.1.2 focuses on answering the study's main research question.

6.1.1 RESEARCH QUESTION TWO

The second research questions asked, "What are the impacts of implementing ISO 27001 on Tonga organisation information security management and information security?" As discussed in chapter 3, the study will answer the question by focusing on the analysis of two areas of impact. The first is the impact of implementing ISO 27001 on the effectiveness of Tonga organisations' information security management. The second is the impact of implementing ISO 27001 on the effectiveness of Tonga organisations information security. Subsequently, this study developed two hypotheses, H1 and H2. H1 focuses on testing the impacts of implementing ISO 27001 on the effectiveness of Tonga organisation' information security management (ISM), while hypothesis H2 focuses on testing the impacts of implement ISO 27001 on the effectiveness of Tonga organisation information security.

The rest of this section is arranged as follows. Section 6.1.1.1 focuses on the impacts of implementing ISO 27001 on the effectiveness of organisation ISM based on the outcome of testing H1. Section 6.1.1 focuses on the impacts of implementing ISO 27001 on the effectiveness of organisation information security based on the outcome of testing H2. Finally, Section 6.1.1.3 provides a conclusive summary of the analysis of question two.

6.1.1.1 EFFECTIVE INFORMATION SECURITY MANAGEMENT

One of the expected outcomes of Implementing ISO 27001, is that given their unique organisational factors and dynamic threat environment, Tonga organisations will develop effective Information security management (ISM). The process of testing the validity of the stated outcome (effective ISM) requires this study to test each characteristic of an effective ISM, identified in chapter 2 and summarised in table 3.1. Specifically, testing hypothesis H1 requires testing of hypotheses H1a to H1g, which represent the various dimensions and critical success factors (CSF) of effective ISM.

Hypothesis H1a indicates a positive relationship between implementing ISO 27001 and improving Tonga organisation top management involvement in information security. An assertion that the gap analysis in section 5.1.1, which is summarised in

Table 5.1, is affirmed. Hypothesis H1b, on the other hand, indicates a direct positive relationship between implementing ISO 27001 and Tonga organisations establishing a comprehensive information security policy. The support data is found in the gap analysis in section 5.1.2, summarises in Table 5.2, and is affirmed.

The third hypothesis H1c indicates a positive relationship between implementing ISO 27001 and improving Tonga organisation information security awareness. The gap analysis in section 5.1.3, is summarised in Table 5.3, confirms the assertion, indicating significant positive impacts. Furthermore, the hypothesis H1d indicates a positive relationship between implementing ISO 27001 and improving Tonga organisation information security culture. The gap analysis in section 5.1.4 agrees indicating implementing ISO 27001 will have significant positive impacts on organisation information security culture.

The fifth hypothesis H1e indicates a positive relationship between implementing ISO 27001 and improvement of Tonga organisation risk management. Whilst hypothesis H1f indicates a relationship between implementing ISO 27001 and improving Tonga organisation information security resources. Both relationships are affirmed by the gap analysis in section 5.15 and 5.1.6, respectively. Implementing ISO 27001 will have significant impacts due to the current state of organisation information security risk management processes and information security resources.

The last hypothesis H1g indicates a relationship between implementing ISO 27001 and improved organisation governance of information security. The gap analysis in section 5.1.7, summarised in Table 5.7 not only affirmed a positive relationship but offers a significant improvement to organisation information security governance due to Tonga organisations lack of information security governance structure.

Finally, hypothesis H1 indicates a positive relationship between implementing ISO 27001 and effective ISM. According to studies in chapter 2, effective ISM employs a holistic approach to systematically address all dimensions and CSF of information security. Consequently, the study confirmed the positive impacts of implementing ISO 27001 on Tonga organisations' ability to establish effective information security management, based on the outcomes of the testing of hypotheses H1a to H1g above and analysis in section 5.1.8.

6.1.1.2 Effective Information Security

The second area that this study theorised that will be impacted by implementing ISO 27001 is the effectiveness of Tonga organisations information security. Effective information security according to studies reviewed in chapter 2 and summaries in Table 3.1 is one that minimised information risks by assessing and treating risks from all dimensions of information security, i.e. technological, human, sociological and cultural dimensions. Furthermore, effective information security is one that is aligned with organisation business objectives and requirements and is continually improved to remain relevant. An effective information security today will be useless in a few months if it is not continually improved to account for changes in organisations' objectives, requirements and information security threat environment, due to the rapid changes in technologies organisations utilise. Consequently, the testing of hypothesis H2 requires testing how implementing ISO 27001 impacted the above characteristics of Tonga organisations' information security. Specifically, testing hypotheses H2a to H2d.

First, hypothesis H2a indicate a positive relationship between implementing ISO 27001 and Tonga organisations ability to effectively address different dimensions and critical success factors (CSF) of information security. The analysis in 5.2.1 confirmed such a positive relationship based on the outcomes of the gap analysis in section 5.1.1 to 5.1.7, which were summarised in section 5.1.8.

Second, hypothesis H2b indicates a positive relationship between implementing ISO 27001 and Tonga organisations minimising information security risks to their information assets. The analysis in 5.2.2 affirmed the assertion based on the significant positive influence of implementing ISO 27001 on Tonga organisation risk management practices according to analysis in 5.1.5. Moreover, according to the analysis in section 5.2.1, implementing ISO 27001 allows Tonga organisations to address all dimensions and CSF of information security.

Third, hypothesis H2c indicates a positive relationship between implementing ISO 27001 and Tonga organisations being able to continually improve their information security. Continuous improvement is critical to the long term effectiveness of organisation information security. The analysis in 5.2.3 supports a positive relationship between implementing ISO 27001 and an organisation's ability to continuously improve their information security.

The last hypothesis H2d indicates a positive relationship between implementing ISO 27001 and Tonga organisations being able to better align their information security with their business and information security objectives requirements. Aligning information security and business objectives and requirements is critical for the long term viability of organisations' information security. Information security on its own is meaningless (less likely to attract support from top management) unless it helps organisations achieve their business goals. Analysis in 5.2.4 confirmed a significant positive relationship between implementing ISO 27001 and organisations' ability to align their information security and business objectives and requirements.

Finally, hypothesis H2 indicates a positive relationship between implementing ISO 27001 and Tonga organisations' ability to implement effective information security. The study confirms the positive impacts of implementing ISO 27001 on the effectiveness of Tonga organisation information security based on the outcomes of testing of hypotheses H2a to H2d above and the analysis in section 5.2.5.

6.1.1.3 SUMMARY DISCUSSION

Question two asked, "What are the impacts of implementing ISO 27001 on Tonga organisations information security management and information security?" Section 6.1.1 discusses how implementing ISO 27001 will impact the effectiveness of Tonga organisations' information security management (ISM), and 6.1.2 discusses how implementing ISO 27001 will impact the effectiveness of Tonga organisations' information security.

The discussions in 6.1.1.1 and 6.1.1.2, of this study can conclusively answer question two. Which is, implementing ISO 27001 will have a significant positive impact on Tonga organisations' ability to effectively manage their information security and the effectiveness of their information security. Specifically and more importantly, implementing ISO 27001 will motivate, influence, and improve top management involvement in Tonga organisation information security.

Top management will, in turn, allocate needed resources, setup information security governance structures, and authorise and oversee the establishment of an ISMS. Developing an information security management (ISMS) will help Tonga organisations to develop and enforce comprehensive information security policies and develop information security awareness programs which in turn help them to develop positive information security cultures. Moreover, developing an ISMS allows organisations to develop holistic risk management processes to effectively manage information risks to their information assets and processes.

