School of Information Systems

Information Security Risk Management (ISRM) Model for Saudi Arabian Organisations

Naser Mansour N Alshareef
0000-0001-7442-5376

This thesis is presented for the Degree of
Doctor of Philosophy
of
Curtin University

February 2022

Declaration

To the best of my knowledge and belief this thesis contains no material previously published by any other person except where due acknowledgment has been made.

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

The research presented and reported in this thesis was conducted in accordance with the National Health and Medical Research Council National Statement on Ethical Conduct in Human Research (2007) – updated March 2014. The proposed research study received human research ethics approval from the Curtin University Human Research Ethics Committee (EC00262), Approval Number # RDBS-19-16.

Signature:

Date: 25 January 2022

Acknowledgments

In the Name of Allah, the Most Beneficent, the Most Merciful

First of all, I thank Allah who continues to grace me with His uncountable blessings, for helping me to complete this long journey. Then, I would like to express my sincere gratitude to my parents, my wife, my children Sharaf and Ahmed, my siblings, and friends who helped me through my degree. Special thanks to my parents for their continued support and prayers. Thanks my beloved wife; without your encouragement, support, understanding, patience, caring and listening, writing this thesis would not have been possible.

I would like to take this opportunity to express my sincere gratitude to my supervisors, especially Dr. Paul Alexander, for his continuous and unfailing support during my years of work in the PhD program. Paul was always there to listen patiently and advise generously. He showed me the different ways in which I could approach and resolve research problems and taught me how to be persistent and dedicated in accomplishing my goals. He was always there beside me to discuss ideas, edit my work and ask the right questions to encourage me to think through my problems. I am very thankful for his support, cooperation, and for leading me to the right way in my PhD journey. Moreover, I would like to thank Dr. Sharyn Curran for her patience and support. She worked patiently with me throughout my journey. Finally, I would like to thank my external supervisor Dr. Mahmood Shah for his support and valuable guidance.

I would like to convey my deep thanks and gratitude to my peers and friends who provided helpful suggestions and comments on my thesis. Finally, my research colleagues in Unit 4 Technology Park have also provided me with an ongoing source of guidance and encouragement and have helped me maintain my passion for this venture.

Abstract

Information is the most valuable property of an organisation, and securing information is crucial in today's information age. Although no particular technology can completely eliminate information security risks, an information security risk management (ISRM) approach can mitigate information security risks and improve organisations' security position. Saudi Arabia faces difficulties in implementing Western technology and standards such as ISRM standards because its government regulations, management styles, culture, values, and mindset differ from those of Western countries.

This research aimed to investigate the factors influencing information security risk management and develop an ISRM model for large Saudi Arabian organisations. The study employed an exploratory research method following a top-down design approach. The research was conducted in two sequential phases: an interview and a focus group discussion. The first phase had two groups (A and B) to identify factors that influence, constitute, and reflect ISRM in large Saudi Arabian organisations. The second phase aimed to enhance and confirm the developed ISRM model for Saudi organisations.

In the first phase, 10 participants in Group A and 8 participants in Group B completed a semistructured interview with open-ended questions. They were drawn from different organisations in Saudi Arabia. Data in the second phase was collected through focus group discussion. The obtained data were analysed using the NVivo software package.

The research identified 14 factors grouped into the people, process, and technology that influence ISRM in large Saudi Arabian organisations. In addition, the research findings revealed that even though large Saudi Arabian organisations face many ISRM challenges, these challenges can be solved by the proposed ISRM model. The proposed model can successfully guide large Saudi Arabian organisations to implement ISRM standards more effectively.

This study makes both theoretical and practical contributions. The theoretical contribution lies in the conceptual ISRM model that combines factors that may influence ISRM effectiveness in the Saudi Arabian context. These factors were derived from academic

research and the participants from the data collection phases one and two. Regarding its practical contribution, the findings of this study can assist large Saudi Arabian organisations to efficiently manage the ISRM standards implementation, thereby securing a better information security posture.

Published work

1. Alshareef, Naser. *A Model for an Information Security Risk Management Framework for Saudi Arabian Organisations*: Paper presented at the International Conferences on Internet Technologies & Society (ITS), and Sustainability, Technology and Education (STE) (Melbourne, Australia, Dec 6-8, 2016).

2. Abu-Salih, Bilal, Bushra Bremie, Pornpit Wongthongtham, Kevin Duan, Tomayess Issa, Kit Yan Chan, Mohammad Alhabashneh, Teshreen Albtoush, Sulaiman Alqahtani, Abdullah Alqahtani, Muteeb Alahmari, Naser Alshareef. *Social credibility incorporating semantic analysis and machine learning: A survey of the state-of-the-art and future research directions.* In Workshops of the International Conference on Advanced Information Networking and Applications, pp. 887-896. Springer, Cham, 2019.

Table of Contents

Table of Figures

List of Tables

CHAPTER 1. INTRODUCTION

1.1 Background

As technology becomes more advanced and organisations continue to depend on information technology to manage their operations and business models have evolved to encompasses data analytics, block chain, cloud computing, and artificial intelligence, information becomes a more valuable asset. Moreover, the COVID-19 pandemic has had an enormous influence on the way many organisations conduct business with many employees working from home and increased demand for technology resources utilisation (*Cost of a Data Breach Report 2020* 2020). Consequently, the risk of exploiting organisations' critical information increases dramatically. Securing information is not a new practice where organisations continue to seek critical information protection from unauthorised access, data loss, modification, or misuse (Breier and Schindler 2014; Trajkovski and Antovski 2017a; Van Niekerk and Von Solms 2010). Information security is as crucial to organisations as it has ever been because technology applied to information creates a high level of risks. It has become an essential part of an organisation to improve consumers' trust and effectively use innovative technologies for the business process (Ashenden 2008; Yaokumah 2013).

Managing the information security risk is considered a crucial component of information security management which plays a vital role in the protection of an organisation's information assets (Alcántara and Melgar 2016; Raggad 2010). Information security risk management (ISRM) balances the operational and economic costs by protecting the entire IT infrastructure and data to support the organisation's missions (Raggad 2010). Indeed, managing the risk of organisations' technological assets alone (e.g., hardware, software, networking) at the expense of managing the risk of other sources of such as people, policies, processes, and culture is no longer valid (García-Porras, Huamani-Pastor, and Armas-Aguirre 2018; Okonofua, Rahman, and Ivanova 2019; Petrescu and Sîrbu 2019). Employees are considered one of greatest threats to an organisation's information assets because the majority of security incidents are caused by their actions, whether intentionally or unintentionally (Govender, Kritzinger, and Loock 2016). People understand risks differently,

depending on the cultural contexts and social structures to which they are exposed and their values (Tsohou, Karyda and Kokolakis 2015).

There is increasing concern that management theories and practices developed in Western countries are less effective when applied in Middle Eastern countries because of the difference of culture, values, and mindset (Al-Adaileh and Al-Atawi 2011; Aldraehim et al. 2012; Alnatheer and Nelson 2009; Maghrabi and Palvia 2012). Culture is a system of social behaviour built on how individuals interact with their surroundings (Alkahtani, Dawson and Lock 2013). It is the combination of ways of thinking, speaking, making traditions, assumptions, language, arts, literature, and feelings that define common norms and values between groups of people (Chu, Luo, and Chen 2018).

Moreover, studies have shown that Saudi Arabia faces many difficulties in implementing Western technology and standards because its government regulations and management styles differ from those of Western countries (Razi and Madani 2013). This is also applicable to the information security management in which most of the standards and best practices have been developed in Europe and the United States, such as ISO 27000 series and COBIT. Studies over the past two decades have provided important information about the influence of cultural values and norms on management practices such as Hofstede cultural dimensions; however, these theories have not been implemented on most management standards and best practices (Maghrabi and Palvia 2012).

In 2020, global spending on information security products and services surpassed $133 billion (Moore 2021). Forecasts indicate that the market will grow 10.1 percent per year, reaching $221 billion in spending by 2025 (Upadhyay et al. 2021). However, cybercriminals are becoming more sophisticated and coordinated in their attacks, leading to exponentially higher costs for the world. It is predicted that cybercrime damages will amount to $6 trillion globally by the end of 2021 and grow by 15 percent annually over the next five years, reaching $10.5 trillion by 2025, up from $3 trillion in 2015 (Morgan 2020).

One of the countries affected most by information security data breaches and cybercrimes is Saudi Arabia. The 2019 IBM Security and Ponemon Institute Cost of Data Breach Report showed that Saudi Arabia and United Arab Emirates (UAE) enterprises, which

represent The Middle East in the reports, are at the top of the list of the average number of records per breach as illustrated in Figure 1.1 (*Cost of a Data Breach Report 2019* 2019). Moreover, Saudi Arabia and UAE are ranked the second-highest regarding the average total cost per data breach from 2018 to 2020 (*2018 Cost of a Data Breach Study: Global Overview* 2018; *Cost of a Data Breach Report 2019* 2019; *Cost of a Data Breach Report 2020* 2020).

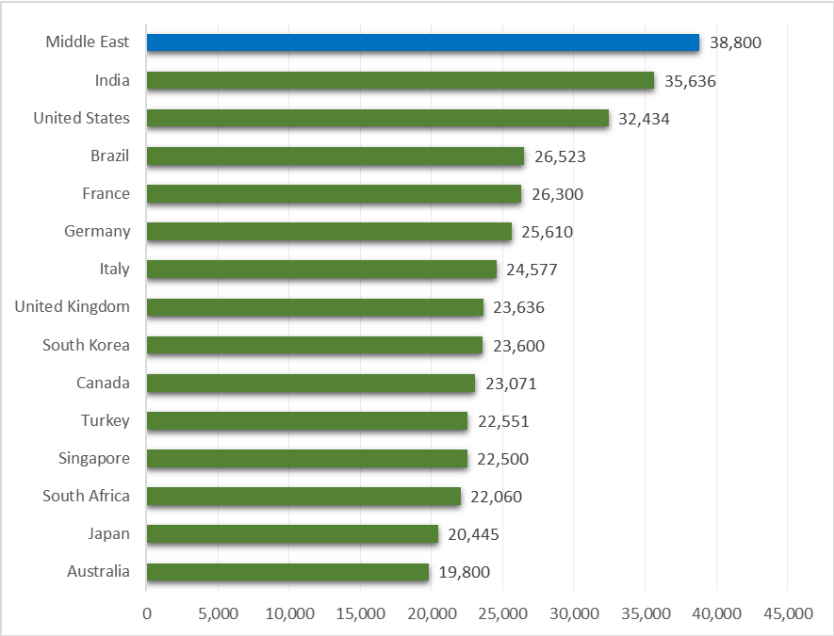

Figure 1.1 The Average Number of Records per Breach by Country 2019

Source: (Cost of a Data Breach Report 2019 2019)

Figure 1.2 shows that in Saudi Arabia and UAE, the average number of breached records per data breach in 2017 was 33,125 records compared to the global average of 24,089 records, which is 37.5 percent higher than the global average. Similarly, Saudi Arabia and UAE were higher than the global average in 2018 (i.e., 36,451 records compared to 24,615 globally) and in 2019 (i.e., 38,800 records compared to 25,575 records globally); that is 48 percent in 2018 and 51.7 percent higher in 2019 than the global average (*2017 Cost of Data Breach Study* 2017; *2018 Cost of a Data Breach Study: Global Overview* 2018; *Cost of a Data Breach Report 2019* 2019). By 2023, according to the MEA Cybersecurity Market report, Saudi Arabia's information and cyber security market will reach $5.5 billion (Geronimo 2019).

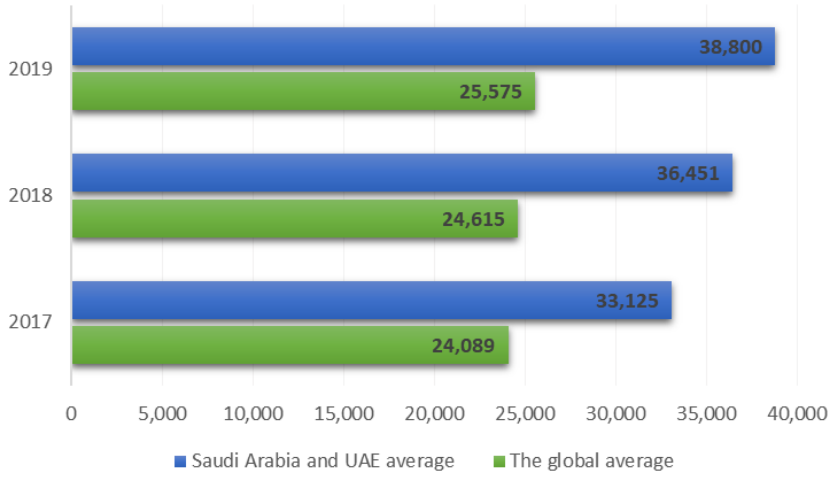

Figure 1.2 The Average Number of Breached Records 2017-2019

Source: (*2017 Cost of Data Breach Study* 2017), (*2018 Cost of a Data Breach Study: Global Overview* 2018), (*Cost of a Data Breach Report 2019* 2019)

Implementing Vision 2030 put Saudi Arabia at the forefront of positive change of digital transformation. In 2016, Saudi Arabia's Vision 2030 was initiated as a strategic plan for economic development in all sectors. Unlike many developed countries, Saudi Arabia quickly adopted e-services strategies such as e-government and e-commerce in recent years. This digital transformation exhibits many economic advantages, yet amplified digitisation has increased the need for more stringent information security standards as the cyberattacks continue to rise. In addition, Saudi Arabia's political conflicts with its neighbouring countries, including Israel and Iran, have increased cyberespionage against Saudi Arabia. For example, on June 19, 2015, more than 500,000 cables and emails from the Saudi Foreign Ministry, including many highly sensitive reports from the Saudi's General Intelligence Services, were breached after an attack by the self-proclaimed "Yemeni Cyber Army" (Blake 2015).

Bitdefender, a cybersecurity technology and research company, reported that critical infrastructure in Saudi Arabia was targeted in January 2019 by Iranian groups that managed to access critical infrastructures in Saudi Arabia for the purpose of a cyberespionage campaign using sophisticated tools (Hassan 2021; Lakshmanan 2020). It is clear that Saudi Arabia appears to be at more risk of data breaches and cybercriminals and has a higher impact per breach than most countries.

The lack of sufficient security budgets is often an obstacle to achieving the desired

level of information security protections (Taylor 2015). However, that is not the case in Saudi Arabia. It has been emphasised that Saudi Arabian organisations invest more in technology than humans in a bid to protect information assets from any vulnerability that could lead to a possible data breach or cybercrimes (Alzamil 2012).

1.2 Problem Statement

There are compelling reasons to conclude that there is no single security approach or practice that will work in all contexts, implying that cultural aspects should be considered when developing effective information security practices as it is believed that other factors (e.g., culture) directly affect various elements of information security (Flores, Antonsen, and Ekstedt 2014). Accordingly, studies have concluded that there is an increased need for Saudi Arabia to develop its standards, policies, and legal standards (Fareed 2017). Moreover, information security risk management effectiveness can be influenced by many factors related to culture and management style. ISRM practices need to be aligned with the business objectives of organisations and applied at business processes, people, and technology (PPT) of the organisation. This indicates a need to explore and understand the various perceptions of the factors which might have a vital influence in the effectiveness of information security risk management implementation in Saudi Arabian organisations.

This research attempts to provide an overview of ISRM practices to better understand the effectiveness of international ISRM standards and best practices in Saudi Arabia. Moreover, it investigates the factors that determine an effective ISRM model for large Saudi Arabian organisations. The research offers essential insights into ISRM practices in Saudi Arabia and their degree of compliance.

1.3 Research Objectives

The overall research objectives are to gain an understanding of factors which influence ISRM in the context of large Saudi Arabian organisations. This can lead to the development of an ISRM model that improves the effectiveness of ISRM to best fit Saudi Arabian organisations. The research was focused on building a reliable and effective ISRM model

relevant to most organisations in Saudi Arabia. The ISRM model suggests a set of factors to Saudi businesses to improve their ISRM experience and effectiveness, and therefore enhances their information security position. This also aligns with the Saudi Arabia Vision 2030 goals, which include digital transformation and information protection.

To achieve that, the following objectives were identified:

***Main objective**: Develop an effective ISRM model for large Saudi Arabian organisations*

***First Sub-objective:** Examine large Saudi Arabian organisations' compliance with ISRM standards*

***Second Sub-objective**: Explore the ISRM standards implementation challenges that large Saudi Arabian organisations face*

***Third Sub-objective**: Explore the factors that influence the effectiveness ISRM standards in large Saudi Arabian organisations*

1.4 Research Questions

To achieve the research objectives, three research questions were constructed which guide the development of the proposed ISRM model intended to assist large Saudi Arabian organisations to effectively implement ISRM.

The research questions are:

3. What is the level of large Saudi Arabian organisations' compliance with ISRM standards?
4. What are the ISRM standards implementation challenges in large Saudi Arabian organisations?
5. What are the factors that must be considered when developing an effective ISRM model for large Saudi Arabian organisations?

1.5 Theoretical Contribution

This research proposes a new Information Security Risk Management (ISRM) model for large-sized Saudi Arabian organisations. Large-sized organisations exhibit some

differences in terms of resources and expertise available which, in turn, may influence the IT and information security adoption in comparison to those found in small and medium enterprises. The significance of this model lies in its concentration on the ISRM factors which consider cultural and social complications in Saudi Arabia because there is evidence of compromise of ISRM as it is practiced in Western countries. There is a lack of ISRM research in a Saudi Arabian context, and development of this model will add to the existing knowledge base for further research and practice. It also provides additional insight into ISRM in Saudi Arabia, and due to its cultural, commercial, and economic similarities to other countries in the Arabian Gulf region, serve as a base for comparative studies between western countries and Middle Eastern countries.

In consideration of the overall objectives of this research, a literature review is presented of the current ISRM approaches relevant to the research topic. The review of the literature provides the essential theoretical background to the research area and identifies existing gaps in the knowledge.

Although there is lack of research that covers ISRM in Saudi Arabia, some of these research attempts to explore and analyse information security management (ISM) in Saudi Arabia includes internal threats and IT governance. None of these efforts provides ISRM a full, explanatory investigation which explores factors the influence ISRM in Saudi context. This includes the lack of understanding of the importance of academic research and relevant theories which comprise the research problem. This research validates the ISRM challenges and factors in Saudi Arabia that contribute to a new ISRM model.

1.6 Practical Contribution

ISRM is a practical business discipline which currently has no localised or regional version. This research provides an ISRM model that improves ISRM implementation effectiveness in Saudi Arabia organisations. Also, it can increase the knowledge base of ISRM in Saudi Arabia to assist organisations in Saudi Arabia to adopt ISRM and implement it more effectively.

The outcomes of this research are relevant to many types of organisations, such as

public and private sectors, to implement ISRM and effectively protect their information assets. This can make business and government processes more efficient and resilient to cybercrime. Moreover, it is also relevant to other Arabian Gulf countries.

1.7 Research Method and Design

This research has been guided by an interpretive research philosophy. It employed a qualitative approach that is comprised of two phases of data collection. The first step was to develop the initial ISRM model obtained from the review of the literature. Then for the phase one data collection step, semistructured interviews were conducted with participants from different large Saudi Arabian organisations and sectors to examine ISRM practices in Saudi Arabia, and also to unveil factors influencing ISRM effectiveness. The findings resulted in an enhanced ISRM model that was evaluated by focus groups in phase two data collection, bringing about further enhancement and development of the proposed ISRM model.

1.8 Research Outline and Structure

This thesis consists of seven chapters, as shown in Figure 1.3:

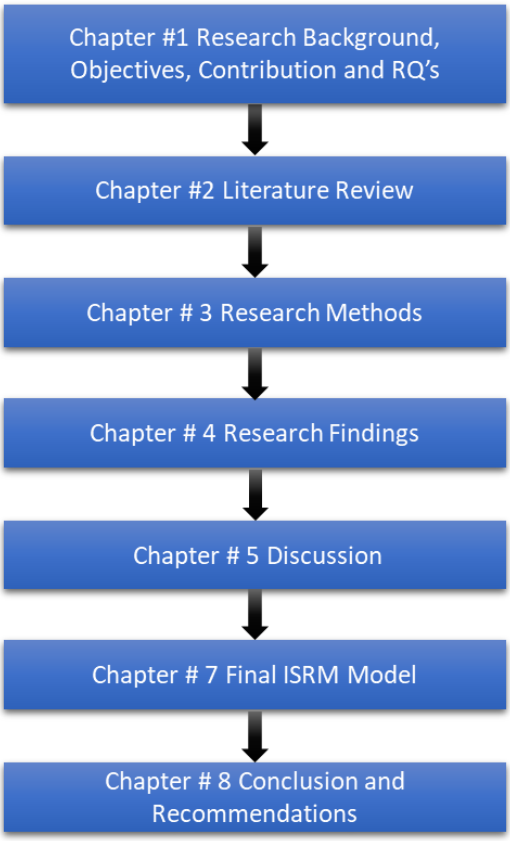

Figure 1.3 Research Outline

Chapter 1 provides an overview of this study's background, objectives, contributions, and research questions along with discussions of the thesis framework.