Finally, developing an ISMS allows organisations to continually improve their information security to ensure it is aligned with their business goals and account for rapid changes in organisations' information security threat environments. In other words, developing an effective ISMS allows Tonga organisations to establish, manage and maintain effective information security.

6.1.2 RESEARCH QUESTION ONE

The main research question of this study is "Is the holistic approach provided by ISO 27001 the best approach for Tonga organisations, given their unique organisational factors and threat environment, to establish effective information security?" As discussed in chapter 3, while the researcher cannot test and answer the question directly, it is possible to answer indirectly by answering a second question.

Firstly, according to the findings in chapter 4 and analysis in chapter 5, Tonga organisations are technologically based, lacked documented processes and lack full information security governance structures, therefore, they are using ad-hoc approaches for their information security. Consequently, comparing Tonga organisation information security to ISO 27001 requirements is comparing ad-hoc approaches to holistic approaches. Therefore answering question two in section 6.1.1 is answering which approach is better.

On that basis, this study is ready to answer the main research question. Given Tonga's unique organisational factors and information security threat environment, implementing ISO 27001 is the best approach for Tonga organisations to establish an effective ISM to effectively protect their information assets. While lack of resources could be a hindrance, however, as discussed in 5.3, Tonga organisations do have the resources to help them successfully implement an ISO 27001 based ISMS.

6.2 Research Limitations

In addition to constraints in chapter 3, section 3.5, one major constraint the study encounter is a lack of information security studies on Tonga organisations information security or smaller countries in the pacific with comparable organisation environments. For instance, while reviewing information security studies for Tonga organisations, the researcher found one paper on information security and one book on Telecommunications.

The biggest constraint on generalising the results of this study are the obstacles placed by COVID-19 travel and contact restrictions. The result was that the researcher had to use other people to talk with the experts in Tonga in a culturally appropriate way. The sample was to be representative of the biggest organisations in Tonga and not an opportunity sample. Again the COVID-19 restrictions placed barriers from getting all the organisations to participate. However, the participants represented a significant number of the biggest and most influential organisations. As a consequence claims can be made from the results but all have to be open to discussion and further moderation by those who did not participate.

The final constraint the study encountered was the lack of formal studies on professional certifications. The researcher noted during the literature review phase that 1. Papers on professional certifications, the majority, are from a decade ago. 2. Lack of studies on professional certifications and their effectiveness in producing industry-ready information security professionals. 3. Many papers comparing different professional certifications focuses on their attractiveness to employers rather on the contents.

While the constraints above are not serious enough to affect the outcome of the study, they do provide areas for future studies.

6.3 SUMMARY OF DISCUSSION

This chapter discussed the findings in chapter 4 and gap analysis of chapter 5. The findings and analysis were mapped and used to test assertions raised by hypotheses developed in chapter 3. Testing and accepting or denying hypotheses' assertions provides an overall view of the impacts of implementing ISO 27001 on Tonga organisation information security.

The discussions identified a significant positive relationship between implementing ISO 27001 and Tonga organisations being able to effectively address different dimensions and critical success factors of information security. Consequently, a significant positive relationship between implementing ISO 27001 and the ability of Tonga organisations to effectively manage their information security and establish efficacious information security, is established.

Finally, the chapter includes a brief discussion of limitations that could affect the ability to generalise from this study.

CHAPTER 7

CONCLUSION

7.0 INTRODUCTION

This chapter provides a summary of the study in 7.1, recommendations on how organisations can improve their information security in 7.2, and recommendations for further studies in 7.3. Finally, section 7.4 provides a brief, conclusive summary of the study.

7.1 SUMMARY OF THE STUDY

This study contributes to research knowledge by providing an overview of existing information security studies findings on information security standards. Furthermore, it provides an overview of what information security looks like in organisations in small countries like Tonga. Finally, it provides an example of how one can utilise both quantitative and qualitative analysis to do a gap analysis of organisations information security against ISO 27001 requirements, which is a departure from the usual maturity models-based studies.

The literature review in chapter 2 focuses on examining: 1.What is information security? 2. Why they are relevant? 3. Who is responsible for developing and maintain information standards? Moreover, chapter 2 discusses information security associations and their role in helping organisations to develop effective information security management (ISM) and why and how organisations assess an ISM. Finally, reviewed information on specific standards and frameworks like ISO 27001, COBIT, PCI-DSS, and ITIL, is completed. The review should give readers a broader understanding of information security and roles of information security standards, frameworks and models. Finally, readers will gain an appreciation of differences and similarities between information security, Information Technology (IT) governance and IT service management.

In chapter 3, the focus was to develop a research design and model based on the studies reviewed in chapter 2. The research model guides the development of the study's research questions and hypotheses. In turn, the research questions and hypotheses determined the type of research data needed and relevant research methods. The chapter also discusses the study aim to collect and analyse the data and constraints which may have an impact on the quality and quantity of data collected.

Chapter 4 focuses on presenting the findings regarding Tonga organisations' information security, which based on data collected, as discussed in chapter 3 as well as secondary data. In chapter 5 a gap analysis of the findings in chapter 4 against ISO 27001 requirements is completed. The gap analysis identifies gaps between Tonga organisations' current information security and organisations with an ISO 27001 based information security.

Finally in Chapter 6 the hypotheses are examined based on the findings in chapter 4 and the gap analysis in chapter 5 to determine whether to reject or accept the hypotheses assertions. Moreover, chapter 6 includes a brief discussion of constraints which may affect the outcomes of the study to allow readers to review the findings discussed in the light of stated limitations. In 6.3, the discussions proposed a significant positive relationship between implementing ISO 27001 and the effective for Tonga organisations' ISM and subsequently, information security.

7.2 Recommendation

Organisations' Information security is more critical today than ever due to the often devastating consequences of information security breaches. Based on this study findings, and findings of studies reviewed in chapter 2, this study compiles a list of recommendations summarise in table 7.1.

Table 7.1: Recommendations

Recommendations
Pacific organisations requested that training provided by APNIC and PACNOG include information security management training since they are the primary source of Information and Communication Technology (ICT) training for many organisations in the Pacific.
Tonga organisations still relying on purely technological solutions for their information security should implement ISO 27001. It is the best way to stay ahead of information security threats.

Information security awareness and management involvement in information security or lack thereof have significant impacts on organisations' information security.
Establishing an information security policy is an essential first step toward implementing effective ISM.
Organisations can be sure of the security of their information assets by employing holistic approaches to addresses all dimensions and critical success factors (CSF) of information security
Organisations must address human and sociological dimensions of information security in order to minimise risks to their information assets.
A comprehensive risks management program make significant differences in organisations information security.
Information security governance, distinct from IT and information security management, is a vital part of effective ISM
Rapid changing in technologies means organisations information threats environment are getting complicated and unpredictable. Therefore, organisations' information security needs to keep up (continually improve) to remain relevant and effective.
Small and Medium Enterprises (SMEs) can implement ISO 27001 successfully, can just start from where they are and according to the resources they have and build up their ISM slowly overtime. They do not have to wait around to have enough resources to implement one huge project.
Organisations should adopt the mind-set that information security is not a destination but a continuous, never-ending journey.

7.3 Further Research

Based on limitations discussed in 6.2, this study proposed further research areas which can not only contribute to Tonga organisations information security but to the general knowledge of information security.

An area of study that will be valuable for organisations in Tonga and information security, in general, is a detailed case study of implementing ISO 27001 on several organisations in Tonga. As indicated by the findings of this study, organisations are willing to implement information security standards, and were willing to participate in this study.

A case study would not only help them to implement the standard but provide researchers opportunities to study implementing ISO 27001. It would provide insights into influential organisational factors that may affect implementing effective ISM, unique to Tonga organisations. Not only that, but researchers get a chance to study how organisations can effectively address those factors to ensure successful implementation of ISO 27001.

The final possible area for further study is the effectiveness of professional certification in developing and validating information security professionals' skills and expertise. According to reports and studies found during the literature review, certification programs are mostly compared based on the employability of their certified members.

Unfortunately, organisations' hiring practices are not a good indication of certifications quality and effectiveness. A study in this area allows researchers to answer questions like how effective are certification programs in producing industry-ready information security professionals? Are certification programs are the best and quickest way to develop industry-ready information security professionals? Answering the questions above are crucial to finding effective ways to address the shortage of security skills for professionals.

7.4 SUMMARY

The objectives of this study are to: 1. Study the current state of information security in key organisations in Tonga. 2. Study the impacts of Implementing ISO 27001 to determine if it is the best approach for Tonga organisations to protect their information assets.

The findings in chapter 4 illustrated the need for Tonga organisations to improve their information security. Not only it is ready for change but it also lacks several key activities of information security. For instance, it requires internal auditing, risk management, incident response, and forensic capability. The gap analysis between Tonga organisations' information security and ISO 27001 requirements in chapter 5 highlights the significant impacts of implementing ISO 27001 on Tonga organisations' information security due to gaps and security provisions significantly lacking in many critical areas of information security.

The discussion of the findings in 6.1 documented the significant improvement for Tonga organisations ISM and information security if they implement ISO 27001. Therefore, this study confirmed a positive relationship between implementing ISO 27001 and Tonga organisations' ability to effectively manage their information security, thereby establishing information security to protect their information assets and processes.

In conclusion, this study achieved its objectives by studying Tonga organisations' information security and analysing the gaps between it and ISO 27001 requirements. In doing so, it was able to compare two information security approaches, ad-hoc and holistic. By comparing the strength and weaknesses of both approaches, the study was able to confirm that implementing ISO 27001 is the best approach for Tonga organisations to improve the management and effectiveness of their information security.

References

'Ofa, S. V. (2008). *The telecommunications sector in the Pacific: a regulatory policy survey*.

'Ofa, S. V. (2011). *Telecommunications Regulatory Reform in Small Island Developing States*.

Abu Talib, M., El Barachi, M., Khelifi ALHOSN, A., Dhabi, A., & akhelifi, U. (2012). Guide to ISO 27001: UAE Case Study. In *Issues in Informing Science and Information Technology* (Vol. 7).

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 149–157. https://doi.org/10.1109/IWBIS.2018.8471700

AGUTTER, C. (2019). Service Relationships. *ITIL® Foundation Essentials – ITIL 4 Edition*, *May 2020*, 20–24. https://doi.org/10.2307/j.ctvckq658.8

Ahmad, R., Sahib, S., & Nor'Azuwa, M. P. (2014). *Effective Measurement Requirements for Network Security Management*.

Al-Ahmad, W., & Mohammad, B. (2013). Addressing Information Security Risks by Adopting Standards. *International Journal of Information Security Science*, *2*(2), 28–43.

Al-mayahi, I., & Mansoor, S. P. (2012). ISO 27001 Gap Analysis - Case Study. *Proceedings of the International Conference on Security and Management (SAM)*, 1–5.

Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019). Cybersecurity Risks and Controls. *CPA Journal*, *89*(6), 36–41.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security*, *28*(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003

Alencar Rigon, E., Merkle Westphall, C., Ricardo dos Santos, D., & Becker Westphall, C. (2014). A cyclical evaluation model of information security maturity. *Information Management & Computer Security*, *22*(3), 265–278. https://doi.org/10.1108/IMCS-04-2013-0025

Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. *2015 12th International Conference on Information Technology - New Generations*, 731–735. https://doi.org/10.1109/ITNG.2015.124

Alshitri, K. I., & Abanumy, A. N. (2014). Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. *2014 International Conference on Information Science & Applications (ICISA)*, 1–4. https://doi.org/10.1109/ICISA.2014.6847396

Anttila, J., & Jussila, K. (2017). Challenges for the Comprehensive and Integrated Information Security Management. *2017 13th International Conference on Computational Intelligence and Security (CIS)*, 586–589. https://doi.org/10.1109/CIS.2017.00136

APNIC. (n.d.). *APNIC Academy / Catalog*. Retrieved August 28, 2020, from https://academy.apnic.net/en/catalog/

Arbanas, K., & Žajdela Hrustek, N. (2019). Key Success Factors of Information Systems Security. *Journal of Information and Organizational Sciences*, *43*(2), 131–144. https://doi.org/10.31341/jios.43.2.1

Assante, M. J., Tobey, D. H., & Board, N. (2011). *Enhancing the Cybersecurity Workforce*. *February*.

Atzeni, A., & Lioy, A. (2006). Why to adopt a security metric? A brief survey. *Advances in Information Security*, *23*, 1–12. https://doi.org/10.1007/978-0-387-36584-8_1

AXELOS Limited. (2019). *ITIL Foundation: ITIL 4 Edition*. The Stationery Office Ltd.

Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. *The Open Medical Informatics Journal*, *11*(1), 37–43. https://doi.org/10.2174/1874431101711010037

Bachlechner, D., Maier, R., Innerhofer-Oberperfler, F., & Demetz, L. (2011). Understanding the management of information security controls in practice. *Proceedings of the 9th Australian Information Security Management Conference*, 40–48. https://doi.org/10.4225/75/57b52b64cd8b6

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Metric-driven information security risk assessment and decision making. *Communications of the ACM*, *50*(10), 101–106.

Beveridge, R. (2019). Effectiveness of Increasing Realism Into Cybersecurity Training. *International Journal of Cyber Research and Education*, *2*(1), 40–54. https://doi.org/10.4018/ijcre.2020010104

Bhardwaj, A., & Kumar, V. (2011). Cloud security assessment and identity management. *14th International Conference on Computer and Information Technology, ICCIT 2011*, *Iccit*, 387–392. https://doi.org/10.1109/ICCITechn.2011.6164819

Bishop, M., & Frincke, D. (2004). Academic degrees and professional certification. *IEEE Security and Privacy*, *2*(6), 56–58. https://doi.org/10.1109/MSP.2004.91

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *Proceedings of the 2001 Workshop on New Security Paradigms - NSPW '01*, 97. https://doi.org/10.1145/508171.508187

Bon, J. van. (2019). *ITIL® 4 - a Pocket Guide*. Van Haren Publishing.

Boyle, R. J., & Panko, R. R. (2015). *Corporate computer security.* (Fourth edi). Pearson.

Braga, G. (2020). COBIT 2019 and the IIA 2019 Guiding Principles of Corporate Governance: Two Frameworks, Many Similarities. *COBIT Focus*, 1–4.

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31. https://doi.org/https://doi.org/10.1016/j.istr.2005.12.001

BSI. (2011). *BS ISO/IEC 27005:2011- Information technology — Security techniques — Information security risk management*.

BSI. (2013). *BS ISO/IEC 27014:2013 - Information technology — Security techniques — Governance of information security*.

BSI. (2014). *PD ISO/IEC TR 27016:2014 Information technology — Security techniques — Information security management — Organizational economics*.

BSI. (2015a). *BS ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*.

BSI. (2015b). *BS ISO/IEC 27010:2015 -Information technology — Security techniques — information security management for inter-sector and inter-organizational communications*.