Chapter 2 reviews the major existing literature related to ISRM and Saudi Arabian ISRM practices and challenges. This chapter provides a critical review of ISRM's contributing factors which assisted in develop in the initial ISRM model. It concludes by highlighting the research gaps.

Chapter 3 describes the research methodology and research process then justify the chosen research design. The data collection process and analysis of data for each phase are discussed and justified. Finally, the different phases of the research are described.

Chapter 4 outlines phase one of the data collection, the semistructured interviews, and observations along with the data analysis.

Chapter 5 discusses the phase one data findings to churn out the enhanced ISRM model.

Chapter 6 highlights phase two of the data collection, the focus groups, observations, data analysis, and a final discussion to further examine the enhanced ISRM model and refine the final version of the proposed ISRM model.

Chapter 7 summarises the research and provides answers to the research questions. The theoretical and practical contributions are discussed. It acknowledges the research limitations, makes recommendations, and suggests avenues for future research. Both the references and appendices conclude this work.

1.9 Summary

International information security risk management standards and best practices provide a framework for managing risks to information security. They are essential tools that assist organisations in protecting their information assets. However, these standards are developed without the consideration of regional or countries differences. It is believed that there no “one size fits all” management standard which applies to information security risk management standards and best practices.

Middle Eastern countries such Saudi Arabia face many difficulties in implementing Western technology and standards due to different regulations and management styles from those of Western countries. Moreover, Saudi Arabia is heavily affected by information security data breaches and cybercrimes.

The objective of this research is to explore factors that influence ISRM effectiveness in the Saudi Arabian context that contribute to the development of an effective ISRM model for large Saudi Arabian organisations. To date, no other models have been developed for Saudi Arabian organisations of this size.

The following chapter presents the literature review which reveals the research gap and factors that assist in developing a conceptual ISRM model.

CHAPTER 2. LITERATURE REVIEW

2.1 Introduction

This chapter provides an overview of the extant research by reviewing the literature related to Information Security Risk Management (ISRM) and its practices in the context of Saudi Arabian organisations. In addition, the chapter also discusses the research gaps and the contributions of previous studies.

As a result of different managerial mindset influenced by culture and other factors, international ISRM approaches and best practices might not be as effective in Middle Eastern countries, and Saudi Arabia in particular (Al-Adaileh and Al-Atawi 2011; Al-Gahtani, Hubona, and Wang 2007). This indicates a need to study the current information security weaknesses in relation to ISRM approaches in the Saudi Arabian context as well as to determine the factors that contribute to an improved ISRM standard for Saudi Arabian organisations.

This review of relevant studies begins by providing background knowledge on information security and managing its risks. It then traces the history of ISRM standards and discusses the most common standards, including a definition of the terminologies pertinent to this area of research. Subsequently, the review identifies and explains the challenges in the current ISRM standards and best practices. It has been argued that developing a general high-level standard without taking into consideration the cultural differences shows drawbacks in implementation of the standards as well as its ineffectiveness. In addition, the review discusses Saudi Arabian organisations' information security issues that are related to ISRM. After that, most of the existing literature in this area that is centred on cases rather than the more holistic ISRM framework theory and practice in the Saudi context is explored. Finally, the chapter lays the foundation for the research questions.

2.2 Information Security

Information, like other business assets, is a vital asset of an organisation and therefore needs to be well-guarded and secured. It could be stored in several formats such as a digital

format and a material format (ISO/IEC27000 2018). It is characterised as "a valuable entity which is independent of the technology that manipulates it" (Borek, Parlikad, and Woodall 2011, p. 477). Information security is "the protection of information and information systems against unauthorised access or modification of information, whether in storage, processing, or in transit, and against denial of service to authorised users" (*National Information Assurance (IA) Glossary* 2010, p. 37). In the same vein, Raggad (2010, p. 204) argued that it is the "protection of information from unauthorised access, use, disclosure, disruption, modification, or destruction in order" to accomplish an organisation's Confidentiality, Integrity, and Availability "CIA-Triad" of information (Raggad 2010; ISO/IEC27000 2018; Wheeler 2011). In addition, it may involve protecting the reliability and authenticity of information to ensure that organisations can be held accountable (Marathamuthu 2015). CIA can be considered as a guideline that illustrate organisations' policies for information security (Antunes et al. 2021). Figure 2.1 illustrates the interrelationship of the CIA-Triad.

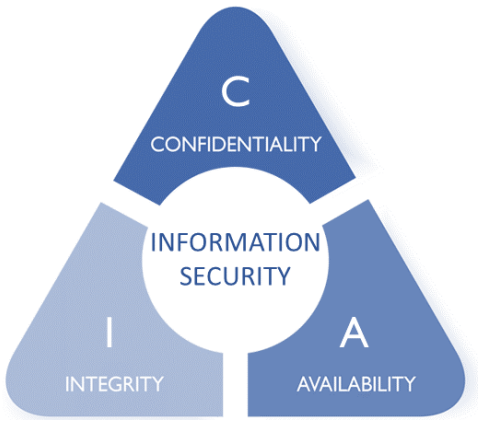

Figure 2.1 The CIA-Triad

Source: (Raggad 2010)

The component terms of the CIA Triad are examined below:

- **Confidentiality**: the "property that is not disclosed to unauthorised individuals, entities, or processes" (ISO/IEC27000 2018, p. 2). It is an important element of privacy and that reflects the ability to protect data from unauthorised access (Andress 2011).
- **Integrity**: the "property of accuracy and completeness" (ISO/IEC27000 2018, p. 5). It is the ability to protect data, partially or fully, from change or deletion via unauthorised access. In addition, integrity is the ability to reverse authorised and

unauthorised changes that need to be undone (Andress 2011).

- **Availability**: the "property of being accessible and usable upon demand by an authorised entity" (ISO/IEC27000 2018, p. 2). It is the ability to access data when needed and prevent interruptions at any point in the chain that could make data inaccessible. Such issues can result from network or cyberattacks, power loss, application issues, or other problems (Andress 2011).

Additional information security properties such as authenticity, accountability, reliability, and non-repudiation have been introduced to the CIA-Triad (Ma, Johnston, and Pearson 2008; Da Veiga and Martins 2015; Szmit 2015). The additional properties are secondary (Dubois et al. 2010) and are examined below:

- **Authenticity**: the "property that an entity is what it claims to be" (ISO/IEC27000 2018, p. 2). It is the assurance of being genuine and can be verified and trusted. It involves proof of identity such as using a username and password or biometric authentication methods such as fingerprint or retinal scans (*National Information Assurance (IA) Glossary* 2010).
- **Accountability**: a principle in which actions of an entity systems can be traced and hold it uniquely responsible for its actions (Bitzer, Brinz and Ollig 2021).
- **Reliability**: the "property of consistent display of intended behaviour and results" (ISO/IEC27000 2018, p. 7).
- **Non-repudiation**: the "ability to prove the occurrence of a claimed action or event and its originating entities" (ISO/IEC27000 2018, p. 6). It is the assurance that the sender of data is provided with delivery proof and the recipient is provided with the sender's identity proof, therefore neither can deny having processed the data (*National Information Assurance (IA) Glossary* 2010).

Information security is as crucial as ever due to a result of the fact that technology applied to information creates a high level of risks to organisations. For example, information might be inappropriately disclosed because its confidentiality is modified or exposed and therefore its integrity is jeopardised, or it is lost because its availability is threatened (Khidzir, Mohamed, and Arshad 2010a). Information security has become a business facilitator and an essential part of an organisation in a bid to improve consumers' trust and to effectively use innovative technologies for the business process (Ashenden 2008; Yaokumah 2013). The field

of information security has grown from a technical initiative to a broader and business-focused field to protect all information within an organisation. Its goals are not just to enhance confidentiality, integrity, and availability of information, but to deliver tangible business benefits by protecting, facilitating, and controlling the sharing of information as well as managing the possible associated risks (Ashenden 2008).

The challenges involved in determining the factors that contribute to information security are complex. However, a variety of management methods and procedures have been developed in the last few decades to achieve a satisfactory level of information security that provides the mechanisms needed to protect the organisations' information assets (Fenz et al. 2014). Therefore, organisations are paying more attention to information security and protection by adopting information security management standards (ISMS) (Susanto and Almunawar 2018).

Alumaran, Bella, and Chen (2015) indicated that information security is not only a technical problem that needs to be examined but is also a management concern that needs to be addressed carefully by information security management members and the management of an organisation at large. Managing information security involves maintaining the level of risk exposure within acceptable levels that is aligned with the business plans and strategy (Fonseca-Herrera, Rojas and Florez 2021; Wheeler 2011). Therefore, the management of information security risks is one of the top crucial issues in the field of information security. Organisations looking to obtain an acceptable level of security must be able to identify security issues and establish an approach to prevent their information assets and operation (Alsaif, Aljaafari, and Khan 2015).

2.3 Risk Management

Risk and risk management have been examined in various domains including insurance, management, medicine, and engineering. Each of these domains addresses risk in a way that is relevant to its perspective (Khidzir, Mohamed, and Arshad 2010a). The International Standards Organisation (ISO) defined risk as "the effect of uncertainty on objectives, regardless of the domain or circumstances" (ISO/TR31004 2013, p. 7). It can also be described

as “the combination of the likelihood of an event and its consequence” (ISO31000:2018 2018, p. 1). However, more precise definitions have been introduced by other institutions such as The National Institute of Standards and Technology (NIST) in which risk was defined as “a measure of the extent to which an entity is threatened by a potential circumstance or event, that is a function of:

- The adverse impact, or extent of the damage, that would result if the situation or event occurred
- The likelihood of occurrence” (NIST 2018, p. 104)

Various types of organisational risks are identified including investment risk, legal liability risk, safety risk, security risk, supply chain risk, and inventory risk (Trajkovski and Antovski 2013). Therefore, in information security context, risk is defined as a combination of:

1. The likelihood that any vulnerability in an information system will be exploited, intentionally or unintentionally, by any threat that result in a loss of confidentiality, integrity, and/or availability, or
2. The potential impact or extent of harm that a loss of confidentiality, integrity, or availability will have on the operations, assets, or individuals (McCumber 2004; Nemati 2010).

Risk management can be defined as “coordinated activities to direct and control an organization with regard to risk” (ISO31000:2018 2018, p. 1). NIST special publication SP800-39 defined risk management as:

> a comprehensive process that requires organisations to frame risk, assess risk, respond to risk once determined, and monitor risk on an ongoing basis using effective organisational communications and a feedback loop for continuous improvement in the risk-related activities of organisations. (Trajkovski and Antovski 2017a, p. 405)

Wheeler (2011) stated that the main goal of risk management is maximising the organisation’s output, including products, revenue, services, and so forth, while minimising the unexpected outcomes (Wheeler 2011). Stoneburner (2002) added that effective risk

management should protect not only the organisation's assets but also have the ability to accomplish its organisational mission (Stoneburner 2002).

Beasley (2007) argued that a risk management process put in place by the management of an organisation and other personnel should be aimed at identifying potential threats that may affect the organisation, and to provide assurance regarding the achievement of the organisational objectives. Trajkovski (2017) stressed that risk management is carried out as an organisational-wide task to addresses risk across all levels, and then to ensure that the risk-based decision making is incorporated into every part of the organisation (Trajkovski and Antovski 2017a). In general, risk management consists of six processes which are: (a) context establishment, (b) risk assessment, (c) risk treatment, (d) risk acceptance, (e) risk communication and consultation, and (f) risk monitoring and review (Javaid and Iqbal 2017; ISO31000:2018 2018) as shown in Figure 2.2.

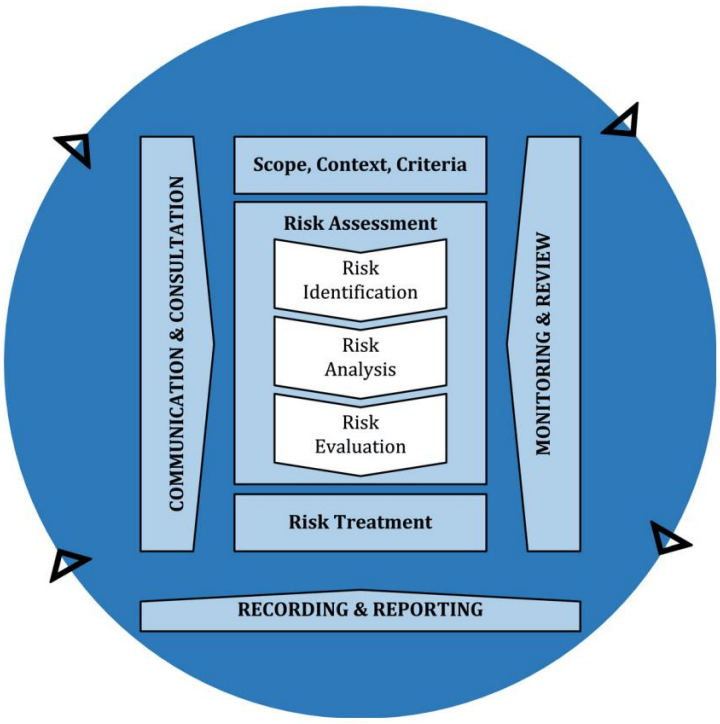

Figure 2.2 Risk Management Process

Source: ISO31000/2018

Beňová (2015) indicated that risk management is not a one-time or periodic activity; it is a permanent and continuous activity that identifies, analyses, evaluates, examines, and treats risks. The development of an effective risk management programme requires the

understanding of the organisation's context, establishing proper policy, assigning risk management roles and responsibilities aligned with organisational processes, allocating of resources, and establishing of communication and reporting channels (Webb 2013). Meanwhile, risk cannot be completely eliminated; it must to be reduced to an acceptable level that the business decides to live with. Organisations invest substantial resources in developing appropriate an information security risk management program that would address the risks they are exposed to. These programs must have firm foundations, which is why organisations look for risk management standards that are widely accepted across several enterprises (Al-Ahmad and Mohammad 2013).

One of the major risk management challenges of organisations is how to manage their potential information security risks due to the increasing use of IT systems (*The Risk It Framework* 2009). Stoneburner (2002) argued that it is primarily an important function of management of organisation rather than a technical function executed by the IT experts in an organisation (Stoneburner 2002). The application of risk management to information security is discussed in the next section.

2.4 Information Security Risk Management "ISRM"

In order to achieve successful information security, organisations need to implement applicable controls through the risk management process and manage them using an information security management programs or systems. This includes "policies, processes, procedures, organisational structures, software and hardware to protect the identified information assets" (ISO/IEC27000 2018, p. 12).

Information Security Management (ISM) is an information security process that identifies the organisation's IT environment and its criticality, prioritising its involvement to the organisation's business capabilities. In addition, it identifies all possible IT security risks as well as assesses and mitigates them. Finally, it provides frequent improvement of the organisation's security risk position (Raggad 2010). Ashenden (2008) defined the management of information security as "that part of the overall management system that is based on a business risk approach, to establish, implement, operate, monitor, review,

maintain and improve Information Security" (p. 197). The goal of information security management is to prevent or minimise to the lowest possible level the potential damage to organisational assets through maintaining quality information infrastructures, following processes and procedures (Alnatheer 2012; Wheeler 2011).

Managing information security is one of the most important information security issues (Alsaif, Aljaafari, and Khan 2015). It ensures that appropriate and proportionate security measures are chosen to protect information assets and provide confidence to interested parties. Information security requires the overlay of a strong management program that can be achieved coherently and efficiently to protect organisations (Ashenden 2008; Alsaif, 2015). According to Okonofua, Rahman, and Ivanova (2019), managing the risk of information security is challenging due to the fast evolution, increasing recurrence, and severity of threats to organisations. The author noted that such threats may come from both internal and external actors and may manifest as system vulnerabilities, technical failures, and external events, among others.

It has been indicated that a crucial component of ISM is the risk management, which has become a formal component of ISM referred to as Information Security Risk Management (ISRM) (Raggad 2010; Alcántara and Melgar 2016; Szmit 2015). Likewise, Blakley (2001) stated that risk management for information security is very important because the technology applied to information nowadays increase risks. In addition, García-Porrasargues, Huamani-Pastor, and Armas-Aguirre (2018) argued that ISRM is a crucial part of the best practices in corporate governance and is no longer considered a major issue for information technology, but as a critical business practice that influence an entire organisation has become the main concern of organisations' corporate governance (Okonofua, Rahman, and Ivanova 2019).

ISRM takes over definitions and procedures of risk management theory that are applied in the area of information security. Information security deals with the protection of information assets against the risks that come from internal or external business environments (Beňová 2015). According to Kuzminykh et al. (2021), ISRM can be defined as:

> a process that consists of identification, management, and elimination or reduction of the likelihood of events that can negatively affect the resources of the information

system to reduce security risks that potentially have the ability to affect the information system, subject to an acceptable cost of protection means that contain a risk analysis, analysis of the “cost-effectiveness” parameter, and selection, construction, and testing of the security subsystem, as well as the study of all aspects of security. (Kuzminykh et al. 2021, p. 602)

It balances the organisation's operational and economic costs by protecting the entire IT infrastructure and data to support their missions (Raggad 2010). According to Naseer (2017), ISRM is a process that guide organisations to continuously identify, integrate, and analyse risks as well as assess the likelihood and impact of threats on businesses, which could help in deciding the appropriate actions to be taken to minimise or eliminate risks to acceptable levels. This process can be applied to the entire organisation, one or more departments within an organisation, or to a specific physical location or service (Beňová 2015).

ISRM enables organisations to accomplish their missions by:

- Securing the CIA-triad of the organisation’s information
- Enabling management to make risk management decisions that justify information security investment
- Assisting management in dealing with potential risks and exercising good practices to eliminate risks (Watkins 2010).

The main objectives of ISRM are:

1. Identifying potential security risks (risk identification)
2. Prioritizing the identified risk according to severity (risk assessment)
3. Determining the most cost-effective ways of controlling risks (risk treatment)
4. Monitoring changes to the risk management program (risk review) (Webb et al. 2014; Mohammed and Mohammed 2017).

Table 2-1 illustrates the tasks of generic ISRM processes and highlights the action description for the generic process for each process and task (Khidzir, Mohamed, and Arshad 2010a).

Table 2-1 Generic ISRM Processes and Task Descriptions

Information Security Risk Management Processes Task	Action Descriptions
1. Risk Identification	• Identify Critical Information Assets • Identify Threats and Vulnerabilities to Critical Information Assets • Identify Security Requirements for Critical Information Assets • Identify Current Security Policies, Practices, and Procedures • Identify Current Technology Vulnerabilities and Threats • Identify Current Organisational Vulnerabilities and Threats
2. Risk Analysis	• Analyse value for information security risks probability and impact to an organisation's ICT services (Evaluate Information Risks) • Analyse which risk need to be addressed based on the nature and the organisation's general tolerance for information risk (Prioritise Risk and Mitigation Approach)
3. Risk Treatment Plan	• Develop Protection Strategy (Security Related-practices) • Develop Risk Mitigation Plan (Plan to reduce risks to organisation's critical information assets and ICT Services) • Develop an Action Plan by specifying a set of actions for protection strategy and risk mitigation plan (Action plan, budget, schedule, success criteria, measures to monitor plans, human-resource required to implement action plan)
4. Risk Treatment Plan Implementation	• Execute all action plans according to the schedule and success criteria (as defined in the Risk Treatment Plan) • Reprioritise work tasks and schedule to incorporate the action plan (if necessary)
5. Risk Monitoring	• Measures the status of action plan with the respect to their schedules and success criteria (Monitor of the progress of action plan • Indicates the presence of new risks or significant changes to existing risks
6. Risk Control	• Analysed data tracking of action plan • Analysed data tracking of key risk indicators • Decision on changes to action plan • Decision on identifying new risks • Execute control decision into action • Start of new risk identification task

Source: Khidzir, Mohamed, and Arshad (2010a)

According to ISO/IEC27005 (2018), the ISRM process involves context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review as illustrated in Figure 2.3. ISRM comprises an iterative and continuous process which starts with establishing the context and then conducting a risk assessment. This is followed by risk treatment if the previous steps have provided sufficient information to determine the proper actions to minimise the risk to an acceptable level. However, if information provided is not sufficient, another iteration of the risk assessment needs to be conducted. Furthermore, if risks have not reached an acceptable level, another iteration of the risk assessment needs to be conducted and then risk treatment (ISO/IEC27005 2018; Amancei 2011).

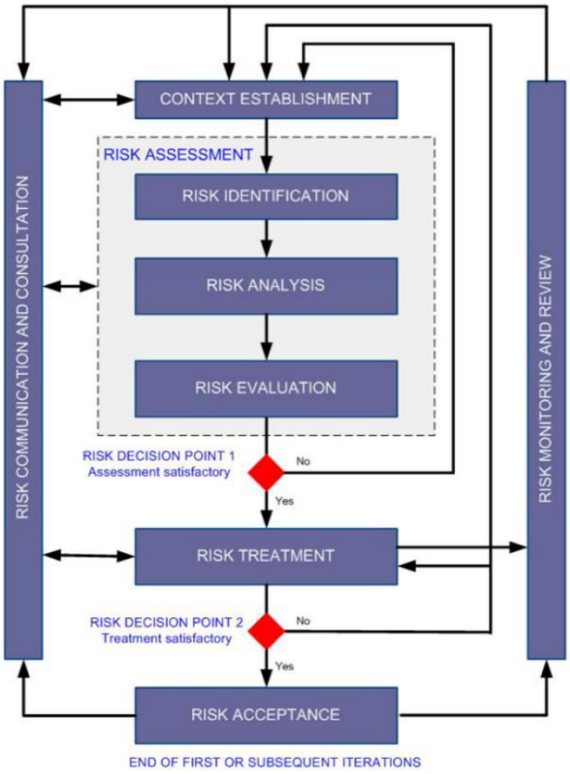

Figure 2.3 ISRM Process

Source: ISO/IEC 27005 (ISO/IEC27005 2018)

ISRM is a holistic activity that influences every aspect of an organisation including its mission, business-planning activities, and the organisational architecture. It allows organisations to determine if they are protecting their information assets using the most effective and cost-efficient means (Webb et al. 2014). Therefore, ISRM not only represents a

technical function carried out by IT professionals but also an important management task of an organisation (Stoneburner 2002). Managing information security risks is a complex continuous activity that requires the entire organisation's involvement. It involves the provision of the strategic vision, goals, and objectives for the organisation by top management while the mid-level management provides planning and execution where individuals are assigned to develop, implement, operate, and maintain the systems that support the organisation's missions and business functions (NIST 2018).

There are several types of ISRM approaches that can be adopted by organisations. The common goal of these approaches is to enable organisations to effectively manage the risks by minimizing them to an acceptable level (Saleh and Alfantookh 2011; Trajkovski and Antovski 2013). Some of the widely accepted and adopted ISRM frameworks are discussed in the next section.

2.5 Information Security Risk Management Frameworks

ISRM is not a new research domain, and other mechanisms have been used for some time. In 1975, the Annual Loss Expectancy (ALE) was proposed by the U.S. National Bureau of Standards for measuring IT risks. ALE was very basic and could not distinguish between a high or low impact of events (Fenz et al. 2014). After a series of workshops in the 1980s by the U.S. National Bureau of Standards, ALE evolved into an iterative process for information security risk management with the following steps:

- Requirements identification
- Threats analysis
- Risk measurement
- Acceptance test
- Protection and implementation (Fenz et al. 2014)

Though some additional steps and process structure enhancement have been developed, current ISRM approaches are mainly based on ALE as it was developed in the 1980s (Fenz et al. 2014).

An information security framework is a set of documented, understandable policies,

procedures, and processes which define the ways that information is managed within an organisation (Mohammed and Mohammed 2017; Wild 2018). The main goal is to lower the risk and vulnerabilities and therefore increase the confidence in an organisation. There are hundreds of information security frameworks that have been developed and used globally for a variety of businesses and sectors (Wild 2018). Likewise, there are several ISRM frameworks that have been published by national and international organisations including ISO, NIST, AS/NZS, BSI. Others have been issued by professional organisations such as ISACA, while a few have been presented and published by research projects. These frameworks have been developed to specific needs so they have a wide range of application, structure, and steps (Al-Ahmad and Mohammed 2015; Wangen 2017; Trajkovski and Antovski 2017a; Hallstensen, Snekkenes and Wangen 2017). These frameworks provide a structure that categorises and organises risks to help organisations measure and monitor the effectiveness of their activities. This can be accomplished through the control objectives outlined in the framework, which enables an organisation to assess both its security posture and goals as well as to improve procedures that minimise risks and protect its assets. In addition, it enables organisations to prioritise and coordinate activities, not only for a single regulatory mandate but across multiple compliance mandates as well (Haber and Hibbert 2018).

An ISRM framework is adopted and implemented by organisations in order to address information security issues using a consistent, repeatable, and auditable approach. It provides a solid foundation for decision-making and budget allocation, among others. In addition, it offers the internal and external stakeholders of an organisation with the confidence that information security is being effectively addressed (Al-Ahmad and Mohammad 2012; Ashenden 2008). Some organisations spend considerable resources in developing effective ISRM frameworks that ultimately address the risks to which they are exposed. These frameworks must be established on solid foundations, which is why most organisations look for frameworks that are widely accepted and common across enterprises (Al-Ahmad and Mohammad 2013).

Barafort (2017) suggested that international information security frameworks and standards provide an open access to structured technical domains, voluntary positioning for certifications, and international consensus. A survey by Association Française de Normalisation (AFNOR), the French National Body for Standardisation, indicated that

standardisation has a positive impact on the economy with clear benefits on organisation performance and results (Barafort, Mesquida, and Mas 2017). Furthermore, in an attempt to differentiate themselves from competitors, ISRM frameworks developers vary in their approach and methodologies. For example, International Standards Organisations (ISO) produce high levels of abstraction in an attempt to ascertain that guidance is widely accepted by all types of organisations. Whilst other ISRM frameworks developed by governments, such as the National Institute of Standards and Technology (NIST), focus mainly on processes, regulations, or operational impacts that do not fulfil non-governmental organisations' needs (Abdur 2015).

Haber (2018) stated that ISRM frameworks such as NIST, ISO, and COBIT are widely accepted by organisations to assess, monitor, and measure their security effectiveness and compliance investments. Regardless of the approach, the goal is to provide guidance and recommendations for organisations by following practices and procedures that create business value and minimise risk (Haber and Hibbert 2018). In selecting a security framework, there is no "one size fits all" (Haber and Hibbert 2018; Saleh and Alfantookh 2011). For example, ISO 27000 series provides breadth and applicability across different industries and organisation sizes, but some organisations adopt it when they need to market their ISO certification. While NIST SP 800-53 was designed specifically for U.S. government agencies, but similar to ISO, NIST could provide information security risk standards that are applicable for different industries and organisation sizes (Haber and Hibbert 2018; Javaid and Iqbal 2017). Each framework was developed to meet a specific need and therefore has a different goals, steps, structure, and application (Saleh and Alfantookh 2011). The following sections discuss the most currently adopted and widely accepted ISRM frameworks.

2.5.1 NIST SP800 Series

The National Institute of Standards and Technology (NIST), a part of the United States Department of Commerce, has developed an information security framework for the federal government and its contractors. The idea is to enhance information security and improve risk management processes (NIST 2011). NIST has developed a number of documents that comprise the United States government's unified information security framework. They cover the entire enterprise from governance and risk management to individual system controls

(Bartol 2014; Javaid and Iqbal 2017).

NIST publications provide guidance for risk assessment processes to achieve successful information security. For example, NIST SP800-30 is a guideline for risk management, NIST SP800-30 Rev. 1 is a risk assessment guideline, NIST SP800-37 addresses risk management and can be used as a guideline, and NIST SP800-39 addresses information security risk and is more specific to risk management and assessment. NIST provides a comprehensive risk assessment mechanism with supporting examples (Knowles et al. 2015; Javaid and Iqbal 2017). The four main components of NIST800-39 are:

- Framing risks: the process of defining risk, creating a risk management strategy that can define how the risk can be assessed, and how to respond to the assessed risk as well as how the risk can be monitored
- Assessing risks: identifying properties of risks, prioritising them, and estimating direct or indirect risk impacts on organisations or individuals that might occur when threats exploit vulnerabilities and the likelihood of such incident
- Responding to risks: creating an organised, consistent, and well-defined response
- Monitoring risks: determining how to monitor risks as well as how to effectively mitigate them (Fenz et al. 2014; Knowles et al. 2015)

In order to achieve more accurate assessment results, NIST800-39 introduced these risk assessment activities: information systems and their data categorisation, security controls implementation to those systems, security controls assessment, and information systems authorisation based on the risk and continuous monitoring of the security controls (Al-Ahmad and Mohammad 2012). Shanthamurthy (2011) argued that the NIST800-39 standard is more for technical risk assessment. It differs from other standards such as ISO/IEC 27005 in that the first step is system characterisation rather than context establishment. In addition, NIST considers vulnerabilities first followed by existing controls; therefore, risk mitigation by existing controls is not taken into consideration (Shanthamurthy 2011).

2.5.2 ISO/IEC 27005

Founded on February 1947, the International Organisation for Standardisation (ISO) is an international standard body comprised of members from different standards organisations

(About Us 2019). It is the largest developer and publisher of international standards with more than 20 million ISO certified or recognised businesses (What Is 'Iso'? 2019). ISO has established joint committees with the International Electrotechnical Commission (IEC) to develop standards and terminology in the electrical field and its related technologies (Sahibudin, Sharifi, and Ayat 2008). The ISO/ICE27000 series provide a range of managerial and technical controls that help organisations to protect their information assets (Webb et al. 2014). It explains the objectives of ISRM in general terms and provides high-level guidance (Flores, Antonsen, and Ekstedt 2014). The general ISO 27000 series of standards are:

- ISO/IEC27000: provides a general overview of information security and terms and definitions
- ISO/IEC27001: specifies the requirements for information security management systems
- ISO/IEC27002: provides guideline for the implementation of the controls
- ISO/IEC27003: provides guidance for the implementation of information security management systems
- ISO/IEC27004: advises on how to monitor and measure the performance of information security management systems
- ISO/IEC27005: provides guidance for ISRM
- ISO/IEC27006: provides guidance for certification of information security management systems
- ISO/IEC27007: provides guidelines for audit an information security management system

The risk management standard ISO/IEC 27005 was first published in 2008 and focused on the protection and security of information assets in organisations, based on the principles outlined in ISO/IEC 27001 (Javaid and Iqbal 2017). It was built on the “knowledge concepts, models, processes and terminologies of ISO/IEC 27001” (Agrawal 2017, p. 265).

ISO/IEC 27005 ISRM standard provides guidelines for managing information security risk and enables organisations to choose their own risk assessment approach based on their objectives (Shanthamurthy 2011; Javaid and Iqbal 2017). Naden (2018) stated that “ISO/IEC 27005 provides the ‘why, what and how’ for organisations to be able to manage their

information security risks effectively in compliance with ISO/IEC 27001" (p. 1). ISO/IEC 27005 outlines a systematic process that is accurate and rigorous in terms of required steps, as well as classifying and treating risks. The ISO/IEC 27005 is different in that it can be used as an enabler for organisations that needs freedom to identify their own risk parameters to implement effective and efficient controls.

This is a different approach to other common standards such as COBIT and NIST SP 800-30 (Shanthamurthy 2011). It was developed to support the successful application of information security through a risk management approach and can be implemented by all organisation types, including commercial enterprises, financial institutes, and government agencies, among others (Bartol 2014; Alcántara and Melgar 2016; Javaid and Iqbal 2017; Mohammed and Mohammed 2017; ISO/IEC27005 2018). ISO/IEC 27005 is simple in design; it discusses ISRM in the context of managerial process and complements with the widely accepted ISO 31000 risk management standard which makes it a rigorous and fully-integrated standard (Webb 2013).

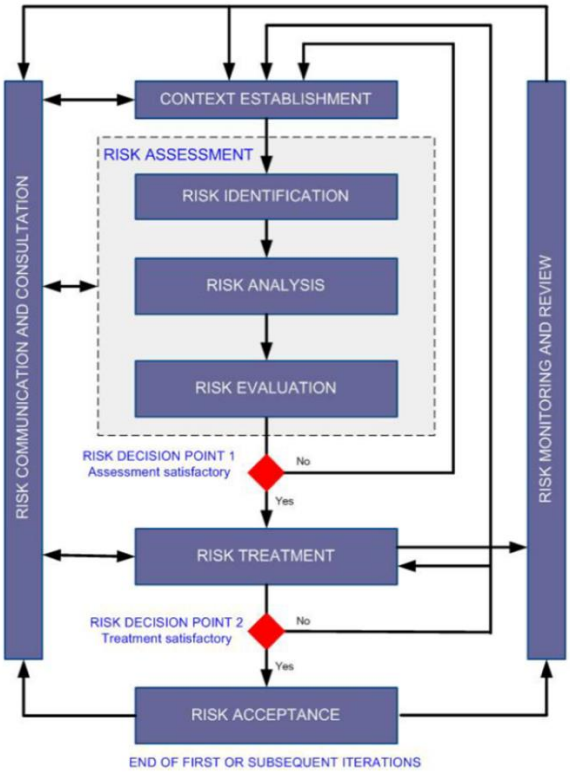

Figure 2.4 ISO/IEC 27005 ISRM Process

Source: ISO/IEC27005 (ISO/IEC27005 2018)

An ISO/IEC 27005 risk management process activity is shown in Figure 2.4. Context establishment involves ISRM basic criteria setting, scope and boundaries defining, and an appropriate organisation operating establishment. Risk assessment is comprised of identification, description, and prioritisation of risks against risk evaluation criteria. Risk treatment involves the selection of controls that may reduce, avoid, or transfer risks and the initiation of the risk treatment plan. Risk acceptance covers the decision to accept risks, recording, and justification of the accepted risks. Risk communication includes sharing of risk information among the decision-makers and other stakeholders within an organisation. Finally, risk monitoring and review involves the monitoring of risks and reviewing risks in case of changes in the context of the organisation (Tsohou et al. 2009; Agrawal 2017). Figure 2.5 provides an overview of the ISO/IEC 27005 standard that shows each of the activities based on the input and output.

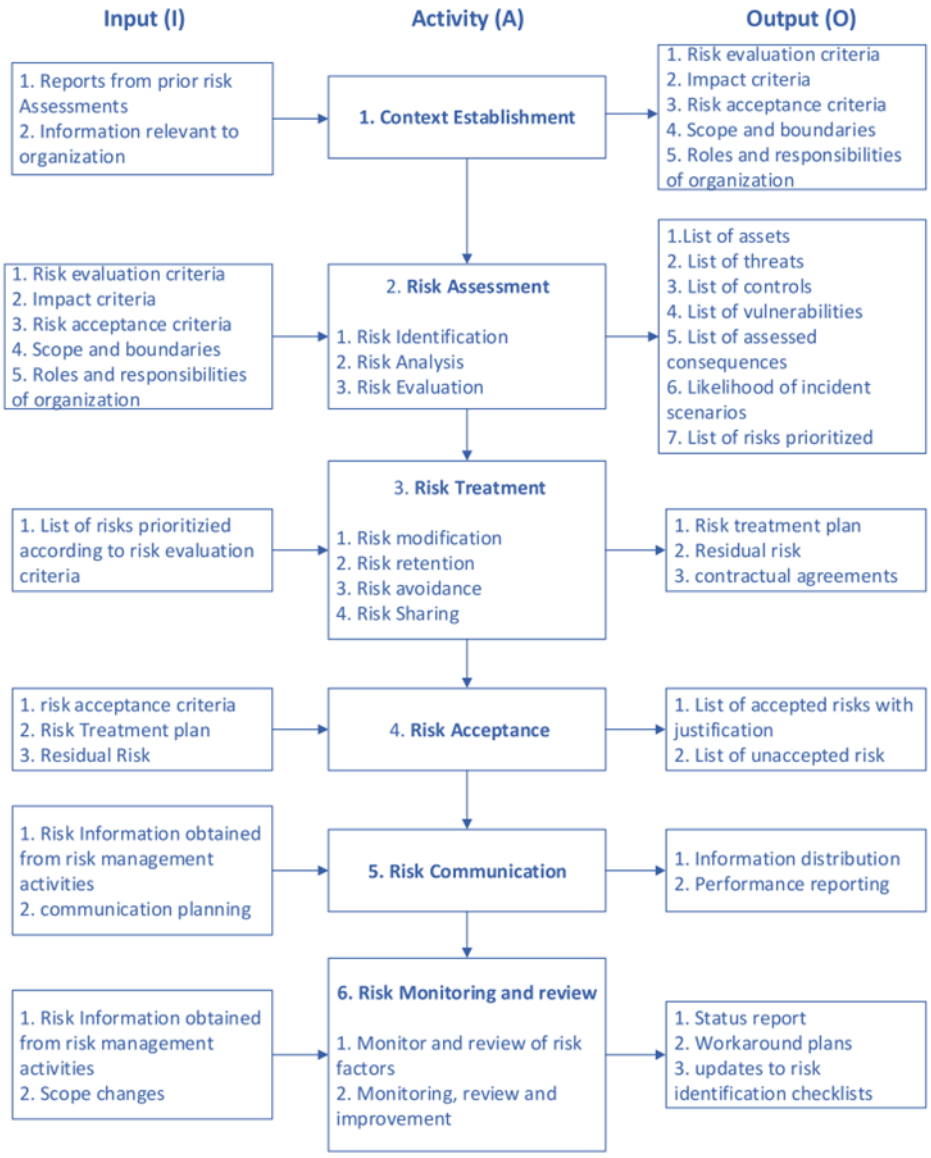

Figure 2.5 An overview of ISO/IEC 27005 Standard Activities

Source: Agrawal (Agrawal 2017)

While the main phases of the ISO/IEC 27005 standard are similar to NIST 800-39, the only difference is organisational aspects which include risk acceptance and risk communication phases (Fenz et al. 2014). Compared to popular ISRM standards such as NIST and OCTAVE, the ISO/IEC 27005 risk assessment approach differs in many aspects. Although ISO/IEC 27005 includes non-critical assets in the risk assessment domain, it requests assigning an asset value (Shanthamurthy 2011). In addition, ISO/IEC 27005 provides a framework to build a security culture that may have an impact on organisational operations and effectiveness (Calder and Watkins 2008; Beckers et al. 2014). Furthermore, while ISO/IEC

27005 defines the “what” and the “how” of the ISRM process, it avoids doing so narrowly. It defines a systematic and iterative process where actions are well-defined at each step, allowing organisations to customise their own procedures to produce effective results (Veltsos 2018).

It was argued that ISO/IEC 27005 provides a high-level framework that lacks operational level details (Al-Ahmad and Mohammad 2012; Javaid and Iqbal 2017). ISO/IEC 27005 does not provide a step-by-step guidance of information systems risk assessment and it requires an understanding of ISO/IEC 27001 and ISO/IEC 27002 for its implementation. In addition, it does not define any risk management implementation mechanism (Javaid and Iqbal 2017). Moreover, ISO/IEC 27005 does not provide an operational level comprehensive risk assessment method. According to Al-Ahmad and Mohammad (2012), it does not provide guidelines for the selection and prioritising of appropriate information systems controls (Javaid and Iqbal 2017). Likewise, Al-Ahmad and Mohammad stated that ISO/IEC 27005 is not intended to be a risk assessment methodology for information security. Its adoption as a means for ISRM is minimal. The standard consists of six annexes and with proper customisation, these annexes can be utilised as the primary assessment methodology for information security risks (Al-Ahmad and Mohammad 2013).

In the same manner, it is agreed that ISO/IEC 27000 series including ISO/IEC 27005 is the dominant information security risk management standard (Bartol 2014; Theoharidou et al. 2015; Barafort, Mesquida and Mas 2017), confirming that they are of high interest for practitioners in information technology settings as they integrate several process activities and implement mechanisms that link information technology and non-information technology entities of an organisation that has addressed risk management challenges. Furthermore, they promote standardisation benefits and risk management standards. Every year, ISO performs a certifications survey and the 2015 results showed that ISO is the leader of information security management certification standards (Barafort, Mesquida, and Mas 2017).

2.5.3 COBIT 5

Control Objectives for Information and related Technology (COBIT) was developed by

the Information Systems Audit & Control Association (ISACA) and regarded as one of the most widely adopted information security frameworks for risk management and IT governance (Al-Ahmad and Mohammad 2013; Javaid and Iqbal 2017; Labuschagne 2004). COBIT focuses on defining and developing IT control objectives, and is comprised of 34 processes which electively manage and control information security for organisations (Jakábová, Urdziková, and Mironovová 2013; Alcántara and Melgar 2016). COBIT can be adopted by organisations from different industry sectors, including education, financial institutions, government agencies, healthcare, and energy, among others. It is used to build the necessary alignment between business and information technology, enhances information technology processes, and establish the information security risk management (Al-Ahmad and Mohammad 2013; Alcántara and Melgar 2016).

The significant contribution of COBIT5 is the integration of people, process, and technology (PPT) of an organisation. It serves as a holistic framework for organisations' governance and risk management that creates business value from information technology infrastructure (Javaid and Iqbal 2017; Maneerattanasak and Wongpinunwatana 2017). Kannan (2016) stated that out of all the various frameworks and standards that are available in the market, COBIT5 is the only one that acknowledges the importance of ethics, culture, and behaviour in the achievement of organisation objectives (Kannan and Sivasubramanian 2016). In addition, it provides a framework of key controls and processes that identify the risks that organisations have decided to mitigate.

Some organisations use COBIT 5 to fulfil their compliance needs and requirements; for example, financial institutes implement COBIT 5 for internal information security audits and risk assessments. Other organisations use COBIT 5 to standardise information security processes and therefore increase maturity levels (Alcántara and Melgar 2016). Although COBIT 5 lays the foundation for a solid information security in organisations, it does not provide a methodology to perform information security risk assessments (Javaid and Iqbal 2017; Al-Ahmad and Mohammad 2013; Alcántara and Melgar 2016). In addition, it does not provide an information security risk assessment method. It only provides a reference for the second line of defence because it defines information security activities in a generic process (Pa et al. 2015). Moreover, COBIT 5 needs further content elaboration and updates for a successful implementation (Al-Ahmad and Mohammed 2015). The following section presents

a discussion on the challenges of ISRM.