BSI. (2015c). *BS ISO/IEC 27013:2015 - Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*.

BSI. (2015d). *BS ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

BSI. (2016a). *BS ISO/IEC 27004:2016 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation (ISO/EC 27004:2016)*.

BSI. (2016b). *BS ISO/IEC 27009:2016 - Information technology — Security techniques — Sector- specific application of ISO/IEC 27001 — Requirements*.

BSI. (2016c). *BS ISO/IEC 27011:2016 - Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations. September*.

BSI. (2017a). *BS EN ISO/IEC 27001:2017 - Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)*.

BSI. (2017b). *BS EN ISO/IEC 27002:2017 - Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 27002:2013)*.

BSI. (2017c). *BS ISO/IEC/IEEE 15939:2017 - Systems and software engineering — System life cycle processes*.

BSI. (2017d). *BS ISO/IEC 27003:2017 - Information technology - Security techniques - Information security management systems - Guidance (ISO/IEC 27003:2017)*.

BSI. (2017e). *BS ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals*.

BSI. (2019a). *BS ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.

BSI. (2019b). *PD ISO/IEC TS 27008:2019 - Information technology — Security techniques — Guidelines for the assessment of information security controls*.

BSI. (2020a). *BS EN ISO/IEC 27000:2020 - Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018) Technologies*.

BSI. (2020b). *BS ISO/IEC 27007:2020 - Information security , cybersecurity and privacy protection — Guidelines for information security management systems auditing*.

BSI. (2020c). *BS ISO/IEC 27019:2020 Information technology — Security techniques — Information security controls for the energy utility industry*.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Information Security Technical Report*, *17*(1–2), 19–25. https://doi.org/10.1016/j.istr.2011.12.002

Calder, A. (2019). PRINCIPLES AND MODEL FOR GOOD GOVERNANCE OF IT. In *ISO / IEC 38500 : A pocket guide , second edition Book*.

Calder, A., & Williams, G. (2019). *PCI DSS: A pocket guide, sixth edition* (6th ed.). IT Governance Publishing.

Campbell, T. (2016). *Practical information security management : a complete guide to planning and implementation.* Apress.

Candiwan, Beninda, M. Y. D., & Priyadi, Y. (2016). Analysis of Information Security Audit Using at IT Division-X Company, In Bandung, Indonesia Information Security Management Framework for Higher Education Institutions View project. *International Journal of Basic and Applied Science*, *04*(04), 77–88. https://doi.org/10.13140/RG.2.1.1483.3044

Candra, J. W., Briliyant, O. C., & Tamba, S. R. (2017). ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study : XYZ institute). *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, *2018-Janua*, 1–6. https://doi.org/10.1109/TSSA.2017.8272916

Carter, N., Bryant-Lukosius, D., Dicenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. In *Oncology Nursing Forum* (Vol. 41, Issue 5, pp. 545–547). Oncology Nursing Society. https://doi.org/10.1188/14.ONF.545-547

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, *2019-June*(June), 1–6. https://doi.org/10.23919/CISTI.2019.8760870

Cater-Steel, A., Tan, W.-G., & Toleman, M. (2009). Using Institutionalism as a Lens to Examine ITIL Adoption and Diffusion. *ACIS 2009 Proceedings*.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

Chen, G., Lai, T. H., Zhang, Y., Teodorescu, R., & Lin, Z. (2019). *Exploitable Hardware Features and Vulnerabilities Enhanced Side-Channel Attacks on Intel SGX and Their Countermeasures*.

Choejey, P., Murray, D., & Che Fung, C. (2016). Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations. *Computer Science & Information Technology (CS & IT)*, 49–61. https://doi.org/10.5121/csit.2016.61505

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752–767. https://doi.org/10.1177/0165551517748288

Cisco. (2019). *Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*.

Cisco. (2020). *Cisco Cybersecurity Report Series 2020: CISO Benchmark Study*.

CMMI Institute. (2018). *CMMI Adoption and Transition Guidance V2.0*.

Coburn, A. (2010). Fitting PCI DSS within a wider governance framework. *Computer Fraud and Security*, *2010*(9), 11–13. https://doi.org/10.1016/S1361-3723(10)70121-4

Comments on Standards in Information Security, Disaster Recovery, Business Continuity and Business Resilience. (2007). In *Critical Information Infrastructures* (pp. 94–144). Springer US. https://doi.org/10.1007/978-0-387-71862-0_7

CSA. (n.d.-a). *About | Cloud Security Alliance*. Retrieved September 30, 2020, from https://cloudsecurityalliance.org/about/

CSA. (n.d.-b). *CCSK | Cloud Security Alliance*. Retrieved April 26, 2020, from https://cloudsecurityalliance.org/education/

CSA. (n.d.-c). *Cloud Security Alliance History*. Retrieved September 30, 2020, from https://cloudsecurityalliance.org/about/history/

CSA. (n.d.-d). *CSA Security Guidance | Cloud Security Alliance*. Retrieved September 7, 2020, from https://cloudsecurityalliance.org/research/guidance/

CSA. (n.d.-e). *Education | Cloud Security Alliance*. Retrieved September 30, 2020, from https://cloudsecurityalliance.org/education/

CSA. (2017). *Cloud Security Alliance Announces Major | Cloud Security Alliance*. https://cloudsecurityalliance.org/press-releases/2017/07/26/security-guidance-v4/

CSA. (2019a). *Cloud Security Alliance Announces Industry's | Cloud Security Alliance*. https://cloudsecurityalliance.org/press-releases/2019/12/04/cloud-security-alliance-announces-industry-s-first-credential-for-cloud-auditing/

CSA. (2019b). *CSA STAR Level and Scheme Requirements*.

CSA. (2019c, August 3). *Cloud Controls Matrix v3.0.1 | Cloud Security Alliance*. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/

CSA. (2020). *Consensus Assessment Initiative | Cloud Security Alliance*. https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/

Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing Industry 4.0 Cybersecurity Challenges. *IEEE Engineering Management Review*, *47*(3), 79–86. https://doi.org/10.1109/EMR.2019.2927559

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. In *Computers and Security* (Vol. 29, Issue 2, pp. 196–207). https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., Eloff, J. H. P. P., Veiga, A. Da, Eloff, J. H. P. P., Da Veiga, A., Eloff, J. H. P. P., Veiga, A. Da, & Eloff, J. H. P. P. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011). Security Issues in Cloud Computing. *International Journal of Cloud Applications and Computing*, *1*(3), 1–11. https://doi.org/10.4018/ijcac.2011070101

Dalton, J. (2019). Goal, Question, Metric (GQM). In *Great Big Agile* (pp. 177–179). Apress. https://doi.org/10.1007/978-1-4842-4206-3_33

Davis, A. (2019). *The Role of Cybersecurity Certifications* (pp. 222–248). https://doi.org/10.4018/978-1-5225-7847-5.ch012

De Haes, S., & Grembergen, W. Van. (2004). *IT Governance and Its Mechanisms*.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Dooey, P., & Oliver, R. (2002). An investigation into the predictive validity of the IELTS Test as an indicator of future academic success. *Prospect*, *17*(1).

Dutta, A., Chao Alex Peng, G. U. O., & Choudhary, A. (2013). Risks in enterprise cloud computing: The perspective of it experts. *Journal of Computer Information Systems*, *53*(4), 39–48. https://doi.org/10.1080/08874417.2013.11645649

Eloff, J., & Eloff, M. (2003a). *Information Security Management-A New Paradigm*.

Eloff, J., & Eloff, M. (2003b). Information Security Management: A New Paradigm. *Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology*, 130–136.

ENISA. (2019). *Industry 4.0 Cybersecurity Challenges & Recommendations*.

Eppler, M. J. (2006). A comparison between concept maps, mind maps, conceptual diagrams, and visual metaphors as complementary tools for knowledge construction and sharing. *Information Visualization*, *5*, 202–210. https://doi.org/10.1057/palgrave.ivs.9500131

Eroğlu, Ş., & Çakmak, T. (2016). Enterprise Information Systems within the Context of Information Security: A Risk Assessment for a Health Organization in Turkey. *Procedia Computer Science*, *100*, 979–986. https://doi.org/10.1016/j.procs.2016.09.262

Esser, F., & Vliegenthart, R. (2017). Comparative Research Methods. In *The International Encyclopedia of Communication Research Methods* (pp. 1–22). Wiley. https://doi.org/10.1002/9781118901731.iecrm0035

Fajar, A. N., Christian, H., & Girsang, A. S. (2018). Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. *Journal of Physics: Conference Series*, *1090*(1), 012060. https://doi.org/10.1088/1742-6596/1090/1/012060

Fal', A. M. (2010). Standardization in information security management. *Cybernetics and Systems Analysis*, *46*(3), 512–515. https://doi.org/10.1007/s10559-010-9227-9

Fathoni, Simbolon, N., & Yunika Hardiyanti, D. (2019). Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001: 2013. *Journal of Physics: Conference Series*, *1196*(1), 012033. https://doi.org/10.1088/1742-6596/1196/1/012033

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/https://doi.org/10.1016/S2212-5671(15)01106-5

Ferreira, L. N., da Silva Constante, S. M., de Moraes Zebral, A. M., Braga, R. Z., Alvarenga, H., & Ferreira, S. N. (2013). ISO 27001 certification process of Electronic Invoice in the State of Minas Gerais. *2013 47th International Carnahan Conference on Security Technology (ICCST)*, 1–4. https://doi.org/10.1109/CCST.2013.6922072

Finau, G., Samuwai, J., & Prasad, A. (2013). *CYBERCRIME AND ITS IMPLICATIONS TO THE PACIFIC*.

Freeman, E. H. (2007). Holistic information security: ISO 27001 and due care. *Information Systems Security*, *16*(5), 291–294. https://doi.org/10.1080/10658980701746478

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, *2017*(2), 5–10. https://doi.org/10.1016/S1361-3723(17)30013-1

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16–30. https://doi.org/10.1016/j.cose.2004.11.002

GIAC Certifications. (n.d.). *Cybersecurity Certifications Overview | GIAC*. Retrieved August 24, 2020, from https://www.giac.org/certifications

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, *23*(4), 367–376. https://doi.org/10.1108/17542731111139455

Gonçalves, A., Correia, A., Matos, R., & Fragoso, B. (2016). A framework to assess information security quality of service based on a communicative action way of thinking. *Advances in Intelligent Systems and Computing*, *444*, 379–388. https://doi.org/10.1007/978-3-319-31232-3_36

Gregory, A., & Binning, E. (2005). *Satellite link to Pacific Islands still down - NZ Herald*. https://www.nzherald.co.nz/telecommunications/news/article.cfm?c_id=93&objectid=10007155

Gregory, P. H., & Miller, L. C. (2018). *CISSP for dummies*.

Gupta, H., Mondal, S., Majumdar, R., Ghosh, N. S., Suvra Khan, S., Kwanyu, N. E., & Mishra, V. P. (2019). Impact of Side Channel Attack in Information Security. *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 291–295. https://doi.org/10.1109/ICCIKE47802.2019.9004435

Hajdarevic, K., Allen, P., & Spremic, M. (2016). Proactive security metrics for Bring Your Own Device (BYOD) in ISO 27001 supported environments. *2016 24th Telecommunications Forum (TELFOR)*, 1–4. https://doi.org/10.1109/TELFOR.2016.7818717

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications*, *33*, 55–65. https://doi.org/10.1016/j.jisa.2017.01.007

Hamidovic, H. (2010). Fundamentals of IT Governance Based on ISO/IEC 38500. *ISACA Journal*, *5*(May), 1–4.

Harisaiprasad, K. (2020). *COBIT 2019 and COBIT 5 Comparison*.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27–47. https://doi.org/10.12821/ijispm040402

Heires, M. (2008). The International Organization for Standardization (ISO). *New Political Economy*, *13*(3), 357–367. https://doi.org/10.1080/13563460802302693

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. *Information Systems Management*, *27*(1), 72–81. https://doi.org/10.1080/10580530903455247

Herrera, S. O. S. (2005). Information security management metrics development. *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology*, 51–56. https://doi.org/10.1109/CCST.2005.1594818

Hohan, A. I., Olaru, M., & Pirnea, I. C. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, *32*, 352–359. https://doi.org/https://doi.org/10.1016/S2212-5671(15)01404-5

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, *2016-March*, 4842–4848. https://doi.org/10.1109/HICSS.2016.600

Hui-Lin, H., Kuei, M. W., & Kuei-, M. W. (2014). The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability. *African Journal of Business Management*, *8*(17), 705–716. https://doi.org/10.5897/ajbm2014.7443

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. https://doi.org/https://doi.org/10.1016/j.istr.2008.10.010

Humphreys, E. (2011). Information security management system standards. *Datenschutz Und Datensicherheit - DuD*, *35*(1), 7–11. https://doi.org/10.1007/s11623-011-0004-3

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech House.

ISACA. (n.d.-a). *About ISACA | Global Business & Technology Community | ISACA*. Retrieved June 8, 2020, from https://www.isaca.org/why-isaca/about-us

ISACA. (n.d.-b). *CGEIT Certification | Certified in Governance of Enterprise IT | ISACA*. Retrieved September 30, 2020, from https://www.isaca.org/credentialing/cgeit

ISACA. (n.d.-c). *CISA, CISM, CGEIT, CRISC, & CSX-P Certifications | ISACA*. Retrieved June 13, 2020, from https://www.isaca.org/credentialing/certifications

ISACA. (n.d.-d). *CISM Certification | Certified Information Security Manager | ISACA*. Retrieved September 30, 2020, from https://www.isaca.org/credentialing/cism

ISACA. (n.d.-e). *CMMI Institute - Home*. Retrieved September 30, 2020, from https://www.cmmiinstitute.com/

ISACA. (n.d.-f). *COBIT | Control Objectives for Information Technologies | ISACA*. Retrieved August 17, 2020, from https://www.isaca.org/resources/cobit

ISACA. (n.d.-g). *CRISC Certification | Certified in Risk & Information Systems Control | ISACA*. Retrieved September 30, 2020, from https://www.isaca.org/credentialing/crisc

ISACA. (n.d.-h). *CSX-P | Cybersecurity Practitioner | ISACA*. Retrieved September

3, 2020, from https://www.isaca.org/credentialing/csx-p

ISACA. (n.d.-i). *Frameworks, Standards and Models*. Retrieved June 8, 2020, from https://www.isaca.org/resources/frameworks-standards-and-models

ISACA. (n.d.-j). *Frameworks, Standards and Models*. Retrieved September 30, 2020, from https://www.isaca.org/resources/frameworks-standards-and-models

ISACA. (n.d.-k). *IT Certification Programs | Information Technology Certifications | ISACA*. Retrieved June 8, 2020, from https://www.isaca.org/credentialing

ISACA. (n.d.-l). *The Business Model for Information Security*. Retrieved September 30, 2020, from https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1