2.5.4 Challenges in the Existing ISRM Frameworks

Okonofua, Rahman, and Ivanova (2019) argued that ISRM cannot be treated as an IT issue any longer; it is a serious component of organisational business practice. Various studies have shown that organisations face various challenges in a bid to have a successful and effective ISRM implementation (Al-Ahmad and Mohammad 2012; Marathamuthu 2015; Trajkovski and Antovski 2013; Wangen and Snekkenes 2013). These challenges are summarised as follows:

1. There are few studies that assist organisations in selecting the proper ISRM standard that fits their needs. For example, a few studies have been conducted to analyse some of the existing ISRM standards with limited recommendations (Al-Ahmad and Mohammad 2013; Wangen and Snekkenes 2013).

2. Resources allocation is another challenge. It was argued that ISRM standards require the existence of appropriate resources including qualified employees, budget, and technologies in order to have an effective risk management process (Trajkovski and Antovski 2013). Unfortunately, most organisations struggle to dedicate all required resources as a result of several limitations. For instance, automated tools for risk assessment are very costly for many organisations (Trajkovski and Antovski 2013). Wahlgren and Kowalski (2018) pointed out that a survey of ISRM practices showed that most organisations do not utilise automated applications for their risk management. Furthermore, there is both inadequate knowledgeable and a lack of skilled ISRM staff, and the available trainings are costly. Moreover, the required risk treatment investment is usually unaffordable, and thus organisations find the exercise frustrating (Al-Ahmad and Mohammad 2012; Trajkovski and Antovski 2013).

3. Existing ISRM standards provide instructions and guidelines that are too generic and do not take other factors into consideration (Al-Ahmad and Mohammad 2012; Al-Ahmad and Mohammad 2013; Flores, Antonsen, and Ekstedt 2014). Cultural differences among countries greatly influence the effectiveness and efficiency of IT deployment and

acceptance (Lin 2014). Many countries such as the United Kingdom, New Zealand, and Australia have developed their own national standards to overcome this problem (Mohammed and Mohammed 2017). It was suggested that each business culture in large organisations should create a single ISMS. For example, the policy and procedures for acceptable email and Internet usage or documenting policies should reflect the organisational culture (Calder 2006).

4. Complexity and a lack of guidance are two of the major ISRM challenges. Most standards provide general guidelines that are either not clear or too general. For example, COBIT's complexity limits its adoption in many organisations which have no expertise and low budgets for its implementation (Al-Ahmad and Mohammad 2012).

5. Absence of top management support is another challenge. The support of management is a key driver for the success of any information technology project including ISRM. The lack of management commitment could results in resources wasting, weak evaluations, and ignoring of risk assessment findings (Abu-Musa 2010; Marathamuthu 2015). Abu-Musa (2010) noted that information security risk is usually not well understood by the executive managers and boards of directors. Upper management has a perception that information security is a task of the information technology department; however, in most business and government agencies, it is the entire organisation's responsibility starting from the top management (AlKaabi 2014; Broderick 2001).

6. Another challenge is improper risk assessment management. Information security risk assessment is probably the most complex and challenging task. However, it is the most important step for the adoption of any ISRM approach as it finds potential security gaps and addresses the proper ways to avoid them (Susanto and Almunawar 2018). Trajkovski (2017) stated that organisation faces challenges in identification and evaluation of risk because it is not often considered as a task for the entire organisation, making most organisations complete it partially and only for important assets (Trajkovski and Antovski 2017b).

7. The ambiguity of language for describing threats is another challenge. Each ISRM standard or framework has its own vocabulary, and the same terminologies could mean

different things. For example, ISO/IEC 27005 defines a threat as a type of damage or loss; conversely, OCTAVE Allegro, another ISRM framework, defines the threat as either a human actor or a technical issue (Hallstensen, Snekkenes and Wangen 2017).

8. The last challenge is the existence of several ISRM approaches. The existence of many ISRM frameworks adds to the ambiguity and uncertainty of what is the most appropriate framework to use (Al-Ahmad and Mohammad 2012). However, some organisations provide a solution to this challenge using a hybrid approach by adopting the usage of more than one standard based on selecting which parts achieve the organisation's risk management objectives (Al-Ahmad and Mohammad 2013). For example, an enterprise could adopt ISO/IEC 27005 for risk management framework and NIST SP 800–30 for risk assessment complement guideline (Setiawan, Putra, and Pradana 2017).

2.6 The Influence of Culture in Information Security

The act of solely focusing on technology when planning information assets security and ignoring the people who could put organisations in a great risk. Studies have shown that employees are the greatest threat to an organisations' information assets. The majority of security breaches are created by employees' actions, whether intentionally or unintentionally (Govender, Kritzinger, and Loock 2016). People understand risks differently depending on the social structures to which they are exposed and the values embedded in them. This means that the values of certain social or cultural contexts shape an individual's perception and evaluation of risks. Therefore, values act as a filter in interpreting risk-related information; for example, individuals with environmental values will evaluate a given piece of information about the probability of accidents in nuclear power plants in a different manner compared to the supporters of nuclear power (Tsohou, Karyda, and Kokolakis 2015). Therefore, the culture which influences employees' behaviour and attitude is a vital contributor in information security for organisations (Govender, Kritzinger, and Loock 2016).

2.6.1 National Culture

Culture is a complex system of social behaviour based on the way people interact with their surrounding environment (Alkahtani, Dawson, and Lock 2013). It is shared norms and values between groups of people and represents the combination of the way of thinking, talking, and creating traditions, assumptions, language, art, literature, and feelings (Chu, Luo, and Chen 2018). According to Hofstede Hofstede, Hofstede, and Minkov (2005), culture is a mental software. Hofstede (1980) defined culture as "the collective programming of the human mind that distinguishes the members of one human group from those of others" (p. 24). Culture is viewed as a benchmark that differentiates different countries or regions. Accordingly, Hofstede developed one of the most established and accepted studies of cultural dimensions referred to as Hofstede's Dimension of Culture. The dimensions are based on holistic research carried out on 72 countries from 1967 to 1973 (Govender, Kritzinger, and Loock 2016). Hofstede identified four cultural dimensions that include power distance, uncertainty avoidance, individualism/collectivism, and masculinity/femininity (Hofstede, Hofstede, and Minkov 2005). The other two dimensions which are long-term orientation and indulgence/restraint were added to the cultural dimensions list a few years later (Hofstede 2011; Chu, Luo and Chen 2018).

Culture is a crucial factor that has been recognised in literatures on cybersecurity risk (Henshel et al. 2016). Studies have shown that national culture has significantly contributed on employees' behaviour, including their behaviour towards information security (Alumaran, Bella, and Chen 2015). There are many cultural factors that may contribute to unsuccessful applications of information security including language, poor infrastructure, and lack of strategic guidance and funding.

National culture directly influences employees' learning ability, which, in turn, impacts organisational innovation and growth (Chu, Luo, and Chen 2018; Looso, Goeken, and Johannsen 2011). Due to this, some information technology specialists analyse employee's different characteristics—including culture—in implementing information security activities (Looso, Goeken and Johannsen 2011) because nations foster powerful initiatives towards the consolidation of language, education, laws, media, economy, and politics. However, some organizations' upper management can be less influenced by national culture than other

members of staff. However, the influence of national culture on the employees does not change over time (Govender, Kritzinger, and Loock 2016).

Schmidt et al. (2008) stated that national culture influences all employees of an organisational as well as management perceptions and privacy-related issues. Each country has different perceptions of relevant information security threats (Schmidt et al. 2008; Xie et al. 2012). In developing countries, for example, technology-based applications such as e-government are highly influenced by national culture (Govender, Kritzinger, and Loock 2016). In addition, Al Omoush, Yaseen, and Atwah Alma'aitah (2012) argued that Arab cultural beliefs are great predictor of information technology transfer resistance. Therefore, enhancing employees' security culture can have a positive and direct influence on the entire organisations security culture (Govender, Kritzinger, and Loock 2016; Hain 2011).

More specifically, Petrescu (2019) argued that organisational culture undoubtedly influences risk management strategy. Therefore, risk management of information security should be correlated with organisational culture for better information security posture. For example, risk analysis treatment programs should involve major changes in an organisation, and these changes must be managed and understood in order to affect an entire organisation. The change may involve the alignment of personnel, processes, and procedures with the organisation's objectives (Petrescu and Sîrbu 2019). Organisational culture is the employees' or stakeholders' values, assumptions, beliefs, and attitudes that they utilise to interact with their organisation's systems and procedures (Ashenden 2008), which implies that organisational culture refers to practices or perspectives of the national culture (Tang, Li, and Zhang 2016).

Employee's behaviour can be correlated by national culture and organisational culture in which national culture influences employees more than organisational culture. Therefore, the awareness of the importance of national culture is vital for better prediction of employee behaviour. Ethical, national, and organisational cultures influence every individual in all organisations; this affects the way they understand the meaning and importance of information security. It is crucial to fully understand the complexity of organisational culture which influences the security culture (Alnatheer 2015). Accordingly, in order to develop an effective information security culture, national culture and organisational culture should be

considered (Dols and Silvius 2010; Lim et al. 2009). For example, organisations which integrate their information security activities with their information security culture could potentially influence their employees for better actions and behaviours towards information security assets (Lim et al. 2009).

2.6.2 Information Security and Culture

In an organisational context, it has been argued that employees are the weakest point in an information security chain due to their security behaviour when dealing with information assets. As discussed earlier, organisational culture and the national culture are the main contributors to the employees' behaviour (Akhyari, Ruzaini, and Rashid 2018).

National culture influences the way information is processed and protected within organisations and therefore affects the information security culture (Veiga and Martins 2017). It has been found that information security behaviour is influenced by national culture values and beliefs (Chaula, Yngstrom and Kowalski 2006). As a result, it has been recommended that there is need to establish a positive information security culture (ISC) using guidelines that influence employee's behaviour towards information security in order to improve the organisation's security posture (Akhyari, Ruzaini and Rashid 2018). It has been indicated that ISC, which is a part of organisational culture, should guide employees' behaviour when interacting with information technology assets. This guidance improves employees' awareness and prevents improper actions which may expose the organisation's assets to security risks (Alassafi et al. 2016; Alnatheer 2015).

Studies have shown that regulations alone are not enough to maintain information security in organisations, but culture that develops and encourages good security-related behaviour through values continues learning as well as assumptions are more effective than regulations which mandate employees' behaviour. It is clear that in order to have effective information security, employees should understand, accept, and follow the necessary precautions (AlHogail 2015). Several studies have revealed that if the ISC is not robust within an organisation, then strong information security measures will be insufficient and can potentially compromise the organisation's information security assets (Fredrik, Joachim, and Martin 2015; Govender, Kritzinger, and Loock 2016). Alassafi (2016) added that the

implementation of effective ISC can support organisational effectiveness in which the information security is normal part of the employees' daily activities. In addition, ISC supports the execution of effective information security policies in an organisation (Alassafi et al. 2016). Successful ISC Implementation may play a significant role in enabling employees to act as a "human firewall" to protect their organisations (AlHogail and Mirza 2014).

Veiga and Martins (2017) noted that there are many factors that influence information security culture in organisations which include management support, information security policies, training, and awareness and change management; however, national and organisational culture are the most influential factors. Furthermore, it was argued that organisations should ensure that culture is integrated between organisational strategies and adopted information security standards (Calder 2006).

However, Govender, Kritzinger and Loock (2016) argued that regardless of the high recommendations by the scholars, it is not clear that guidelines are available to establish ISC which will effectively influence employees' information security behaviour. Current guidelines and standards for establishing Information Security Management such as ISO/IEC 27001 do not consider ISC, and also cannot assure its effectiveness in employee's security behaviour. Moreover, regardless of the number of ISC related studies, there is yet no clear and comprehensive methodology that can be used as ISC practical guidelines for organisations (Govender, Kritzinger, and Loock 2016).

2.7 Information Security Risk Management in Saudi Arabian Organisation

This section develops an idea of the characteristics of ISRM in Saudi Arabian organisations. It highlights current practices in order to determine the national conditions that might either facilitate or impede the effectiveness of the international ISRM standards and best practices.

2.7.1 Saudi Arabia Profile

Saudi Arabia, officially known as the Kingdom of Saudi Arabia (KSA), is situated in Southwest Asia or the Middle East and occupies most of the Arabian Peninsula, bordering the

Arabian Gulf in the east and the Red Sea in the west. The Kingdom is ruled by a large Al-Saud family with Islamic Sharea lines (Talib et al. 2018; The World Factbook: Saudi Arabia). Saudi Arabia is the second-largest country in the Middle East and North Africa "MENA" with approximately 2,150,000 km2 landmass and a population of approximately 34.2 million (The Total Population in 2019 2019; Internet World Stats 2019). The official language is Arabic; however, English is widely adopted as many of non-Arab expatriates work in various professions and industries across the country (Zahrani 2018). Table 2-2 provides a summary of socio-economic indicators of Saudi Arabia.

Table 2-2 The Global Competitiveness Index: Saudi Arabia Performance Overview

Key Indicators (2019)	Rank/137
Global Competitiveness overall Index ranking	36th
Innovation capability	36th
Institutions	37th
Infrastructure	34th
Macroeconomic stability	1th
Health	58th
Skills	25th
Market size	17th
Financial system	38th
ICT Adoption	38th
Product market	19th
Business Dynamism	109th

Source: (*The Global Competitiveness Report 2019* 2019)

Saudi Arabia is one of the fastest-developing countries in the Middle East and has had a massive growth in the use of communication technologies in the last few years (Alotaibi et al. 2016; World Economic Situation and Prospects 2017 2017). In 2022, it is estimated that approximately 93 percent of the population—more than 30 million users—will have access to the Internet (Internet User Penetration in Saudi Arabia 2021). This high demand for Internet services is a result of a high use of social media applications and gaming applications, as well as video streaming and downloading (Telecommunication Indicators in the Kingdom of Saudi Arabia by the End of Q3-2017 2018).

2.7.1.1 Economy

From an economic perspective, Saudi Arabia relies heavily on oil and owns more than 22 percent of the world's oil reserves, according to the Organisation of the Petroleum Exporting Countries OPEC (Opec Share of World Crude Oil Reserves 2019; Moshashai, Leber, and Savage 2020). It is ranked as the largest exporter of oil and plays a leading role in OPEC. The oil sector accounts for about 87 percent of the country's revenue and 90 percent of export earnings (The World Factbook: Saudi Arabia 2021). It is also ranked as one of the richest countries in the world (Alqahtani, Goodwin, and de Vries 2018).

Saudi Arabia enjoys a buoyant economy with a GDP of USD 792.9 billion and an annual growth of 0.3 percent in 2019 (Saudi Arabia: Gross Domestic Product 2021; Saudi Arabia GDP). However, the exceptional dependence on oil revenue has led to major problems; for instance, the drop in oil prices affects the Saudi economy resulting in cuts in subsidies and other government expenditures. Thus, the country has started implementing several efforts to diversify its economy to non-oil sectors such as manufacturing, among others. In addition, Vision 2030 has been put into effect to cushion the economy with a reform plan known as the National Transformation Plan (NTP), which provides the roadmaps for its achievement based on milestones (Alqahtani 2018; Hathaway, Spidalieri, and Alsowailm 2017; Moshashai, Leber, and Savage 2020). It is a long-term economic blueprint developed to reduce the dependence on crude oil revenue. The initiative will have a direct influence on all aspects of the Saudi economy by outlining the regulation, budget, and policy changes. The main goal is to boost non-oil government income from USD 43.5 billion to USD 267 billion by 2030 (Alqahtani 2018; Alassafi et al. 2017; Envisioning an Ict Led Approach to the National Transformation Program for the Kingdom of Saudi Arabia 2016; Moshashai, Leber, and Savage 2020).

2.7.1.2 Saudi Arabian Culture

Saudi Arabia is a very traditional country where Islamic values and Arabian culture play a major role in Saudis' behaviour. The population is based on an ancient desert society and has the most homogenous population in the Middle East, with almost all Saudis being Arabs and Muslims (Al Asmri 2014). In Saudi Arabia, Islamic values and Arabian culture have a

stronger influence than Western culture by the enforcement of their social norms and common beliefs on people (Maghrabi and Palvia 2012). Islam influences Saudi's culture by defining the traditions, obligations, and societal practices.

In addition, tribal and kinship systems influence the place of the people in society and could potentially affect their success, and is also considered to have major impacts on the workplace (Aldraehim et al. 2012). The importance of family has been emphasised by the Muslim's holy book, the Koran, with self-interest coming after the family interests in Saudi society (Aldraehim et al. 2012; Zahrani 2018). As part of the strong values towards family collectivism, managers are expected to provide employment opportunities and privileges to family members and relatives (Aldraehim et al. 2012). Moreover, Saudi Arabian culture has a deep sense of tradition and history; thus, people have closer and stronger connections over time (Maghrabi and Palvia 2012). Moving alongside traditional and Islamic values, Saudis face the challenges of modernisation of Western technology that could impact their culture and Islamic values (Al Asmri 2014). Saudi Arabian culture is fairly homogenous, like many Middle Eastern nations. Business leaders and managers face challenges in a bid to improve organisational performance as a result of cultural issues and work compared with those in Western and international companies (Idris 2007).

According to Hofstede as cited in Maghrabi and Palvia (2012), Saudi Arabia scores high on the dimension "uncertainty avoidance" reflecting how the people as a whole are not ready to accept change (Maghrabi and Palvia 2012). In addition, it has been characterised by a high "power distance" which indicates that a hierarchical order is dominant in the society (Saxena 2018; Maghrabi and Palvia 2012). Saudi Arabian organisations hierarchy "is seen as a reflection of inherent inequalities, where centralisation is popular, subordinates expect to be told what to do and the ideal boss is a benevolent autocrat" (What About Saudi Arabia? 2019, p. 1). On the other hand, "individualism" is rare and is considered a factor in a collectivistic society. In the same manner, loyalty is paramount as it overrides other societal rules and regulations (Maghrabi and Palvia 2012).

In collectivist societies, employment and promotion decisions are perceived in moral terms (Hofstede 2019). Collectivism would potentially shape people's beliefs and behaviours regarding the adoption of information technology and interaction (Maghrabi and Palvia

2012). Additionally, it indicates that the society "will be driven by competition, achievement and success, with success being defined by the winner which starts in school and continues throughout organisational life" (What About Saudi Arabia? 2019, p. 1). Finally, Saudi Arabia scores low on the "long-term orientation" dimension. It was indicated such societies would "have a strong concern with establishing absolute truth; this means they are normative in their thinking. They exhibit great respect for traditions with a relatively small propensity to save for the future, and a focus on achieving quick results" (What About Saudi Arabia? 2019, p. 1). This explains the reasons that Saudi people have normative thinking and a high respect for traditions with more focus on obtaining quick results and a lower tendency to save for the future (Alzeban 2015; Saxena 2018).

Bjerke (1993) conducted a comparison study between Saudi and United States' culture based on Hofstede's dimensions, and the findings revealed that there are major cultural differences between the two nations. Thus, majority of management theories developed in the United States may not be applicable to the culture of Saudi Arabia. This can be applied to most of the business management theories developed in Western countries that are inadequate in the setting of a developing country like Saudi Arabia (Bjerke and Al-Meer 1993). In a similar manner, Aldraehim et al. (2012) argued that Saudi culture emphasises the importance of home, traditions and its influence on information technologies.

2.7.1.3 ICT

One of the key enablers and driver of the Saudi Vision 2030 is technology (Rizvi, Roudev, and Lyons 2019; Saira and Jhanjhi 2020). As a result, Saudi Arabia has the largest and fastest-growing ICT sector in MENA and plans to develop a national digital infrastructure to boost the related sectors and industries. This includes the digitisation that will play a role in achieving the National Transformation Plan (NTP) milestones (*Envisioning an Ict Led Approach to the National Transformation Program for the Kingdom of Saudi Arabia* 2016; Alassafi et al. 2017; Rizvi, Roudev, and Lyons 2019). Meanwhile, Saudi Arabia is continuously working to modernise its ICT infrastructure to achieve a higher level of digital maturity of e-government services. Saudi Vision 2030 aims to digitise the government, boost its economy, and establish a digital society by creating a globally competitive ICT hub. Currently, the Saudi National Portal

provides about 2,500 e-government services for 70 government agencies (Saira and Jhanjhi 2020).

Furthermore, it is expected that the usage of information technology and digitisation will accelerate the execution of Saudi Vision 2030 and the NTP programs, and plans will be helpful in improving the economic (*Envisioning an Ict Led Approach to the National Transformation Program for the Kingdom of Saudi Arabia* 2016; Alassafi et al. 2017; Rizvi, Roudev and Lyons 2019; Saira and Jhanjhi 2020).

As such, Saudi Arabia is aware of cybersecurity threats as its economy becomes more digitised (Rizvi, Roudev and Lyons 2019). Therefore, a sound information technology security plan should be aligned with the Vision 2030 and enforced in NTP in order to achieve it. The National Cybersecurity Authority (NCA), founded in October 2017, is a government security entity responsible for matters pertaining to cybersecurity in Saudi Arabia and reports directly to the Saudi Arabian King (About NCA 2020; Rizvi, Roudev and Lyons 2019). Both government entities and private companies which provide national infrastructure are required to comply with the NCA's cybersecurity controls (Rizvi, Roudev, and Lyons 2019).

In addition, government entities must implement the Communications and Information Technology Commission (CITC) information security policy framework, which helps in managing information security risks (Rizvi, Roudev, and Lyons 2019). CITC is a government entity for policies, laws, legislation, and regulation that coordinates all concerned parties, including investors, providers, and customers (Ajmi et al. 2019). In addition, this body is in charge of regulating the internet and the national firewall which blocks access to sexual and political website content (*Saudi Arabia Information Technology Report - Q1 2015* 2015).

2.7.1.4 Political Conflicts and Cybersecurity

Saudi Arabia is one of the most targeted countries in the Middle East in terms of unity, decision-making, and security. It has been involved in many wars against terrorism and the protection of national security. However, Saudi Arabia is known for its religious and political weight and its strong economy, which makes it a target by those who wish to influence its stability (Al Amro 2017). Saudi Arabia's former oil minister, Khalid Al-Falih, stated that:

> I am concerned though about the security of oil supplies from threats from state and non-state actors that we've seen. We've seen ships being attacked, we've seen pipelines being attacked, we've seen drones being launched from militias that are agents of Iran and putting the global energy supply at risk. (Jones 2019, p. 1)

The United States has sent approximately 500 soldiers to one of the Saudi Arabia's air bases and sent other manned and unmanned intelligence and surveillance to the Middle East to counter Iran and protect Saudi Arabia (Jones 2019).

Tensions among Saudi Arabia and some of its neighbouring countries such as Iran, Yemen, and Syria have escalated in recent years (Perlroth and Krauss 2018). The confrontation between Saudi Arabia and Iran has greatly played itself out in Yemen and Syria during the last few years, and the conflict has drifted to the cyber (AboulEnein 2017; Kshetri 2016; Perthes 2018; Perlroth and Krauss 2018). Iran poses a potentially serious threat to oil facilities in the eastern province of Saudi Arabia (Saudi Arabia Oil Facilities Ablaze after Drone Strikes 2019). It has been argued that Iran will likely rely on irregular and unconventional means and actors, including cyberattacks, and utilise its allies like the Houthis in Yemen to conduct attacks. Cyberattacks provide unlimited range, virtually, and low attribution which is very attractive for the Iranians which enhance plausible deniability and the sabotage of other operations (Al Amro 2017; Jones 2019).

Saudi Aramco, the national petroleum and natural gas company, has made a significant progress in protecting its infrastructure; however, the threat of Iran and its allies remains a serious challenge (Jones 2019). A partial disruption of production facilities would have a significant impact on oil prices. On 14 September 2019, the Abqaiq facility in Saudi Arabia, the largest crude oil stabilisation plant in the world, was attacked by targeted drones and missiles, causing major damage. Approximately half of the facility's oil output was shut down for a few weeks as a result of the attack. Houthi, Yemen's Iran-aligned rebels, claimed responsibility for the attacks (Saudi Arabia Oil Facilities Ablaze after Drone Strikes 2019). Moreover, Saudi Arabia's wealth makes it an attractive, financially motivated cybercrimes target. In light of this, Kshetri (2016) argued that cyberthreats confronting the energy sector as a result of the lack of sufficient security awareness of such threats are very serious and problematic.

2.7.2 Information Security in Saudi Arabia

Saudi Arabia is the largest Information and Communications Technology (ICT) market in the Middle East in both capital volume and spending (Saudi Arabia - Information and Communications Technology 2018; Hathaway, Spidalieri, and Alsowailm 2017). In 2019, Saudi Arabia's ICT spending rose to USD 34.5 billion (Manek 2019). The compounded annual growth rate (CAGR) of 16.6 percent is expected between 2020 and 2023 (Alwazir and Dichter 2020). The Saudi Arabia ICT market also represents over 51 percent of the total Middle East market (Alqahtani 2018; Manek 2019). Saudi Arabia has initiated a 20-year ICT plan to support the adoption of technology and telecommunications across households and businesses in the country, and has embarked on a massive ICT infrastructure programme which will turn Saudi Arabia to a regional information technology powerhouse. Rapidly increasing ICT projects to modernise the country's infrastructure, including e-government and the liberalisation of the telecommunication industry, have shown a massive improvement in usage, competition and service levels (Saudi Arabia - Information and Communications Technology 2018). Yet, the ICT market in Saudi Arabia is considered to be import-driven with more than 80 percent of ICT products and services owned and controlled by foreign companies (Hathaway, Spidalieri, and Alsowailm 2017).

Saudi Arabia transformed into IT-based society since the adaption of computers and Internet services in 1997 (Ajmi et al. 2019). The usage of computers became a norm at public and business levels by 2007. In 2005, the Communication and Information Technology Commission (CITC), which is the Saudi Arabian regulatory body for technology and communication services, was established to regulate the information technology procedures and implement policies and laws enacted by the government in Saudi organisations. It is the key contributor to the transformation vision of Saudi Arabia, significant in achieving the Saudi goal of providing universally available and affordable ICT services of high quality (Ajmi et al. 2019; About CITC 2019).

Saudi Arabia has addressed cybersecurity issues through recently launched programs, which are The National Cyber Security Agency (NCA) and the Saudi Arabia Federation for Cybersecurity, Programming & Drones (SFCPD) (Iqbal and Khan 2019). Public and private organisations are now required to comply with the NCA's essential cybersecurity controls.

Additionally, it must implement an information security policy provided by the CITC to assist Saudi organisations in managing their information security risks (Rizvi, Roudev, and Lyons 2019). On the other hand, SFCPD is a government initiative with a goal to develop professional competences in the field of cyber security and programming in compliance with international standards. The objective of this institution is to increase the level of cyber defence capacity of Saudi Arabia to that of developed countries. Recently, many competitions and hackathons were organised by SFCPD to promote the cybersecurity profession across Saudi Arabia (Iqbal and Khan 2019).

Another key legislation is the recently approved E-Commerce law. The E-Commerce law, published in July 2019 and effective October 2019, is designed to regulate and oversee transactions conducted online in order to restrain online fraud and boost economic growth (Alzamil 2018; Wright 2019). However, after being affected by Iranian cyberattacks, Saudi Arabia has pursued enhanced cybersecurity strategies in order to protect its infrastructure (Ajmi et al. 2019). Furthermore, in May 2017, the Saudi Arabian Monetary Authority (SAMA) developed the SAMA Cyber Security Framework (CSF) in order to improve SAMA-regulated organisations information security and resilience against cyberthreats (Diab 2019). Financial institutions including banks, insurance and reinsurance companies, and finance companies regulated by SAMA are required to comply with the SAMA cybersecurity framework (Rizvi, Roudev and Lyons 2019).

Saudi Arabia was ranked 13th globally out of 175 countries in the Global Cybersecurity Index (GCI) in 2018, an increase of 33 spots, and the first on regional level according to the International Telecommunication Union (ITU) (Geronimo 2019). However, with Saudi Arabia aiming at its 2030 vision and making effort towards digital transformation and growth in GDP, cyber security is crucial for the country's success. It is the major cyber conflicts target in the region as a result of the high economic activities, digital transformation, high adoption of technology and skyrocketing sales in the oil and petrochemicals industries (Hakmeh 2017; Alelyani and Kumar 2018). Alshammari and Singh (2018) added that Saudi Arabia is both the prime target and the worst victim of cybercrime in the Gulf region.

In a similar manner, the geopolitics and wealth of the country makes cyberattacks likely to happen with malicious actors trying to create social unrest, obstruct oil production, or for

financial theft (Talib et al. 2018; Wright 2019). It has been confirmed that the large number of strategically important companies operating in Saudi Arabia makes it an attractive target for cyberattacks (SPONG 2018). Government agencies and businesses in Saudi Arabia face exceptional challenges as a result of the increase of sophisticated cyberattacks by foreign governments and hacker activists (Ajmi et al. 2019). Alarifi (2012) stated that Saudi Arabia is among the top levels of information security protection (Alarifi, Tootell, and Hyland 2012). Moreover, Alsmadi (2018) argued that some Middle Eastern countries are in a maturing stage in cybersecurity such as Oman, while many others are still in initiating stage such as Saudi Arabia (Alsmadi and Zarour 2018).

Menachery (2018) indicated that Saudi Arabia has been categorised as a high-risk country according to the Kaspersky Security Network statistics in 2018 with more than half of the Industrial Control System computers attacked by malware. Furthermore, in Middle Eastern countries, including Saudi Arabia, ransomware ranked first on the list of top malware with 29 percent, compared to 7 percent of global malware (Sawada 2018). It was found that 1 in 175 emails in Saudi Arabia is blocked as malicious compared to 1 in 412 in the global average (SPONG 2018). The National Centre for Cyber Security reported approximately 160,000 daily cyberattacks in Saudi Arabia (Ajmi et al. 2019). Al Amro (2017) indicated that approximately 6.5 million Saudi Arabian residences were affected by internet crime in 2016.

Another report by Ponemon Institute and IBM found that the average data breach cost for Saudi Arabia and Emirates is $6 million compared to the global average of $3.86 million and ranked second worldwide (*Cost of a Data Breach Report 2019* 2019). Moreover, Saudi Arabia is ranked top of the list on the largest average number of breached records with 38,800 records compared to the global average of 25,575 records (*Cost of a Data Breach Report 2019* 2019). In addition, Saudi Arabia and Emirates have the world's longest length of data breach lifecycle, with an average of 381 days compared to global data breach lifecycle with an average of 279 days (Gibbon 2019; *Cost of a Data Breach Report 2019* 2019).

According to a Kaspersky Lab report, around 60 percent of organisations in Saudi Arabia experienced virus and malware attacks in 2017 ("Study: 60% of Saudi Institutions Hit by Virus Attacks, Malware" 2018). Another report by Symantec, the Internet Security Threat Report 2019 (ISTR), revealed that Saudi Arabia is at high risk and topped the list of malicious email

rate and email phishing rate by country (O'Gorman 2019). Finally, the 2019 cyber threat defence report by Cyber Edge Group showed that Saudi Arabia tops the list of the countries that are most affected by ransomware, followed by Turkey and China (*2019 Cyberthreat Defense Report* 2019). Saudi Arabia's National Cyber Security Centre (NCSC) 2017 report revealed that as a result of the geopolitical situation, most of the threats were directed to government sectors, oil and gas sectors, and petrochemical and telecommunication sectors, which are very important to national economy (Alabdulatif 2018). Cybercrime attacks cost Saudi Arabia's economy up to $8 billion by the end of 2020. Cybercrime targeted at Saudi Arabia continues to increase than most of the countries in the world (Biscoe 2018); (Bell 2018).

Saudi Arabia has been exposed to damage from politically motivated cyberattacks during the last few years. For instance, Saudi Arabia's political conflicts with Israel, Iran, Syria, and Yemen have significantly contributed to deadly cyberthreats (AboulEnein 2017; Ajmi et al. 2019; Kshetri 2016). As reported by Bitdefender in June 2020, a sophisticated attack targeted critical Saudi Arabian organisational infrastructure, including air transport and government agencies by Iranian groups. Since 2018, the attackers have managed to access their targets and went undiscovered for more than a year and a half with the goal of data exploration, exfiltration, and espionage. The attacks involved the use of social engineering by tricking targeted victims to run a remote administration tool in which the attacker activity occurred on the weekends (Lakshmanan 2020; Arsene and Rusu 2020).

Although there are no statistical reports that truly disclose security incidents and data breaches in Saudi Arabia, threats are increasing and occur at all levels (Alzamil 2018). Hakmeh (2017) confirmed that there is no reliable data that disclosed the incidence of cyberattacks; however, news reports and statements by government officials indicate that the problem is increasing. Some of the significant data breaches and cyberattacks in Saudi Arabia are as follows:

1. The Saudi ARAMCO Oil Company was struck by a significant cyberattack in 2012 in which more than 30,000 computers were hit by a devastating virus called "Shamoon." The data on the computers were destroyed and hard drives were wiped clean with the aim of stopping oil production (Elnaim 2013). Data regarding production and drilling were

lost, as well as the company's management offices information across the country and in some overseas offices. The Advanced Research Centre was also affected (Bronk and Tikk-Ringas 2013). Shamoon is considered the most significant cyberattack on the oil industry. Some studies argued that it is equivalent to an attack against Saudi Arabia because it took more than two weeks to partially recover from the attack, which cost Saudi ARAMCO millions of dollars (Aldosari 2019; Kshetri 2016).

2. A group called Cyber of Emotion hacked 24 government agencies websites within two hours in August 2015. The hackers warned the administrators that their websites lacked adequate security prior to the hack and asked them to enhance their security. These websites included municipalities, education departments, hospitals, and health departments (Alshammari and Singh 2018).

3. Four years after Shamoon, one of the most destructive data erasers—an updated version of it called Shamoon 2—struck Saudi Arabia again, but this time in three waves. The first was on 17 November 2016, the second one was on 29 November 2016, and the final strike was on 23 January 2017. News reports revealed that 15 government agencies and private organisations were affected by Shamoon 2 (Alshammari and Singh 2018). These organisations include Sadara Chemical Co (a joint venture company owned by Saudi Aramco), Dow Chemical, and Saudi Telecom Company (STC). They experienced a network disruption and their computer hard drives were erased as well (Shamseddine 2017).

4. National Industrialisation Company Tasnee's computers were shut down in January 2017 in a similar occurrence to Aramco attack in 2012. In this instance, the company's computers hard drives were destroyed and data were lost. Tasnee hired information security experts from Symantec and IBM to analyse the attack (Krauss 2018). Reports indicated that there should be a complete overhaul of the company's security standards in order to prevent future attacks (Perlroth and Krauss 2018).

5. In August 2017, a petrochemical company in Saudi Arabia was hit by another sophisticated cyberattack. The attack was designed to sabotage operations and trigger an explosion. A mistake in the attackers' code prevented the explosion that would have

killed a sizeable number of people (Groll 2017; Perlroth and Krauss 2018).

6. A variant of Shamoon struck Saudi Arabia in December 2018. The attackers targeted SAIPEM's servers in Saudi Arabia. Reportedly, it was uploaded to the Industrial Control Systems and spread over the network to all connected computers and then irreversibly encrypted all data on infected computers' hard drives (Quadri and Khan 2019).

2.7.3 ISRM Compliance in Saudi Arabian Organisations

It was noted that most organisations adopt information security standards to achieve compliance with internal/external regulations and corporate government rule that would eventually improve their information security posture, leading to an enormous gap between the required information security standards implementation and the actual implementation by organisations (Telekomunikasi 2014). A few studies have been carried out on the information security management standards in Saudi Arabia (Alshitri and Abanumy 2014; Alzamil 2018). Alzamil (2012) reported that the available studies indicated that Saudi Arabian organisations focus more on information security technologies rather than the human aspect in a bid to protect information assets from any vulnerability that could lead to possible data breach or attacks, which represents an ineffective ISRM implementation (Alzamil 2012).

Nabi, Mirza, and Alghathbar (2010) conducted a survey on organisations in Saudi Arabia, including government agencies, defence, banks, and private enterprise, to evaluate the current state of information security. The result showed that 20 percent of these organisations are ISO 27001 certified. The results further revealed that 50 percent of the organisations follow a risk-assessment process and procedure. The results also showed that approximately 30 percent of organisations do penetration testing, a technique used to determine information security control's effectiveness and process of risk assessment (Nabi, Mirza and Alghathbar 2010). The ISO 27001 certificates survey (2020) indicated that out of 36,362 ISO 27001-certified companies around the world, there were only 97 Saudi Arabian certified companies in 2019 (*The Iso Survey 2019* 2020).

Alshitri (2014) urged that Saudi Arabia is not mature enough in terms of quality practices and organisational culture required to implement management system standards. The

author's argument relies on the different environment in which the systems and practices are "hostile to its teaching" (Alshitri and Abanumy 2014, p. 1). AbuSaad et al. (2011) studied 8 out of 13 ISO 27001 certified Saudi Arabian organisations and concluded that during the ISRM implementation phase, identifying the organisation's assets and team's lack of experience are the major obstacles. Moreover, the primary reason for adopting the ISO 27001 standard was enhancing the organisation's security in order to gain competitive advantage (AbuSaad et al. 2011).

Organisations may encounter difficulties in complying with information security standards as many information security compliance projects such as ISO 27001 fail and may cause the loss of billions of dollars (Susanto and Almunawar 2018). Alshitri and Abanumy (2014) conducted a study on Saudi organisations to determine why there is a low adoption of information security standards. The study revealed that the reasons for the low adoption of information security standards are human resources and management issues. This includes a lack of information security expertise, a lack of training and awareness programs, and a lack of local good quality consultants, among others. Another study by AbuSaad et al. (2011) which investigated eight ISO 27001 certified Saudi organisations revealed that more than 60 percent of interviewed respondents stated that managing information systems are not audited in Saudi Arabian organisations.

2.8 Factors Influencing ISRM in Saudi Arabia Organisations

People, process, and technology (PPT) are the main elements for organisational process improvement (Prodan, Prodan, and Purcarea 2015). PPT is considered one of the key elements that influences the effectiveness of ISRM in any organisation. This approach focuses on these three areas in order to enhance the overall improvement of organisation (Prodan, Prodan, and Purcarea 2015; Billings 2018). ISRM practices need to be aligned with the business objectives of organisations and applied at business processes, people, and technology of the organisation. Ignorance of some aspects may make it less effective or even cause a faulty outcome that would have serious consequences on the activity of risk management and return of investment (ROI) for any organisation (Javaid and Iqbal 2017). A limited number of studies have explored the information security practices within the Saudi

Arabian context (Alzamil 2018). The following subsections discuss the factors that influence ISRM in Saudi organisations, which would help in developing the initial conceptual model for this research.

2.8.1 People

People are crucial for the successful implementation and maintenance of risk management in an organisation. The people element is crucial as risks management cannot be fully automatised without the people. Trained teams, adequate understating of the risk culture, and the right mix of representatives are important for successful ISRM in organisations (Trajkovski and Antovski 2017a). Leveraging more people and processes and less technology is important for achieving better security. This can be accomplished by improving security awareness, providing security-specific training regularly, and improving the security culture within the organisation (Nicastro 2006).

2.8.1.1 National Cultural

Focusing on technology and ignoring people when planning information assets security could put organisations at a great risk. Studies have shown that employees are the greatest threat to an organisation's information assets. The majority of security breaches are created by employees' actions, whether intentionally or unintentionally (Govender, Kritzinger, and Loock 2016). Culture is one of the main information security standards adoption criterions (AlHogail and Mirza 2014; Alkahtani, Dawson, and Lock 2013; Übelacker 2013). Protecting important assets is directly influenced by national culture and, thus, the decisions of implementing an information security management standard such as ISO 27001 is influenced by culture (Fomin, Vries, and Barlette 2008). AbuSaad (2011) argued that different cultures have a positive or negative impact on the selection and implementation of standards (AbuSaad et al. 2011), which could be as a result of cultural conflicts and diverse cultural values between the management style of Western countries and Saudi business leaders and their employees (Aldraehim et al. 2012).

Cultural factors tend to be obstacles and can affect the adoption of information security standards and practices in Saudi Arabian organisations (Alnatheer and Nelson 2009; Mahfuth

et al. 2017). A study by AbuSaad et al. (2011) on Saudi organisations concluded that "Saudi Arabia's culture was indeed a major obstacle during their implementation process for ISO 27001" (p. 4). However, a study by Shojaie (2018) revealed that more than 50 percent of the participants did not agree that culture is not a factor or obstacle for implementing information security standards such as ISO 27001. Furthermore, it was argued that subjective norms within the Saudi culture, which have a high rating in power distance and low rating in individualism, would positively influence the intention to use technology; however, that would also be dependent on age and experience which may negatively moderate such an influence (Al-Gahtani, Hubona, and Wang 2007).

Aldossary and Zeki (2013) argued that employees in Saudi organisations are less aware of information security risks as a result of the local culture and lack of knowledge. In another study conducted by Aldossary and Zeki (2015) on two university students in Saudi Arabia showed that culture influences students' perception of information security, which also impacts their behaviour towards security. The study further indicated that cultural behaviour significantly affects students' knowledge over security issues and that their knowledge is highly influenced by the local culture. Alzamil (2018) added that cultural issues could negatively affect compliance with information security roles and policies within Saudi organisations. Likewise, Alkahtani, Dawson, and Lock (2013) confirmed that Saudi culture could potentially make information security very vulnerable, which may affect the success of businesses in the country.

There is low acceptance of technology by ordinary workers in the Arabian region (Al-Gahtani and Hu 2013). Indeed, it is theorised that instead of being driven by personal motivations and perceptions like that of workers in a more mainstream contexts, Saudi workers are influenced by family as well as collective norms and values in adopting technology (Hu, Al-Gahtani, and Hu 2013). Therefore, socio-cultural traditions may serve as a constraint to the acceptance of and diffusion of technology (Alqahtani 2018).