ISACA. (n.d.-m). *What We Offer and Whom We Serve*. Retrieved September 30, 2020, from https://www.isaca.org/why-isaca/what-we-offer

ISC2. (n.d.-a). *(ISC)^2 CBK | Common Body of Knowledge*. Retrieved May 12, 2020, from https://www.isc2.org/Certifications/CBK

ISC2. (n.d.-b). *Cloud Security Certification | CCSP - Certified Cloud Security Professional | (ISC)^2*. Retrieved September 3, 2020, from https://www.isc2.org/Certifications/CCSP

ISC2. (n.d.-c). *Code of Ethics | Complaint Procedures | Committee Members*. Retrieved May 8, 2020, from https://www.isc2.org/Ethics

ISC2. (n.d.-d). *Continuing Education Courses | Professional Development Institute | (ISC)^2*. Retrieved May 8, 2020, from https://www.isc2.org/Development

ISC2. (n.d.-e). *Cybersecurity Certification| CISSP - Certified Information Systems Security Professional* . Retrieved September 30, 2020, from https://www.isc2.org/Certifications/CISSP

ISC2. (n.d.-f). *Cybersecurity Certification and Training | (ISC)^2*. Retrieved May 1, 2020, from https://www.isc2.org/About

ISC2. (n.d.-g). *Cybersecurity Research | (ISC)2*. Retrieved May 8, 2020, from https://www.isc2.org/Research

ISC2. (n.d.-h). *Healthcare Security Certification | HCISPP - HealthCare Information Security and Privacy Practitioner | (ISC)^2*. Retrieved September 30, 2020, from https://www.isc2.org/Certifications/HCISPP

ISC2. (n.d.-i). *IT Security Certification | SSCP - Systems Security Certified Practitioner | (ISC)^2*. Retrieved September 30, 2020, from https://www.isc2.org/Certifications/SSCP

ISC2. (n.d.-j). *NICE Cybersecurity Framework Map*. Retrieved June 13, 2020, from https://www.isc2.org/NICE-Cybersecurity-Framework-Map

ISC2. (2020). *The ultimate guide to the CISSP*.

ISO. (n.d.). *ISO - The ISO Story*. Retrieved April 20, 2020, from https://www.iso.org/the-iso-story.html

ISO. (2019). *ISO in brief*.

Jadhav, H. (2018). Tech Certified: IT Credentials for CPAs. *California CPA*, *87*(6), 24–25.

Johnson, G. (2014). *Measuring ISO 27001 ISMS processes*.

Jouini, M., & Ben Arfa Rabai, L. (2016). A Scalable Threats Classification Model in Information Systems. *Proceedings of the 9th International Conference on Security of Information and Networks - SIN '16*, *20-22-July*, 141–144. https://doi.org/10.1145/2947626.2947630

Jouini, M., & Rabai, B. A. (2018). *Threats Classification : State of the Art Mouna Jouini*.

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/https://doi.org/10.1016/j.procs.2014.05.452

Kaban, E., & Legowo, N. (2018). Audit information system risk management using ISO 27001 framework at private bank. *Journal of Theoretical and Applied Information Technology*, *96*(1), 90–99.

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Roning, J. (2006). Information Security Standards and Global Business. *2006 IEEE International Conference on Industrial Technology*, 2091–2095. https://doi.org/10.1109/ICIT.2006.372505

Kajava, J., & Savola, R. (2005). Towards better information security management by understanding security metrics and measuring processes. *Proceedings of the European University Information Systems (EUNIS)*, 16.

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, *15*, 47–59. https://doi.org/10.1016/j.ijcip.2016.10.001

Katos, V., Rostami, S., Bellonias, P., Davies, N., Kleszcz, A., Faily, S., Spyros, A., Papanikolaou, A., Ilioudis, C., & Rantos, K. (2019). *State of Vulnerabilities 2018/2019 - Analysis of Events in the life of Vulnerabilities — ENISA*. European Union Agency For Network and Information Security. https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities

Katsuno, Y., Kundu, A., Das, K. K., Takahashi, H., Schloss, R., Dey, P., & Mohania, M. (2016). Security, Compliance, and Agile Deployment of Personal Identifiable Information Solutions on a Public Cloud. *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)*, 359–366. https://doi.org/10.1109/CLOUD.2016.0055

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, *6*(14), 4982–4989. https://doi.org/10.5897/AJBM11.2323

Kelly, M., Furey, E., & Blue, J. (2019). GDPR Article 17: Eradicating Personal Identifiable Information &amp; Achieving Compliance in a Hybrid Cloud. *2019 30th Irish Signals and Systems Conference (ISSC)*, 1–6. https://doi.org/10.1109/ISSC.2019.8904966

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29–42. https://doi.org/10.1016/j.ijinfomgt.2003.12.001

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management’s effect on culture and policy. *Information Management and Computer Security*, *14*(1), 24–36. https://doi.org/10.1108/09685220610648355

Koziolek, H. (2008). Goal, question, metric. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *4909 LNCS*, 39–42. https://doi.org/10.1007/978-3-540-68947-8_6

Krag, B. W. (2009). *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*.

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1–

48. https://doi.org/10.1016/j.cosrev.2019.05.002

Kurnianto, A., Isnanto, R., & Puji Widodo, A. (2018). Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs. *E3S Web of Conferences*, *31*, 11013. https://doi.org/10.1051/e3sconf/20183111013

Kusumah, P., Sutikno, S., & Rosmansyah, Y. (2014). Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC). *2014 International Conference on ICT For Smart Society (ICISS)*, 1–6. https://doi.org/10.1109/ICTSS.2014.7013193

Kwok, L., & Longley, D. (1997). Code of Practice: A Standard for Information Security Management. *Information Security in Research and Business*, 78–90. https://doi.org/10.1007/978-0-387-35259-6_7

Lainhart, J. (2018). Introducing COBIT 2019: The Motivation for the Update? *COBIT Focus*, *October 2018*, 1–3.

Laulaupea'alu, S., & Keegan, T. T. (2019). *Cyber Security Vulnerabilities in Tonga*.

Lawrence, H. (2017). *An Introduction to the Business Model for Information Security*. https://silo.tips/download/an-introduction-to-the-business-model-for-information-security-4

Le, N. T., & Hoang, D. B. (2016). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, 1–7. https://doi.org/10.1109/PCCC.2016.7820663

Lehtinen, R., & Gangemi Sr, G. T. (2006). *Computer Security Basics: Computer Security*.

Li, J., Huo, M., & Chao, S. (2015). A Study of Information Security Evaluation and Risk Assessment. *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, 1909–1912. https://doi.org/10.1109/IMCCC.2015.405

Lidster, W. W., & Rahman, S. S. M. (2018). Obstacles to Implementation of Information Security Governance. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1826–1831. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00276

Livshitz, I. I., Nikiforova, K. A., Lontsikh, P. A., & Karasev, S. N. (2016). The new aspects for the instantaneous information security audit. *2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS)*, 125–127. https://doi.org/10.1109/ITMQIS.2016.7751920

Lovrić, Z. (2012). Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard. *Ceciis.Foi.Hr*, 347–351.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A systematic literature review: Information security culture. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6. https://doi.org/10.1109/ICRIIS.2017.8002442

Martins, A., & Elofe, J. (2002). *Information Security Culture* (pp. 203–214). Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35586-3_16

Mataracioglu, T., & Ozkan, S. (2011). GOVERNING INFORMATION SECURITY IN CONJUNCTION WITH COBIT AND ISO 27001. *International Journal of Network Security & Its Applications (IJNSA)*, *3*(4). https://doi.org/10.5121/ijnsa.2011.3410

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law and Security Report*, *24*(6), 540–554. https://doi.org/10.1016/j.clsr.2008.07.001

Mousavi, M. Z., & Kumar, S. (2019). Analysis of key Factors for Organization Information Security. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 514–518. https://doi.org/10.1109/COMITCon.2019.8862191

Nasser, A., & Nasser, A. A. (2017). Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen. *International Journal of Scientific Research in ______________________________ Research Paper. Multidisciplinary Studies E*, *3*(11), 4–13. https://doi.org/10.26438/ijsrms/v3i11.413

Northcutt, S. (2005). Global Information Assurance Certification: Securing Today and Tomorrow. *Certification Magazine*, *7*(10), 28–31.