2.8.1.2 Management Commitment and Support

Organisational leaders and managers are regarded as the "shapers and builders" of organisational culture (Soomro, Shah, and Ahmed 2016). Management commitment and

support for information security refers to the degree to which organisational leaders understand the information security function, the importance as well as being involved in defining and communicating a security policy, assigning responsibilities to individuals, assuring the availability of resources, and monitoring information security effectiveness (Alnatheer 2015). Management and their roles in organisations are crucial in forming the desired culture because security of information is mainly a management issue; therefore, upper management should be fully aware of the significance of the development and implementation of ISP (Veiga and Martins 2017; Soomro, Shah, and Ahmed 2016; Glaspie and Karwowski 2018). These leaders and managers define an organisation's information security strategy and lead by example (Veiga and Martins 2017). Furthermore, management's commitment and support for information security is crucial not only for information technology resources allocation but also for employees to see that management promotes information security as an important organisational attribute (Carey-Smith 2011) as this enables the promotion of a successful information security program and improves information security management activities in organisations (Alnatheer 2015). Okonofua, Rahman, and Ivanova (2019) stated that the role of management in improving ISRM in organisations is underestimated as a result of inadequate knowledge of the subject matter. The authors further confirmed that supportive management brings about superior ISRM outcomes in an organisation. ISRM execution is one of the responsibilities of the management of an organisation, and the management is also responsible for aligning the execution with organisations vision and policies (Okonofua, Rahman, and Ivanova 2019). Sanusi and Satirenjit (2021) stated that "Top management commitment and support involves establishment of corporate objective on risk minimisation, risk management policy formulation, financing setting up committees for monitoring, supervision and training as well as evaluation of risk management result" (P. 276).

Carey-Smith (2011) conducted a study that compared two organisations with different information security management support levels. The study indicated that one organisation had a high level of management support, which reflected positively on employees' reaction and behaviour towards information security. On the other hand, the management of another organisation appeared to have a great understanding of the importance of information security but did not translate this understanding into action. As such, employees at this

second organisation are less likely to comply with information security practices, therefore exposing the organisation to risk. Thus, the author recommended that managerial staff undergo an awareness program on the importance of information security (Carey-Smith 2011).

In support of this argument, Reza et al. (2013) stated that the administrative role in information security management is to deliver a clear message on the importance of information security policy to the rest of the organisation. This could be done by the allocation of adequate information security budget and resources. Moreover, the management staff must fully support information security management program and should understand that information security has a direct relationship with the core of the organisation's activities (Reza et al. 2013).

Alnatheer (2015) also argued that the establishment of a security culture by the management is more important than the support of the existence of information security management. The author stressed that security culture cannot be established without upper management's involvement and commitment because culture plays a crucial role in the perception of management towards information security commitments and support levels (Alnatheer 2015). Similarly, Alqahtani, Goodwin and de Vries (2018) stated that cultural conditions influence the adoption of technology and management support levels. The study further indicated that management styles and practices of organisations across the world are influenced by differences in diverse national cultures as cultural conditions determine whether, when, and how a new innovation or technology organisations leaders and managers will adopt (Alqahtani, Goodwin, and de Vries 2018). Alkahtani, Dawson, and Lock (2013) confirmed that culture in Saudi Arabia has great influence on management styles, decisions, and behaviour.

Finally, the understanding of the Saudi Arabian cultural differences such as language, hierarchy, gender communication, and fear of public shame can have a strong impact on the success of information security of an organisation (Alkahtani, Dawson, and Lock 2013). Aldraehim et al. (2012) indicated that the cause of unsuccessful information security management and approaches in Saudi Arabia revolve around conflicts of culture in the management style of Western and Arab leaders and managers.

2.8.1.3 Information Security Policies Non-compliance Behaviour

The information security policies (ISPs) describe the organisation's information security approach and provide a framework for determining procedures, risk assessment, and risk management processes (Veiga and Martins 2017). It provides management with “direction and support for information security in accordance with business requirements and relevant laws and regulations” (Veiga and Martins 2017, p. 80). However, non-compliance behaviour is deliberate or non-deliberate risk-taking by employees who disregard an organisation’s policies (Dols and Silvius 2010). Employees’ compliance with ISP in an organisation is crucial in reducing the risk of information security. It was argued that employees’ adherence to ISP is directly influenced by culture cultivated in an organisation (Nasir, Arshah and Ab Hamid 2017).

Chua et al. (2018) stated that “numerous research studies have warned that different cultural backgrounds can influence one’s perception and tolerance of information privacy and security” (p. 1773). Dols and Silvius (2010) added that non-compliant behaviour towards an organisation’s policies and the perception of risk by employees is an influenced and culturally determined attitude. Other factors that could influence employees’ ISP compliance behaviour are self-efficacy, normative beliefs, the use of rewards, perceived severity, and the readability and understandability of policy language (Tsohou, Karyda, and Kokolakis 2015). A recent study found that 74 percent of individuals surveyed ignore the reading of privacy policy notices, mostly because they are too lengthy, confusing, and contain complex content (Chua et al. 2018). Similarly, Xie et al. (2012) argued that organisational culture is one of main factors that influences policy non-compliance behaviour. The study further stressed that it influences effective implementation of ISP as it has significant impacts on the perception of employees towards information. The authors further asserted that policies, through continuous education and collaboration, can in turn define organisational culture (Xie et al. 2012).

Chua et al. (2018) argued that some employees choose not to follow ISP practices because they may hinder their job routines. In addition, this generates contradictory interests between their job’s functionality and information security (Chua et al. 2018). Therefore, knowledge and behaviour should be aligned in order to have effective non-compliance behaviour in organisations (Alassafi et al. 2016; Li et al. 2019). It is believed that the

enforcement of ISP may reduce the risk of information security vulnerability in organisations while Intrinsic and extrinsic motivations could possibly change employees' behaviour towards non-compliance with organisation's ISP (Alfawaz 2011). This simply means that healthy Information security culture and organisational culture are crucial as they are capable of promoting positive effect on the behaviour of ISP (Fredrik, Joachim, and Martin 2015; Safa et al. 2015).

Alzamil (2018) asserted that employees' low perception of the importance of internal and external threats as well as vulnerabilities could potentially impact effective ISP compliance in Saudi organisations.

2.8.1.4 Low Information Security Awareness

Information security awareness as defined by the Information Security Forum (ISF) is "the extent at which members of an organisation understand the importance of information security, the level of security required by the organisation and their individual security responsibilities as well as acting accordingly" (Limited 2011, p. 165). Employees fail to adopt proper security practices either because they are not aware of the potential risks or their lack of understanding of the implications of security violations (Tsohou, Karyda, and Kokolakis 2015). Almarhabi (2016) confirmed that employees are often regarded as a significant factor affecting information security in organisations. In most cases, security incidents are a result of the lack of awareness of the organisation's information security policies and procedures by the employees (Alnatheer 2015). In addition, Mahfuth et al. (2017) indicated that employees' lack of security awareness is one of the key contributors to security incidents.

Information security awareness is considered as a precautionary measure to prevent risks due to employees' ignorance of security awareness (Von Solms and Von Solms 2004). A review by Chua et al. (2018) revealed that organisations which provide a sufficient level of policy awareness have a lower number of employees misusing the IT infrastructure and also a remarkably low number of computer attacks. In addition, the study argued that organisations with well-established policy awareness programs would have positive IT attitude employees with good intention to comply. The review demonstrated that employee awareness and their behaviour towards complying to IS policies and protective IT structure is

significantly influenced by cultural factors (Chua et al. 2018).

Kshetri (2016) stated that low levels of information security awareness leads to further vulnerability of Saudi Arabia and other GCC economies; the study further stressed that cybersecurity threats confronting the energy sector as a result of insufficient awareness of such threats in the region are problems of special concern. Moreover, a recent study by Aldosari (2019) highlighted that information security awareness is very low in Saudi Arabia; in support of this finding, Omar (2017) argued that one of the main reasons that has made Saudi Arabia a frequent target for cyberattackers is very low levels of awareness and capabilities. Further supporting the claims of these other studies, Alzahrani and Alomar (2016) revealed that 91 percent of respondents in Saudi Arabia have never had any security awareness training courses, and the study concluded that there is a lack of security awareness training in Saudi Arabia, which is a major security risk.

Likewise, Almarhabi (2016) argued that the level of information security awareness in the public sector organisations is very low in Saudi Arabia, and the study stressed that the important factors that influence the low level of information security awareness are culture and the country's educational system (Aldossary and Zeki 2013; AlKaabi 2014). Similarly, Alotaibi et al. (2016) noted that the level of awareness has not measured up with the level of utilisation of security measures and technologies in Saudi Arabia, and recommended Saudi organisations play an effective role in improving cybersecurity awareness among their employees. Hence, it was concluded that there are inadequate studies regarding Information Security Awareness in Saudi Arabia (Alzahrani and Alomar 2016). As Alkahtani, Dawson, and Lock (2013) and Alharbi, Atkins, and Stanie (2017) stated, the security awareness gap needs to be addressed in Saudi organisations.

2.8.1.5 Shortage of Skilled Information Security Professionals

The 2019 Global Information Security Workforce Study revealed that information security global gap is estimated at 4.07 million, in which the estimated information security global workforce needs to be increased by 145 percent (ICS2 2019). In recent times, all organisations are confronted with the problem of not having sufficient resources with the necessary expertise and knowledge, as well as limited skilled and experience human

resources in risk management (Singh and Joshi 2017).

The shortage of skilled human resources is another barrier that Saudi Arabia has experienced in its information security initiatives. It was suggested that more than 3,000 information security experts with high levels of experience and skills are needed as well as "tens of thousands" of people with lower-level skills and experience (Al-Saud 2012; Kshetri 2016). According to the Minister of Communications and Information Technology, Abdullah Al-Swaha, Saudi Arabia is short over 50,000 ICT specialists, including information security specialists (Hathaway, Spidalieri, and Alsowailm 2017). The need for localised IT expertise is vital as Saudi Arabia depends greatly on expatriates who possess a low level of knowledge as well as having a counterproductive policy that could potentially hinder IT becoming an integral component of Saudi Arabia economic development (Bronk and Tikk-Ringas 2013).

Alkahtani, Dawson, and Lock (2013) and Alharbi, Atkins, and Stanier (2017) stated that information security qualifications need to be addressed in Saudi organisations. Moreover, Alshitri and Abanumy (2014) argued that the shortage of human resource information security expertise paired with a high salary demand are the main concerns of Saudi organisation leaders. The shortage is exacerbated as a result of the increased price of oil, investment in big projects in the country, and growing economic liberalisation. Management and human resources professionals in Saudi organisations must understand the reasons behind the high salary demand and turnover. It was suggested that in order to improve the retention rate, management should adopt appropriate action programs such as incentives and training designed to minimise these problems (Alshitri and Abanumy 2014).

Alshitri and Abanumy (2014) further argued that increased in the demand for skilled information security professionals implies that the shortage is unlikely to improve soon, even with several Saudi universities having information security, information assurance, and cybersecurity programs. Table 2-3 summarises the different cybersecurity related programs delivered by Saudi universities (Alsmadi and Zarour 2018). Two universities have undergraduate programs, while the remaining four universities have information security and cybersecurity postgraduate programs. More universities have recently established their new information security and cybersecurity programs such as Dar Al-Hekma University, among others. However, there is a crucial need to establish more information security programs at

other universities across Saudi Arabia in order reduce the shortage gap (Alsmadi and Zarour 2018).

Table 2-3 Information Security Related Programs in Saudi Universities as of 2018

University	Program Level	Program Title
Imam Abdulrahman bin Faisal University	Undergraduate	Bachelor of Science in Cyber Security
University of Prince Mugrin	Undergraduate	Forensic Computing and Cyber Security
King Fahd University of Petroleum & Minerals	Graduate	Master of Science in Security and Information Assurance
Saudi Electronic University	Graduate	Master of Science in Information Security
Naif Arab University for Security Sciences	Graduate	Master of Science in Information Security
Prince Sultan University	Graduate	Master of Science in Cybersecurity

Source: (Alsmadi and Zarour 2018)

An estimate is that more than 200,000 new jobs are created yearly, which makes it feasible to attract and keep skilled professionals over the next years; however, business leaders and human resources professionals in Saudi Arabia need to understand the reasons for the high turnover (Alshitri and Abanumy 2014).

2.8.2 Process

Process can be defined as “a set of interrelated work activities characterised by a set of specific inputs and value added tasks that make up a procedure for a set of specific outputs” (Prodan, Prodan, and Purcarea 2015, p. 3). It can be described as an enabler of operation or tasks by combining policy, standards, procedures, and guidelines together in secure environment (Nicastro 2006). Process is a repeatable action that can theoretically generate the same result independent of who performs it (Khanduri 2020). One of the main goals of developing a process in an organisation is to ensure that the policy and procedure is adhered to and followed consistently (Nicastro 2006).

2.8.2.1 Sharing of Information Security Knowledge

Knowledge sharing is the exchange of information among a group of individuals in an organisation that can be carried out in both formal and informal settings for the purpose of improving employees' performance and productivity (Almuqrin et al. 2020). In information security contexts, sharing of information security knowledge is defined as the collaboration with others by exchanging information security related experiences, knowledge, and ideas in the interest of protecting an organisation's information assets (Safa and Von Solms 2016).

Jung (2013) stated that sharing of knowledge and information among organisations has a positive impact; in support of this, Renukappan et al. (2020) confirmed that knowledge sharing has many positive outcomes in an organisation including effectiveness, innovation capability, and enhanced productivity performance. Furthermore, Flores, Antonsen, and Ekstedt (2014) argued that knowledge sharing is one of the main predictors of an employee's behaviour and decision making; thus, both are critical in order to mitigate security risks. A study by Gal-Or and Ghose (2005) concluded that security knowledge sharing by two organisations would have a positive impact on their information security investment. Thus, organisations should consider establishing knowledge sharing mechanism among employees and organisational levels (Flores, Antonsen, and Ekstedt 2014).

A study conducted by Chandran and Alammari (2020) which examined knowledge sharing among academic staff in a Saudi university revealed that there is a low level of adoption of knowledge sharing among the academic staff. In a similar study by Almuqrin et al. (2020) to examine knowledge sharing in higher education in Saudi Arabia, it was revealed that shared vision, shared language, social and cultural background, and organisational and relational identifications are the main factors that influence knowledge sharing behaviours in Saudi Arabia. Consequently, Al-Adaileh and Al-Atawi (2011) stated that there are inadequate studies in the field of knowledge management and knowledge sharing which explore issues relating to the knowledge sharing within Saudi Arabian organisations.

2.8.2.2 Information Security Policy (ISP)

Most organisations fail to have an effective ISP because they are unable to explain the

needs and concepts of information security to their employees. Höne and Eloff (2002) stated that “the common problem with most information security policies is that they fail to impact users” (p. 14). Organisations are required by a regulatory authority to have a level of ISP in place (Glaspie and Karwowski 2018). The aim of having ISP is to clarify the rights and responsibilities of information resource to users in an organisational setting, to help the employees to understand information resources’ acceptability and responsible behaviours, and to ensure the secure handling of information assets in their daily work (Höne and Eloff 2002). Calder and Watkins (2010) indicated that while risk management is the core of information security, ISP assists organisations to have risk management in place. The authors argued that defining ISP is crucial during the first phase of ISRM planning because risk management activities cannot be carried out without the existence of the ISP (Calder and Watkins 2010).

Okonofua, Rahman, and Ivanova (2019) noted that ISRM policy must be decided at the board level of organisations and implemented by information technology leadership. Karyda, Kiountouzis, and Kokolakis (2005) also argued that an ISP must be aligned with the organisation’s pre-existing cultural norms as well as evaluated and updated accordingly as this will also result in having the information security policy to support the organisation’s code of ethics (Karyda, Kiountouzis, and Kokolakis 2005). Moreover, evaluation of an ISP is crucial for an effective ISP as it is the process of measuring the impacts of the policies in order to determine appropriateness, effectiveness, and efficiency. Defining policy goals, expected outcomes, audience, and evaluation objectives are the first step in ISP evaluations while the final step is assessing the evaluation. Measurable results and assessments are essential steps for implementing an ISP in organisations (Almarhabi 2016).

Chua et al. (2018) argued that some employees choose not to follow ISP practices as they may hinder their job routines; they may feel that ISP practices generate contradictory interests between their job’s functionality and information security. Therefore, knowledge and behaviour should be in line in order to have effective compliance behaviour in an organisation (Alassafi et al. 2016; Li et al. 2019). It is believed that ISP enforcement reduces the risk of information security vulnerability in an organisation. Intrinsic and extrinsic motivations could possibly change employees' behaviour towards compliance with an organisation’s ISP (Alfawaz 2011); however, it was indicated that a healthy Information

security culture and organisational culture are crucial in order to promote a positive effect on ISP behaviour (Fredrik, Joachim, and Martin 2015; Safa et al. 2015).

In a study conducted by Talib et al. (2018) to compare Saudi Arabia's government attitude toward ISP and privacy with Australia and the UK. The results revealed that Saudi Arabia has less policy, readiness, and practices as well as low levels of rewards and sanctions to achieve compliance compared to the other two countries. The principle of sanctions and rewards is not practiced as a result of the gap in measuring policy implementation in most of the Saudi Arabia government organisations. The authors suggested that in order to enhance the adherence to security and privacy policies in Saudi organisations, both education and training should be provided to employees to improve their level of awareness (Talib et al. 2018).

Alzamil (2018) conducted a study covering 41 Saudi organisations by collecting feedback from 69 employees and 65 managers (N = 134). The results showed that there are significant concerns over employees' understanding and the ability to comply with ISP. The study revealed that most organisations have an established ISP; however, many are not enforcing and publicising their ISP effectively. The author indicated that although most of the organisations have a good information security technologies investment, they are less effective as a result of the poor policy enforcement (Alzamil 2018). The author indicated that the employees' low perception of the importance of internal and external threats and vulnerabilities could potentially impact ISP compliance in Saudi organisations (Alzamil 2018).

Another study by Almarhabi (2016) comparing Saudi Arabian organisational ISPs with Western countries' revealed that most employees are unaware of the privacy policies and the policies were scattered, overly broad, and outdated. Moreover, employees were not trained or educated to follow policies. The authors suggested that Saudi Arabian organisations' policies have to be clearly documented, accessible, updated, and, most importantly, include a proper training of staff (Almarhabi 2016). The authors found that Saudi Arabian organisations lack of readiness policies, putting policies into action, and implementing rewards and sanctions practices (Almarhabi 2016).

2.8.2.3 ICT Outsourcing

Although ICT is not the core business of most organisations, they need professional labour and huge technological investment in order to establish and continue ICT operations. Accordingly, outsourcing is utilised in most cases to overcome this problem (Moon et al. 2018). ICT outsourcing is an act by which some or all of the IT-related business processes, internal activities decision-making rights, and services are delegated or transferred to external providers who create, manage, and administrate them for a certain period of time according to an agreed contract; this enables organisations to reduce costs, accelerate time, and benefit from expertise and assets (Elsayed 2014; Khidzir, Mohamed, and Arshad 2010b). The ICT outsourcing market is constantly increasing due to the expanding scope of ICT in most organisations. As a result, the information security risk increases accordingly (Moon et al. 2018).

Studies have shown that ICT outsourcing is one of the critical information security risks (Khidzir, Mohamed, and Arshad 2010a). Recently, security incidents from ICT outsourcing have dramatically increased. For example, the issue of information security risk increases when bringing in and removing organisations' unauthorised equipment as well as the increase of the number of people who can access organisation ICT assets (Moon et al. 2018). However, if not managed properly, the outsourcing of ICT could result to an information security risk that is difficult to mitigate. Therefore, proper risk management for ICT outsourcing is vital to manage information security risk (Khidzir, Mohamed, and Arshad 2010a).

In the same vein, Bronk and Tikk-Ringas (2013) argued that the Saudis have invested significantly in computing and telecommunications; however, ICT projects are mainly outsourced and facilitated by foreign entities. Moreover, due to the shortage of skilled people in Saudi Arabia's working population, more migrant labour is needed from different countries (Dinglasa 2020; Straub, Loch, and Hill 2001). The studies of Almubayedh et al. (2018) and Alelyani and Kumar (2018) confirmed that IT outsourcing is one the main information security risk factors in Saudi Arabian organisations. Spong (2018) argued that in Saudi Arabia, "some critical country infrastructures are partially or completely managed by private entities, which need to increase their maturity in order to guarantee the country's resilience" (p. 1).

2.8.2.4 Information Technology Audit

An IT audit can be defined as “the evaluation of systems, processes, and controls performed against a set standard or documented process” for an organisation (Wright 2008, p. 5). It determines whether internal controls protect organisations assets, ensure data integrity and are aligned with the organisations goals (Cole 2014). An IT audit provides an independent assessment through evaluation of the system or process. The key objective of performing an IT audit is to measure and report risks in which top management can find answers to the questions about organisation’s exposed risks (Florea and Florea 2016; Wright 2008).

A study conducted by Alzeban (2015) to investigate the effect of cultural dimensions on IT audit in 67 Saudi Arabian organisations. They study revealed that national culture negatively affects internal audit because it is not given a sufficient credence and importance. A similar study carried out by Abu-Musa (2009) which examined auditing processes for information technology governance in 127 Saudi organisations from different industries including banking, oil and gas, manufacturing, and government agencies revealed that most of the respondents reported that IT auditing processes are not completely conducted in Saudi organisations. The study showed that most of the organisation in Saudi Arabia intend to conduct internal IT audit; however, the process is either not started nor not complete. The author further indicated that there is inadequate research related to IT auditing and evaluating IT-related activities in developing countries including Saudi Arabia.