Northcutt, S., & Frisk, J. (2007). SANS GIAC: Real-World Expertise Security Professionals. *Certification Magazine*, *9*(1), 28–40.

Oxford Learner's Dictionaries. (n.d.). *framework noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary*. Retrieved August 24, 2020, from https://www.oxfordlearnersdictionaries.com/definition/english/framework

Ozdemir, Y., Alcan, P., Basligil, H., & Kandemirli, B. M. (2014). EVALUATION AND COMPARISON OF COBIT, ITIL AND ISO27K1/2 STANDARDS WITHIN THE FRAMEWORK OF INFORMATION SECURITY. In *Article in International Journal of Technical Research and Applications* (Vol. 11).

Pacific Islands Report. (2000). *GOODBYE CABLE AND WIRELESS, HELLO TONGA LOCAL CONTROL | Pacific Islands Report*. http://www.pireport.org/articles/2000/08/29/goodbye-cable-and-wireless-hello-tonga-local-control

PacNOG. (n.d.). *PacNOG: The Pacific Network Operators Group*. Retrieved August 28, 2020, from https://www.pacnog.org/

Pan, L., & Tomlinson, A. (2016). A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering*, *6*(2), 270–281. https://doi.org/10.2495/SAFE-V6-N2-270-281

Papadaki, E., Polemi, D., & Damilos, D. K. (2008). A Holistic, Collaborative, Knowledge-Sharing Approach for Information Security Risk Management. *2008 The Third International Conference on Internet Monitoring and Protection*, 125–130. https://doi.org/10.1109/ICIMP.2008.19

Park, C.-S., Jang, S.-S., & Park, Y.-T. (2010). A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance. *IJCSNS International Journal of Computer Science and Network Security*, *10*(3), 10.

PCI SSC. (2008). *Payment Card Industry (PCI) Data Security Standard Validation Requirements For Qualified Security Assessors (QSA) Version 1.2*.

PCI SSC. (2017). *Payment Card Industry (PCI) Data Security Standard Qualification Requirements For Approved Scanning Vendors (ASV)*.

PCI SSC. (2018a). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2.1*.

PCI SSC. (2018b). PCI DSS Quick Reference Guide 3.2.1. *PCI Security Standard Documents*, 1–40.

Petri, P., Siponen, M., Puhakainen, Siponen, Petri, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757. https://doi.org/10.2307/25750704

Pike, J. (2008). GIAC: The Hands-On IT Security Certification. *Certification Magazine*, *10*(6), 24–39.

Pinheiro, F. S., & Ribeiro, W. (2005). Information Security. In *Database and Applications Security* (Vol. 3, Issue 3, p. 9). Auerbach Publications. https://doi.org/10.1201/9780203486061.ch3

Pompon, R., & Pompon, R. (2016). Internal Audit. In *IT Security Risk Control Management* (pp. 275–282). Apress. https://doi.org/10.1007/978-1-4842-2140-2_22

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646. https://doi.org/https://doi.org/10.1016/j.cose.2004.10.006

Prabhakar, T. V., & Varati, N. K. (2018). *Block-2 Introduction to ISO 27000*.

Price, R. K. (2002). *Information systems security enters the 1990s*. 870–872. https://doi.org/10.1109/milcom.1991.258388

Proença, D., & Borbinha, J. (2018). Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. In *Lecture Notes in Business Information Processing* (Vol. 320, pp. 102–114). Springer Verlag. https://doi.org/10.1007/978-3-319-93931-5_8

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*, *28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Rao, U. H., & Nayak, U. (2014). The InfoSec Handbook. In *The InfoSec Handbook: An Introduction to Information Security*. Apress. https://doi.org/10.1007/978-1-4302-6383-8

Rode, K. (2004). Security certification staples. *Network World*, *21*(38), 45.

Rudolph, C., Creese, S., & Sharma, S. (2020). *Cybersecurity in Pacific Island Nations*. https://doi.org/10.1145/3378550

Russell, D., & Gangemi Sr, G. T. (1991). *Computer Security Basics*.

SANS. (n.d.-a). *Cyber Security Certifications - GIAC Certifications*. Retrieved September 30, 2020, from https://www.giac.org/?msc=homepage&_ga=2.44283236.1351139907.1601432554-1414751354.1601432554

SANS. (n.d.-b). *Cyber Security Resources | SANS Institute*. Retrieved September 30, 2020, from https://www.sans.org/security-resources/

SANS. (n.d.-c). *List of GIAC Information and Cyber Security Certifications*. Retrieved June 9, 2020, from https://www.giac.org/certifications/categories

SANS. (n.d.-d). *Reading Room | SANS Institute*. Retrieved May 8, 2020, from https://www.sans.org/reading-room/

SANS. (n.d.-e). *SANS Institute: About*. Retrieved April 17, 2020, from https://www.sans.org/about/

SANS. (n.d.-f). *SANS Institute - CIS Critical Security Controls*. Retrieved May 8, 2020, from https://www.sans.org/critical-security-controls/

SANS. (2016). *CIS Critical Security Controls Effective Cybersecurity-Now*.

Schmid, M., & Pape, S. (2019). A Structured Comparison of the Corporate Information Security Maturity Level. In *IFIP Advances in Information and Communication Technology* (Vol. 562, pp. 223–237). Springer New York LLC. https://doi.org/10.1007/978-3-030-22312-0_16

Semisi, D., Prescott, M., & Hooper, K. (2015). Governance in small Pacific Businesses: Tongan Business Cases. In *undefined*.

Shojaie, B., Federrath, H., & Saberi, I. (2014). Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A. *2014 Ninth International Conference on Availability, Reliability and Security*, 259–264. https://doi.org/10.1109/ARES.2014.41

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, *27*(5), 644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Smith, R. F. (2005). Evaluating Security Certifications. *Security Administrator*, *5*(1), 13–16.

Smyth, S. J., Curran, K., & McKelvey, N. (2019). *The Role of Education and Awareness in Tackling Insider Threats* (pp. 33–52). https://doi.org/10.4018/978-1-5225-7847-5.ch003

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Spremić, M. (2013). Holistic approach for governing information system security. *World Congress on Engineering 2013 Vol II*.

Stamer, D., Zimmermann, O., & Sandkuhl, K. (2016). What Is a Framework? - A Systematic Literature Review in the Field of Information Systems. In *Lecture Notes in Business Information Processing* (Vol. 261, pp. 145–158). Springer Verlag. https://doi.org/10.1007/978-3-319-45321-7_11

Standards Australia. (2020). *Pacific Islands Cyber Security Standards Cooperation Agenda*.

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, *25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Stewart, J. M., Chapple, M., & Gibson, D. (2015). Personnel Security and Risk Management Concepts. In *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide*.