2.8.3 Technology

Technology is the final step after having both people and processes in place. Technology is the tools and techniques people use to work and communicate efficiently. It includes information systems and their management hardware and software (Prodan, Adriana and Anca 2015). Technology provides the tools needed to implement the organisational process and automate it, regardless of its complexity (Khanduri 2020). At present, technologies such as cloud services, mobile applications, and big data are rapidly changing the way that business is being executed as technology is getting more important and visible (Prodan, Adriana and Anca 2015). There are many technology tools in the market that are tempting and attractive

for many organisations in need. More often, organisations spend massively on technology in order to gain competitive advantages. However, organisations need to be cautioned and careful when acquiring any of these tools. They have to make sure that the technological tools intended to be acquired is the best fit for the organisation (Khanduri 2020).

2.8.3.1 Risk Management Technology Tools

Technology provides the tools that the people can use to implement the process. It also helps to automate some parts of the process. Ideally, the latest and fastest technologies have the most impact (Nicastro 2006). Risk management is a complex and iterative process that involves different people from different levels across an organisation. Due to the complexity and multi-layering of activities involved in risk management, most organisations have reached a point where risk management tools such as emails and spreadsheets are insufficient (Billings 2018). Billings (2018) stated that technology has introduced risk management tools and solutions to streamline risk management processes, automate tasks, and assure people's accountability (Billings 2018). It was also argued that these tools can assist organisations in resolving risk management and compliance issues as well as improving their business alignment (Bundy 2021).

In a rapidly changing risk landscape, risk assessment activities such as the data collected could quickly became stale and, as a result, serious critical blind spots are created that negatively affect the entire risk management cycle (Atul 2020). Hamilton (2020) argued that the risk level's real-time visibility is impossible if risk assessment activities are being handled and managed manually (Hamilton 2020). Atul (2020) confirmed that managing the enormous volume of risk data cost-effectively and efficiently can only be achieved by utilising risk management software that would can also increase business resilience and help avoid disruption. For example, effective risk mitigation requires ongoing monitoring and planning activities which are time- and resource-consuming. However, risk management software could potentially reduce time and cost by providing opportune and more accurate data that assist in risk mitigation activities.

2.8.3.2 Information Security Awareness Measurement

It was shown that if an employee's information security level of knowledge increases, their behaviour towards information security policy improves, which results in better information security culture within the organisation (Parsons et al. 2017). In a study conducted by Parsons et al. (2017) measuring the effectiveness of ISA training among over 1,600 working Australians from different industries including government agencies, financial institutions, and employees from a range of other organisations, it was revealed that ISA quizzes could help in identifying employees' strengths and weaknesses, which requires more education and training. The study further revealed that most employees could be targeted by spear-phishing attacks as they were unable to recognise the danger associated with clicking email links despite the fact that they had taken ISA training sessions prior to the test. The results, however, improved employees' awareness and enhanced more effective ISA training programs (Parsons et al. 2017).

Pape et al. (2020) revealed that there is a large number of information security training and awareness research targeting different domains and areas in academia. However, information security awareness quizzes that measure employees' behaviour are mostly commercial without a detailed description; consequently, there is no standard measurement tool for employees' security behaviours. There have also been minimal attempts to develop a comprehensive method of measuring security awareness; these attempts are promising as they come from diverse cultural settings which indicate that there is a global interest in security awareness effectiveness measurements (Parsons et al. 2017).

2.9 The Reasons for Developing an ISRM Model for Saudi Arabian Organisations

Overall, this research has three main area of interest: information security, risk management, and Saudi Arabia as shown in Figure 2.6. The research elements should lie within the overlap area.

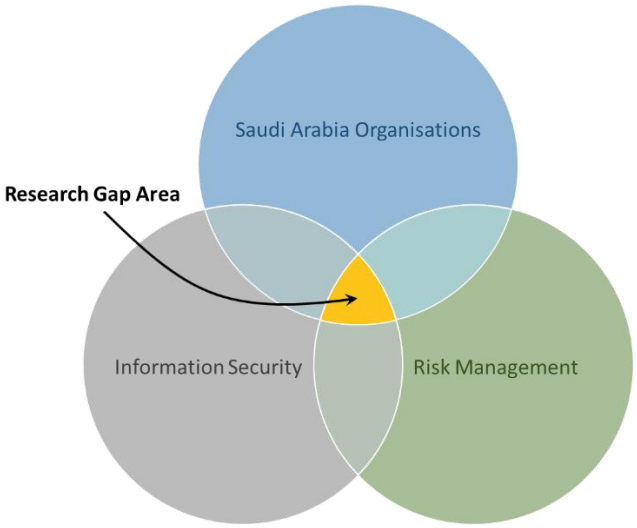

Figure 2.6 Research Gap Area

Source: Researcher's Compilation (2021)

The People, process, and technology (PPT) are the main elements of the proposed conceptual model of this research in which the proposed factors are categorised under the PPT. Although some studies have highlighted the main challenges associated with international ISRM adoption in Saudi organisations, little research has been carried out to develop regional- or cultural-specific ISRM models. In addition, none of the reviewed ISRM standards addresses all the factors identified in the literature.

Alnatheer and Nelson (2009) confirmed that there is a real knowledge gap in terms of information security studies in developing countries including Saudi Arabia as the majority of the research about ISM were carried out in technologically leading countries. In addition, little has been done to investigate cross-cultural considerations. These considerations are significant because culture has a direct impact on these phenomena. National culture directly influences employees' learning ability which in turn impact organisation innovation and growth. That is why there is a need to analyse different characteristics of employees including culture in implementing information security activities (Looso, Goeken, and Johannsen 2011). Schmidt et al. (2008) stated that national culture influences the entire employees of an organisation as well as management perceptions and privacy-related issues. Each country has different perceptions of relevant information security threats (Schmidt et al. 2008; Xie et al. 2012). In addition, Al Omoush, Yaseen, and Atwah Alma'aitah (2012) argued that Arab cultural

beliefs are significant predictor of information technology transfer resistance.

Researchers should consider cross-cultural differences such as uncertainty avoidance, collectivism-individualism, and power distance relationships as a result of their importance in other IT contexts (Aldraehim et al. 2012; Alnatheer and Nelson 2009; Flores, Antonsen, and Ekstedt 2014). According to Hofstede (as cited in Al-Gahtani, Hubona, and Wang 2007), Saudi cultural dimensions differ from Western societies' cultural dimensions; this has a major impact on the validity of using satisfactory management theories developed in Western countries in a Saudi context. In addition, Malaika (1993) conducted a study to compare Western societies with Saudi Arabians and other Arabs and societies. The findings revealed that management theories and practices are "more culture-bound than is realised" (Malaika 1993, p. 207). The study found that Arabs are more careful about Western practices, theories, and ways of life. They do not want Western contact and technology to influence their beliefs and culture (Malaika 1993).

Bjerke and Al-Meer (1993) stated that as a result of the gap between the United States and Saudi cultures, U.S. management practices are not applicable for the Saudi culture. Furthermore, a study by Al-Adaileh and Al-Atawi (2011) on knowledge management in Saudi Telecom Company (STC), the Middle East's largest telecom company in Saudi Arabia, it was revealed that knowledge management theories practical in other cultures are not applicable for Saudi Arabia because of cultural differences. The authors concluded that managers in Saudi Arabian organisations should assess the culture of their organisation and management theories in order to obtain the best results (Al-Adaileh and Al-Atawi 2011). Thus, there is a need for a region-specific ISRM standards that combines all of these identified factors, thereby reflecting the real-world situation.

Therefore, the overall aim of this research is to develop an ISRM model based on these newly identified factors. To the best of the researcher's knowledge, there is no study that has examined these factors in order to develop a regional-specific ISRM model. Thus, this research intends to fill this research gap.

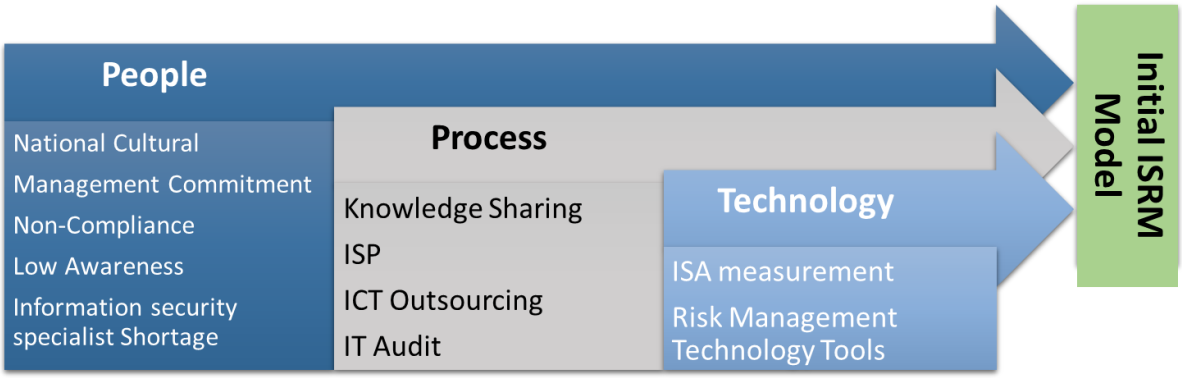

Figure 2.7 Initial ISRM Model

Source: Researcher's Compilation (2021)

This research has taken into consideration the factors that have been addressed by previous literatures. The initial ISRM model is shown in Figure 2.7 to illustrate these factors. This model has been utilised in the preparation of the first phase of data collection with the use of semistructured interviews as well as data validation as described in CHAPTER 3. Next, the outcome of the analysis of the responses from the interviews will enhance the development of the proposed ISRM model.

2.10 Summary

The understanding of how ISRM practices affect organisations' information security posture could help to understand some of the current perceptions of the security function that need to be overcome. It can drive security decisions such as confidentiality, integrity, availability, and accountability, and will also inform the requirements to mitigate risks.

This chapter provided a review of the relevant literatures related to ISRM and Saudi Arabia's information security. The review presented an overview of international ISRM standards, Saudi Arabia's information security position, the factors contributing to ISRM effectiveness in Saudi Arabian organisations, and the gaps in the previous research. The initial findings from this chapter revealed the various factors that should be considered which match current needs for ISRM model for Saudi organisations. PPT process improvement was used to group these factors. Human factors were national culture, management commitment, ISP

non-compliance behaviour, information security awareness, and information security specialist shortage. Process factors were information security knowledge sharing, information security policy, ICT outsourcing, and information technology audits. Finally, the technology factors were risk management technology tools and information security awareness measurement. Thus, this chapter highlighted the need for a region-specific ISRM model and reemphasised the significance of this research.

CHAPTER 3. RESEARCH METHODOLOGY

3.1 Introduction

The previous chapter reviewed the literature to better understand and to develop the initial ISRM model that this research is founded upon. This chapter explains how this research was carried out in terms of research design, data collection, analysis, ethical issues, and reporting. It discusses the research methodology adopted to develop an ISRM model for large Saudi Arabian organisations.

Firstly, the researcher's philosophical position and the research approach are discussed, followed by the research timeframe and a description of the methodological design elements of phenomenological research. The process within the adopted research design is explained, followed by an account of how this process was carried out in the context of this research. The research quality is then discussed followed by the approach to sampling procedure, data collection, and how the research philosophy and strategy were be incorporated into the data analysis.

3.2 Research Philosophy and Strategy

Creswell and Poth (2018) described research philosophy as "the use of abstract ideas and beliefs that inform our research. We know that philosophical assumptions are typically the first ideas in developing a study, but how they relate to the overall process of research remains a mystery" (p. 16). Research philosophy influences the selection of researcher of methodology, choice, and approach of data collection and analysis. Myers (2009) argued that the most relevant philosophical assumptions that guide the research are "those that relate to the underlying epistemology" (p. 41). Research epistemologies are classified into positivist, interpretive, and critical research (Myers and Avison 2002; Myers 2009).

3.2.1 Positivism Research

Positivist studies "are premised on the existence of a priori fixed relationships within

phenomena that are typically investigated with structured instrumentation. Such studies serve primarily to test theory, in an attempt to increase predictive understanding of phenomena" (Myers and Avison 2002, p. 55). In positivism, reality can be objectively defined and measured using the researcher's perceptions; independent tools and knowledge can be validated according to sensory experiences and proofs. Therefore, positivist studies are scientific in that they view the world as objective, stable, and external to individuals' mindsets of. In addition, they consider knowledge as factually constructed, which means that human beliefs are categorised as either true or false. Methods of enquiry in positivism are based on statistical, measurable data.

Altiny, Paraskevas, and Jang (2015) and Myers and Avison (2002) suggested that positivist research philosophy relates to deduction and quantitative research, such as surveys, experiments, and field studies. This includes natural science research, such as physics, geology, and chemistry. Conversely, qualitative research relates to the interpretive research philosophy.

3.2.2 Interpretive Research

Walsham (1995) stated that interpretive research philosophy is research that:

> adopts the position that our knowledge of reality is a social construction by human actors. In this view, value-free data cannot be obtained, since the enquirer uses his or her preconceptions in order to guide the process of enquiry, and furthermore the researcher interacts with the human subjects of the enquiry, changing the perceptions of both parties. (p. 376)

Interpretive research is based on investigation, observation, and understanding of a social phenomenon. It enables the researcher to determine the research issues by utilising and evaluating small samples in detail (Alkahtani 2018). Interpretive research aids in the understanding a particular phenomenon of interest from the participants' point of view in its natural settings (Armstrong 2013; Kaplan and Maxwell 2005). Interpretive research tends to utilise qualitative data and methods. It collects data using interviews, case studies, and observations in which the collected data must be able to answer the research questions

(Armstrong 2013).

Interpretive research focusses on variables such as cultural diversity, localised realities, socioeconomic conditions, and human experiences and perceptions rather than testing a hypothesis through an objective scientific framework. Truth can be seen as defensible knowledge claims rather than objective empirical data (Walsham 1995). Dhillon and Backhouse (2001) added that an interpretive philosophy offers advantages regarding information systems security research. It provides a holistic insight of the problem domain.

3.2.3 Critical Theory Research

Critical theory combines elements of both interpretivist and positivist philosophies. Critical theory research proposes that reality is not a matter of evaluations, personal preferences, or attitudes as may be indicated by the interpretivist philosophy. It embraces the concept of an objective reality, regardless of human knowledge. Critical paradigm researchers have suggested that the human understanding and human behaviour of reality are culturally and historically constructed and a collection of established values, beliefs, and social structures or discourses that become naturalised to the degree of their invisibility and recognition are limited (Bisman 2010).

Therefore, the aim of the approach is to uncover the economic, cultural, and political complexities embedded within such discourses to expose, criticize, and potentially change power and dominance in relationships in contemporary society. It includes deconstructing hidden power structures which can relate to culture, age, race and other variables, thereby giving voice to the non-mainstream, marginalised, and post-colonial individuals. Thus, critical research methods challenge positivist research methods, both quantitative and qualitative, which argue that they are scientifically objective (Kincheloe and McLaren 2011).

3.2.4 Research Philosophy and Strategy Choice

The researcher views the world in a way that influences the appropriate choice of research philosophy and strategy. The researcher's assumptions should support the approaches, paradigm, and methods chosen (Creswell and Poth 2018).

Given the nature of this research, the proposed research strategy is explorative in nature. Exploratory research try to determine "what is happening, seeking new insights, and generating ideas and hypotheses for new research" (Runeson et al. 2012, p. 13). The lack of ISRM phenomenon systematic research in the Saudi Arabia context justifies the exploratory nature of this research.

This research is based on the observation and investigation of people's perspective of information security risk management, experience, and cultural influence in order to maintain a holistic view of the problem domain. In addition, it is analytical research in which the researcher analyses existing information security risk management practices in Saudi Arabian organisations and evaluate events by asking participants *why* and *how*. Therefore, this research has adapted an interpretive research philosophy due to its applicability to comprehend the nature of the research carried out. In addition, it provided clarity of the research questions and a better understanding of the conceptual boundaries surrounding the research questions.

3.3 Research Approach

The research approach illustrates the style of the conducted research in which the researcher can utilise more one or more approaches. This includes qualitative/quantitative and inductive/deductive styles (Creswell 2014). Each are discussed in the following sections.

3.3.1 Inductive and Deduction

The inductive approach begins with specific observations of phenomena in order to make a broader generalisation. It is more scientific in nature as the conclusion is drawn based on observations rather than theories. Inductive studies use specific individual observations and then categorise them into patterns in order to uncover generalisations and then conclusions. Inductive reasoning is used in cases that involve forecasting, prediction, or expected behaviour. Therefore, the inductive approach is applicable to case studies, phenomenological research, action research, and other social science research methods that involve human behaviour. Inductive reasoning begins with observations, assembles them into

patterns, and generalises these patterns into a probable theory (Rovai, Baker, and Ponton 2013). The inductive approach is more involved with the collection of qualitative data because it utilises descriptive language which cannot be applied when research uses numbers alone, such as in quantitative data (Brink et al. 2006). Inductive studies usually begin with very general research questions to narrow down the scope of the study rather than with a rigorous hypothesis (Creswell 2014). Rich interviews and focus groups are examples of qualitative research methods aligned with an inductive approach.

The deductive approach, on the other hand, begins with a premise or assumption and proceeds to a conclusion that is based on logic. For example, it begins with a hypothesis and narrows it down to a logical conclusion. It provides an absolute certainty of being correct if the primary premises were correct. Deductive reasoning moves from general principles to very specific conclusions by generating a new hypothesis or conducting observations to test whether or not the hypothesis is valid. Deductive research lends itself to a quantitative approach utilising numbers in order to be precise and scientific.

3.3.2 Qualitative and Quantitative

Creswell and Poth (2018) define qualitative research as:

> an inquiry process of understanding based on distinct methodological approach to inquiry that explores a social or human problem. The research builds a complex, holistic picture, analyse words, report detailed views of participants, and conducts the study in a natural setting. (p. 326)

Thus, qualitative research study items in their natural settings and interpret phenomena or try to make sense of data. Qualitative research involves subjective analysis, focuses on the respondents' experiences, and identifies the phenomena they have experienced. Qualitative research is descriptive and exploratory and in focus, which provides greater flexibility. This type of research is concerned with the experiences and opinions of individuals, which provides the researcher with subjective data. The researcher, in qualitative research studies, identifies one or more traditions of inquiry. Qualitative research involves detailed methods, a rigorous data collection approach and analysis, and report writing. Qualitative research seeks

to uncover patterns within the data, document them, and then interpret them in subjective matter. Qualitative research introduces comprehensive understandings of contextual, rich, and unstructured data. This is achieved by engaging in conversations with the participants in a natural setting (Creswell 2009). Table 3-1 below outlines the key differences between qualitative and quantitative research approaches.

Table 3-1 Qualitative vs. quantitative research

Criteria	Qualitative research	Quantitative research
Orientation/view	Interpretivist: seeks to gain a deep understanding and provide explicit interpretation of a social phenomenon or a particular case	Positivist: seeks to provide a superficial description of a large sample of population and variables for the purpose of generalisation
Nature of reality and how it is constructed	Existence of multiple realities/perspectives. Reality is socially constructed and meaning is embedded in the context of socio-cultural values and institutions (context-specificity)	Existence of one objective reality that can be observed and explained through properly organised scientific procedures (universality)
Knowledge & how it is acquired	Being interpretive, qualitative research tradition accepts the multiple social constructions of meaning and knowledge. Truth is relative, meaning that ultimate truth Knowledge is usually value-laden and drawn from interpretation of what is observed	What is accepted as 'knowledge' is something that has been directly observed by the senses; and it is theory-neutral & value-free. Objective knowledge can be gained from direct observation or experience, but is not perfect. Theories, hypotheses assumptions, background knowledge and values of the researcher influence observations
Approach and purpose of research	Inductive approach: seeks to explore, describe, understand, explain, change and/or evaluate. Explanation of social phenomena is approached through analysis of the frames of meanings of social actors obtained from everyday concepts/meanings/accounts. Findings are specific to time and place.	Deductive approach: Formulation & testing hypotheses; General laws and theories guide explanation and prediction. Statistical generalisation of the results is possible
Guide to inquiry	No clear research question and hypotheses. Inquiry is guided by a broad research question that is refined as analysis continues	There is an explicit research question and hypotheses that are specified right at the beginning of the study
Participants/ subjects & relationship with researcher	Research participants/subjects are active and participate in constructing reality/meaning with the researcher	Subjects are passive. The researcher is detached and always strives to be objective to avoid bias
Measurement & data	Interpretation of words and meanings to gain understanding of phenomena under study is the key tenet of this tradition. It refers to the what, how, when and where of a thing, its essence and atmosphere. Analysis is characterised by thick descriptions & explanations	Measurement: standard instruments are used. Measures obtained using indicators of concepts and data quantified and analysed numerically through statistics. It refers to counts and measure of things. Analysis is characterised by thin descriptions/explanations

Source: (Masue, Swai, and Anasel 2013)

Qualitative research involves a wide range of methods in order to obtain a better understanding of the subject matter. Researchers use multiple systems of inquiry in the research of phenomena and seeks involvement of their participants in data collection phase to build credibility with the individuals. Creswell and Poth (2018) categorised qualitative research approaches into five main streams as follows: narrative research, phenomenology, grounded theory, ethnography, and case study. The main characteristics of the five approaches are described by Creswell and Poth (2018) in Table 3-2.