Stoll, M., & Breu, R. (2012). Information Security Governance and Standard Based Management Systems. In *Strategic and Practical Approaches for Information Security Governance* (pp. 261–282). IGI Global. https://doi.org/10.4018/978-1-4666-0197-0.ch015

Stringer, R. (2008). (ISC)2 rolls out two new courses for information security professionals. *Infosecurity*, *5*(7), 12–13. https://doi.org/https://doi.org/10.1016/S1754-4548(08)70119-0

Suby, M., & Dickson, F. (2015). The 2015 (ISC)^2 Global Information Security Workforce Study. *A Frost & Sullivan White Paper*, *2013*, 1–28.

Swanson, M., & Guttman, B. (1996). *NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems*.

Swinhoe, D. (2020). *The 15 biggest data breaches of the 21st century | CSO Online*. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Tashi, I., & Ghernaouti-Hélie, S. (2007). Security metrics to improve information security management. In *Proceedings of 6th Annual Security Conference*.

Taylor, R. G. (2015). Potential Problems with Information Security Risk Assessments. *Information Security Journal: A Global Perspective*, *24*(4–6), 177–184. https://doi.org/10.1080/19393555.2015.1092620

Tessin, P. (2016). *COBIT Celebrates 20 Years of Guidance*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/cobit-celebrates-20-years-of-guidance

Thomas, M. (2018). A New COBIT Is in Town and I Really Like How It Looks. *COBIT Focus*, *December 2018*, 1–8.

Thomas, T. M., & Stoddard, D. (2011). *Network Security First-Step: NETWORK SECURITY FIRST ST_p2*. Cisco Press.

Thompson, G. (2018). *CCSK vs CCSP: An Unbiased Comparison | Cloud Security Alliance*. https://cloudsecurityalliance.org/blog/2018/04/24/ccsk-vs-ccsp-unbiased-comparison/?_ga=2.17315454.693038262.1591935438-1835666565.1590567869

Tittel, E. (2006). Certification Top 10. *Certification Magazine*, *8*(11), 18–25.

Tofan, D. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/https://doi.org/10.1016/j.cose.2017.09.001

Tu, Z., Yuan, Y., Paper, R., Tu, Z., & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. In *20th Americas Conference on Information Systems, AMCIS 2014*.

van Niekerk, J. F., & von Solms, R. (2010). Research methodologies in information Security Research: The road ahead. *IFIP Advances in Information and Communication Technology*, *330*, 215–216. https://doi.org/10.1007/978-3-642-15257-3_19

Vasileiou, I., & Furnell, S. (2019). Cybersecurity Education for Awareness and Compliance. In I. Vasileiou & S. Furnell (Eds.), *Cybersecurity Education for Awareness and Compliance: Vol. i*. IGI Global. https://doi.org/10.4018/978-1-5225-7847-5

Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., & Moscoso-Zea, O. (2018).

Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. *2018 International Conference on Information Systems and Computer Science (INCISCOS)*, 294–300. https://doi.org/10.1109/INCISCOS.2018.00049

von Solms, B. (2001). Information Security — A Multidimensional Discipline. *Computers & Security*, *20*(6), 504–508. https://doi.org/https://doi.org/10.1016/S0167-4048(01)00608-3

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50–58. https://doi.org/10.1108/09685229910255223

von Solms, S. H. (Basie). (2005). Information Security Governance – Compliance management vs operational management. *Computers & Security*, *24*(6), 443–447. https://doi.org/10.1016/j.cose.2005.07.003

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. https://doi.org/https://doi.org/10.1016/j.cose.2004.01.012

Walker, D. H. T. (1997). Choosing an appropriate research methodology. *Construction Management and Economics*, *15*(2), 149–159. https://doi.org/10.1080/014461997000000003

Wang, A. J. A. (2005). Information security models and metrics. *Proceedings of the 43rd Annual Southeast Regional Conference on - ACM-SE 43*, *2*, 178. https://doi.org/10.1145/1167253.1167295

Wang, A. J. A., Xia, M., & Zhang, F. (2008). Metrics for Information Security Vulnerabilities. *Journal of Applied Global Research*, *1*(1), 48–58.

Wang, C., Guo, E., Chen, S., Zhu, S., & Wu, J. (2018). Appraisal of mask manufacture information security based on ISO27001 and common criteria. *IEEE International Conference on Industrial Engineering and Engineering Management*, *2017-Decem*, 2317–2320. https://doi.org/10.1109/IEEM.2017.8290305

Warsinske, J., Vasquez, M., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., Pajari, G., Parker, J. T., & Seidl, D. (2019). *The Official (ISC)2 Guide to the CISSP CBK Reference*. John Wiley & Sons, Incorporated.

Wei, Y.-C., Wu, W.-C., & Chu, Y.-C. (2018). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing*, *279*, 48–53. https://doi.org/10.1016/j.neucom.2017.05.106

Weill, P., & Ross, J. W. (2004). *IT governance : how top performers manage IT decision rights for superior results.* Harvard Business School Press.

Weldehawaryat, G. K., & Katt, B. (2018). Towards a Quantitative Approach for Security Assurance Metrics. In *The 12th International Conference on Emerging Security Information* (Issue September).

Westbrook, T. (2019). *Severed cable sends Tonga "back to beginning of the internet" - Reuters*. https://www.reuters.com/article/us-tonga-internet/severed-cable-sends-tonga-back-to-beginning-of-the-internet-idUSKCN1PI0A8

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/https://doi.org/10.1016/j.cose.2019.101640

Williams, C. (2011). Research Methods. *Journal of Business & Economics Research (JBER)*, *5*(3), 65. https://doi.org/10.19030/jber.v5i3.2532

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, *28*(3), 1846–1852. https://doi.org/10.1016/j.ifacol.2015.06.355

Wood, B. J., Saydjari, O. S., & Stavridou, V. (2000). *A proactive holistic approach to strategic cyber defense*.

World Bank. (2013). *High Speed Broadband Goes Live in Tonga*. https://www.worldbank.org/en/news/press-release/2013/08/21/high-speed-broadband-goes-live-in-tonga

World Bank. (2019). *Closing the digital divide in Tonga*. https://www.worldbank.org/en/results/2019/09/16/closing-the-digital-divide-in-tonga

Wright, S. (2006). *Measuring the Effectiveness of Security using ISO 27001*.

Wu, J. (2020). *Security Risks from Vulnerabilities and Backdoors* (pp. 3–38).

Springer, Cham. https://doi.org/10.1007/978-3-030-29844-9_1

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Yunis, R., Djoni, & Angela. (2019). A Proposed of IT Governance Model for Manage Suppliers and Operations Using COBIT 5 Framework. *2019 Fourth International Conference on Informatics and Computing (ICIC)*, 1–6. https://doi.org/10.1109/ICIC47613.2019.8985979

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. *International Journal on Advanced Science, Engineering and Information Technology*, *6*(6), 904–913. https://doi.org/10.18517/ijaseit.6.6.1371

Zeb, T., Yousaf, M., Afzal, H., & Mufti, M. R. (2018). A quantitative security metric model for security controls: Secure virtual machine migration protocol as target of assessment. *China Communications*, *15*(8), 126–140. https://doi.org/10.1109/CC.2018.8438279

APPENDIX A

ETHICS EXCEPTIOIN

EXCEPTIONS TO ACTIVITIES REQUIRING AUTEC APPROVAL

The following activities do not require AUTEC approval:

6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise.

- See more detail at:

http://www.aut.ac.nz/researchethics/guidelines-and-procedures/exceptions-to-activities-requiring-autec-approval-6