Table 3-2 Contrasting Five Qualitative Approaches

Characteristics	Narrative Research	Phenomenology	Grounded Theory	Ethnography	Case Study
Focus	Exploring the life of an individual	Understanding the essence of the experience	Developing a theory grounded in data from the field	Describing and interpreting a culture-sharing group	Developing an in-depth description and analysis of a case or multiple cases
Type of Problem Best Suited for Design	Needing to tell stories of individual experiences	Needing to describe the essence of a lived phenomenon	Grounding a theory in the views of participants	Describing and interpreting the shared patterns of culture of a group	Providing an in-depth understanding of a case or cases
Discipline Background	Drawing from the humanities including anthropology, literature, history, psychology, and sociology	Drawing from philosophy, psychology, and education	Drawing from sociology	Drawing from anthropology and sociology	Drawing from psychology, law, political science, and medicine
Unit of Analysis	Studying one or more individuals	Studying several individuals who have shared the experience	Studying a process, an action, or an interaction involving many individuals	Studying a group that shares the same culture	Studying an event, a program, an activity, or more than one individual

Source: Creswell (2018)

Creswell (2009) defined quantitative research as:

> a means for testing objective theories by examining the relationship among variables. These variables, in turn, can be measured, typically on instruments, so that numbered data can be analysed using statistical procedures. The final written report has a set structure consisting of introduction, literature and theory, methods, results, and discussion. (p. 2)

Deductive approaches are fundamentally the main characteristics of quantitative research. They start with measuring variables and then finding relationships between these variables that lead to patterns or correlations relationships. Quantitative research values include objectivity, neutrality, and an acquisition of a sizeable scope of knowledge (Leavy 2017).

3.3.3 Research Approach Choice

The research questions tend to follow an inductive reasoning approach as they attempt to extend the existing literature through theoretical contributions in the field of information security risk management. Moreno (2002) stated, “researchers to use phenomenology to obtain a better understanding of the nature of the human experience in organisations” (p. 1760). In addition, Moreno (2002) encouraged researchers to employ phenomenology to gain a better understanding of the essence of human experience within organisations.

Consequently, this research has adopted a phenomenological research method in order to understand empirical matters from the perspectives of participants. It describes the meaning of lived experiences for about a phenomenon or concept and obtain data from multiple individuals who experienced the phenomenon. The aim is to gain a deeper understanding of the meaning or nature of the phenomenon. In addition, primary data using a qualitative approach has been adopted by conducting semistructured interviews.

The main reason for adopting a qualitative research methodology is the ability to interact with the participants and to better understand their views and opinions about the researched phenomena. The ability to interact with the participants helps the researcher to better understand people and their surrounding cultural and social environment. Therefore,

qualitative research study could investigate the ISRM standards' adoption level by participant's organisations, factors influencing the level of the ISRM standards adoption, and participant's recommendation to improve ISRM standards to best fit large Saudi Arabian organisations.

3.4 Research Time Horizons

A research time horizon in scientific research is the time the researcher estimates to collect relevant research data and how the data are collected over that time period. In this regard, research data is obtained in two ways: cross-sectional or longitudinal. The time horizon to choose for a given research project depends on the expected value of the information to be collected. It is largely independent of the research strategy or approach adopted. In either case, the time horizon works as a reference for all changes that have taken place or are yet to happen (Philips, Claxton, and Palmer 2008).

A cross-sectional horizon entails gathering, using, and analysing data from an entire population being observed or from representative segments of that population. In a cross-sectional study, all data is collected in relation to a particular point in time. As such, a cross-sectional study provides detailed snapshots only for the events of a given period of time (Philips, Claxton, and Palmer 2008).

On the other hand, a longitudinal horizon indicates that the study unfolds over a period of time. A longitudinal study usually takes a longer period of time to collect enough research data by retrospectively analysing the events which have occurred over a period of time in the past or is expected to occur in future during the study's timeframe (Neale 2012).

This research employs a cross-sectional time horizon for data collection. The advantage is that data can be collected within a shorter timeframe. Participants can be observed simultaneously at a defined moment in time. In addition, this shorter time horizon is achievable and the process requires less effort. The researcher is able to gather needed data immediately at that specific point in time and there is less chance that participants will withdraw from the study or that the researcher will abandon the study before it is completed (Brain 2001). Finally, the nature of the data collection of this research, which is interviewing

information security experts, requires less interaction with the participants due to the sensitivity of the data.

3.5 Research Design

A research design is "the logical sequence that connects the empirical data to a study's initial research questions and, ultimately to its conclusions" (Yin 2003, p. 26). Research design is essential because it is the strategy for achieving the research goals. It enables the researchers to find answers to their research questions by establishing connections to the data that have been collected. The design of this research is a top-down design approach as illustrated in **Error! Reference source not found.** to ensure that the research has not been p reviously undertaken, and the gap in knowledge can be filled by the proposed research (Armstrong 2013). Accordingly, Figure 3.2 demonstrates the research stages progress design based on top-down approach.

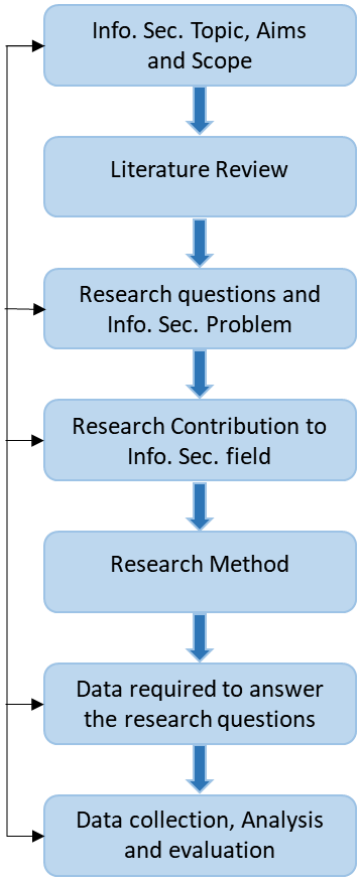

Figure 3.1 Top-Down Approach

Source: (Armstrong 2013)

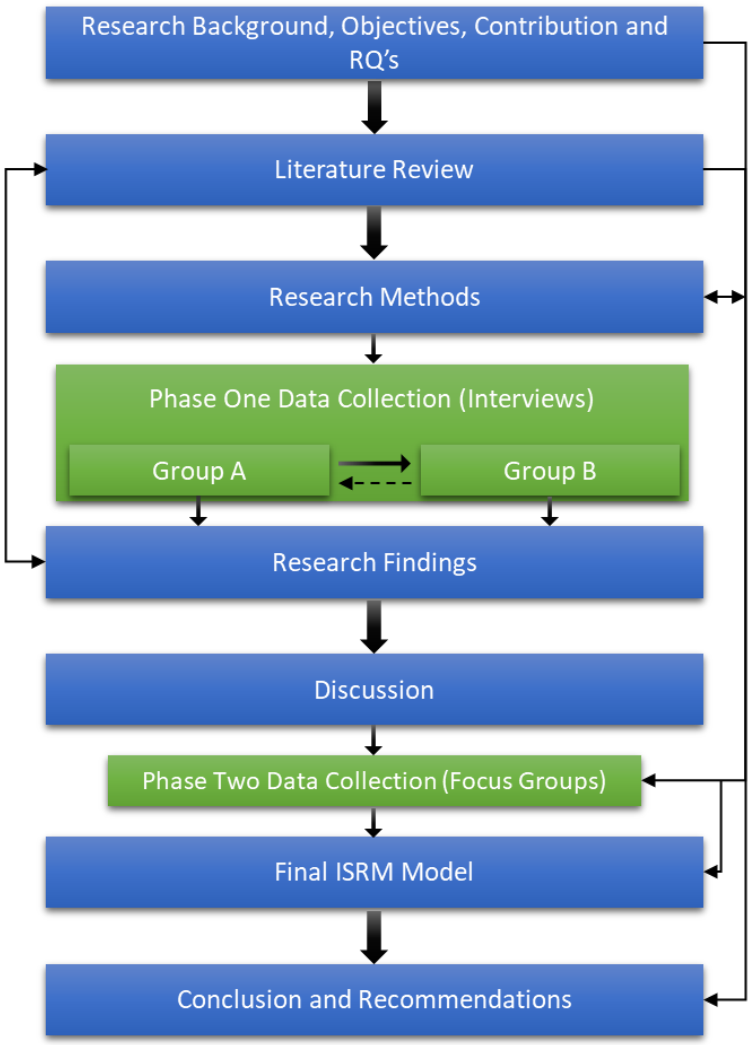

Figure 3.2 Outline of Research Design Stages and Process

Source: Researcher's Compilation (2021)

3.5.1 Research Background and Objectives

In the preliminary investigation stage, the researcher gathered fundamental knowledge related to ISRM in Saudi Arabian organisations. A comprehensive review of the literature was undertaken. This stage's outcome revealed a lack of academic literature in terms of ISRM in the Saudi Arabian context. Very little is known about ISRM and local culture relation and effects. The research objectives and question were created based on what was found in this stage.

3.5.2 Literature Review

This research involved a comprehensive literature review relevant to ISRM in general, as well as ISRM in the Saudi context and its related factors—including cultural factors. There is a knowledge gap that led to the development of the initial model to overcome this gap. The initial model was developed based on the literature review and analyses. However, the literature did not provide a deep understanding of the factors that could affect ISRM in Saudi Arabian organisations. Therefore, more investigation was required to examine these specific factors and define other factors that influence ISRM in Saudi Arabian organisations. As a result, the researcher conducted exploratory qualitative interviews to find out the factors that influence ISRM in the Saudi context.

3.5.3 Data Collection

The objective of this stage is to identify factors that influence ISRM effectiveness in the Saudi context using qualitative method. In this research, there are two phases of qualitative primary data collection. Semistructured interviews in phase one were the main data collection source that enables identifying and formalising the factors to develop an ISRM model in order for Saudi Arabian organisations. The second phase involved focus group interviews that evaluated the ISRM model for further enhancements. The following sections discuss the data collection process in detail.

3.5.3.1 Semistructured Interviews

In qualitative research, in-depth semistructured interviews are considered one of the most important tools for data gathering (Harvey-Jordan and Long 2001; Myers and Newman 2007). They are commonly used to explore the reasons why individuals behave in a particular way. This could be achieved by examining the experiences, understandings, and reactions of the participants. In addition, they are utilised to generate new ideas that enhance or change a certain practice as well as an evaluation tool (Harvey-Jordan and Long 2001).

Semistructured interviews enable researchers to identify key themes and also ask relevant questions without a fixed sequence. Semistructured interviews utilise pre-

formulated questions; however, the researcher does not have to strictly adhere to them. Questions emerge during the interview via the social interaction between interviewer and each participant (Myers 2009). The researcher has the opportunity to ask the participants for elaboration and clarification if an answer is unclear (Creswell 2014).

According to Galletta (2013), semistructured interviews in interpretive research can be utilised to understand the nature of a phenomenon and to obtain knowledge regarding processes and settings in social contexts (Galletta 2013). Semistructured interviews are considered for uncovering concepts related to particular practitioners (Galletta 2013). Accordingly, in the information systems discipline, semistructured interviews are considerably appropriate, especially if research and theory are in their early formative stages. This allows the researcher to examine the phenomenon as perceived by users, explore the state of practice, understand the nature of the real-life processes, and conduct research in areas in which few studies exist (Recker 2008).

Thus, semistructured interviews are an appropriate data-gathering technique of conducting research in information security management. Accordingly, semistructured interviews were considered as a data collection tool this research. The researcher used semistructured interviews with open-ended questions to contextualise and enrich conceptual propositions about ISRM in the Saudi Arabian context. The aim was to identify the main factors that influence, constitute, and reflect information security risk management in the large Saudi Arabian organisations context. The analysed data form the interviews in conjunction with the reviewed literature facilitated the conceptual model development.

The semistructured interview participants were divided into two different groups of participants, A and B, to achieve data triangulation. Data triangulation is “the process of comparing concurrently collected qualitative findings” (Adams et al. 2015, p. 95). Semistructured interviews were considered as a qualitative research strategy in order to check the validity of data by converging the results from different sources of data or respondent groups (Flick 2004; Carter et al. 2014; Adams et al. 2015). Thurmond (2001) stated that data triangulation “increasing confidence in research data, creating innovative ways of understanding a phenomenon, revealing unique findings, challenging or integrating theories, and providing a clearer understanding of the problem” (p. 254). In addition, triangulation can

be considered a “tactic for testing or confirming findings” (Miles, Huberman, and Saldaña 2014, p. 294). However, data triangulation can result in inconsistent or conflicting findings which need to be explained as to “why” they exist (Miles, Huberman, and Saldaña 2014).

Data triangulation can be achieved by collecting of data from multiple types of samples or population to gain different perspectives and validation of data. This includes individuals, families, groups, and communities (Carter et al. 2014).

Group A and B participants characteristics is discussed in detail later in Section 3.5.3.3.

The objectives of the interviews were to gain an understanding of:

1. Whether or not their organisations comply with any ISRM standards
2. The reasons for ISRM standards compliance
3. The effectiveness of the ISRM standards adopted
4. Factors that influence ISRM standard effectiveness and compliance
5. Factors that could improve ISRM standard effectiveness to best fit large Saudi Arabian organisations

In order to conduct the interviews, the researcher adhered to the following steps to create interview protocols (Jacob and Furgerson 2012):

- Research objectives and questions should guide interview questions
- Develop a script for the beginning and the end of the interview
- Start with basic background questions, then pose easy-to-answer questions, and move towards more informative or controversial questions
- During the interview, ask for elaboration to clarify important findings

Group A data collection phase started from November 2016 to September 2017. While Group B data collection phase started July 2017 to March 2018.

The process of the interviews is discussed in detail in Section 3.5.3.3.

3.5.3.2 Focus Group

A focus group is a qualitative data collection technique that is distinct from other qualitative data collection techniques such as one-to-one interviews. It has been used for decades in various research disciplines including marketing, health science, and communications (Guest, Namey, and McKenna 2017). It is “a special type of group in terms of purpose, size, composition, and procedures. The purpose of conducting a focus group is to better understand how people feel or think about an issue, idea, product, or service” (Krueger 2015, p. 2).

Focus groups centre on the insights and personal experiences of each member of the group in an interactive environment. Focus group members are encouraged to interact with the moderator and, in some cases, with other members. Focus groups are used to gather opinion (Krueger 2015; Myers 2009).

Participants are selected because they have certain characteristics in common and experiences which relate to the topic of the focus group. The researcher creates a permissive environment in the focus group that encourages participants to share perceptions and points of view without pressuring participants to vote or reach consensus (Myers 2009; Krueger 2015). It can be a controlled group discussion in which the moderator must complete the social arrangements required to produce targeted outcomes. In addition, it can be used to determine the different perspectives of individual respondents where they are able to speak to others, in an informal setting, about the topics introduced by the moderator (Smithson 2000).

The moderator’s role during the focus group sessions is to ask questions, keep the conversation on track, to listen, and to encourage everyone to share their thoughts and all types positive and negative comments (Krueger 2015; Barbour and Morgan 2017). The moderator should identify the main factors of the study related to the participants. In addition, the researcher should ensure an effective communication process within the focus group for the best data quality (Barbour and Morgan 2017).

The focus group mechanism is very useful as an exploratory method and can be used in concept testing and evaluation. Detailed diagrams, concept descriptions, or product prototype testing can be discussed with the focus group participants. The researcher is allowed, therefore, to identify participants' needs and evaluation regarding the new concept. Accordingly, the new concept or product can be modified and updated to be more practical (Edmunds 1999).

This research employed a focus group in order to evaluate the enhanced ISRM model applicability and usability for large Saudi Arabian organisations by information security experts. In addition, focus group participants provided feedback on the validity, the accuracy, and the appropriateness of the research findings and to improve the enhanced ISRM model (O'Connor and Gibson 2003).

Similar to the approach used in interview participant selection used in this research, the researcher approached and recruited the focus group participants through LinkedIn and conducted online audio focus group via the WebEx and Zoom online meeting platforms.

The researcher must ensure data saturation in order to determine the sample size. The recommended number of focus groups for this type of research is three to four focus groups. In addition, the recommended size for online focus group is four to six participants in each group (Krueger 2015; Guest, Namey, and McKenna 2017; Hennink, Kaiser, and Weber 2019).

The ISRM model and key findings have been reviewed and evaluated by focus groups that resulted in further refining of the proposed ISRM model. Focus group participants included CIOs, IT managers, security engineers and security analysts with four to six participants in each of the three focus groups. Focus groups data were analysed using NVivo software.

3.5.3.3 Sampling and Participants Characteristics

A purposive sampling method was chosen to generate a heterogeneous sample in order to obtain the maximum benefit from adopting phenomenological interpretative approach. This enriched the diversity of exploration and facilitate the development of theory that

reflects the nature of ISRM across different organisations and sectors (Creswell 2013). Participant selection criteria was applied to ensure the heterogeneous purposive sampling approach in terms of level of experience, position, and organisation sector.

According to Balter et al. (2006), the recommended number of interviews is between five and twenty-five for a phenomenological study in order to reach data saturation. Saturation is "the most common guiding principle to assess the adequacy of data for a purposive sample" (Hennink, Kaiser and Weber 2019, p. 1483). It is the point where new information generates no or little change to the researcher's codebook in data collection and analysis (Guest, Namey and McKenna 2017). The researcher must ensure data saturation in order to determine the sample size. In this research, saturation was achieved after conducting eighteen interviews with eighteen participants. The data became redundant as most of the themes were mentioned and confirmed by more than one participant.

To prevent any industry-specific predisposition, organisations from different industries were chosen. Eighteen interviews were conducted in both private and public sectors organisations to collect data and achieve an understanding of the current problem. The participants' organisations were selected in such a way that there was at least one organisation from private, government, and semi-government sectors. They represent different industries including oil and gas, education, financial service, government agencies, manufacturing, and health services as shown in Table 3-3. No organisation is named in this research and all organisations remain anonymous throughout the research.

In this research, Group A participants are information security specialist that have been prequalified from the top 100 companies in Saudi Arabia 2017 as per Forbes Middle East (Top 100 Listed Companies in the Arab World 2018 2018), public universities, government agencies, and IT security vendors within Saudi Arabia. Participants included CIOs, IT managers, security engineers, and security analysts. Those participants were individuals with specialised insight on ISRM, and possessed the experience and perspective in information security management that this research wishes to understand. They had a variation from five years to more than twenty years of experience in information security field, different levels of positions, and different organisational sectors as shown in Table 3-3 and Table 3-4.

Table 3-3 Group A Participants Organisations Industry and their Job Roles

	Participants Roles					
Organisation's Industry	**CIO**	**CISO**	**Security Specialist/Lead**	**Risk Manager**	**IT Governance Specialist**	**Total**
Financial Services		1		2		**3**
Government Agency					1	**1**
Manufacturing	1					**1**
Education		1	1			**2**
Oil and Gas			1			**1**
Health Services			1			**1**
Retail			1			**1**
Total	**1**	**2**	**4**	**2**	**1**	**10**

Table 3-4 Group A Participants Details

Participant ID	Job Title	Years of Experience	Organisation's Industry/Classification
P1	IT and Security Head	13	Manufacturing/Private Sector
P2	Head of Information Security	15	Financial Institute/Private Sector
P3	Information Security Specialist	8	Oil and Gas/Semi-government
P4	Senior Information Security Specialist	9	Education/Government
P5	Information Security Advisor	15	Retail/Private sector
P6	IT Governance Specialist	5	Government Agency/Public Sector
P7	Chief Information Security Officer "CISO"	7	Education/ Public Sector
P8	Business Continuity Manager	12	Financial Institute/Private Sector
P9	Head Of Information Security Risk	11	Financial Institute/Private Sector
P10	Information Security Analyst	5	Health/Public Sector

Finding an appropriate sample of experienced information security professionals was one of the challenges of this study because of the specialised nature of the knowledge. In order to solve this problem, the researcher utilised the LinkedIn platform, which is a professional networking web portal, to search for verified experienced information security professionals working in Saudi Arabian organisations and connected with them to request an

interview. LinkedIn is a social networking website that focuses on business and professional networking. The aim of the website is to allow members to establish networks of people whom they know or by their qualifications (Rouse 2016, Johnson 2019). In general, LinkedIn profiles reflect the qualifications of an individual accurately, which can be a trustworthy tool for researchers. It is "a great source of truth if your research revolves around people who are employed" (Krueger 2018, p. 1). The researcher utilised LinkedIn's advanced search engine to locate potential participants according to their job titles, work locations, education, and total years of experience. After that, an invitation email, as shown in Appendix 3, was sent to approach the potential participants using LinkedIn and the university email and included the following:

- Introducing the researcher
- The research Introduction
- The interview purpose
- Interviews' expected duration
- The willingness to carry out the interview at the convenient for the interviewee
- Assuring the interviewee's anonymity and the privacy and confidentiality if the data collected

In the first round, the researcher approached approximately 23 Information security specialists who have 12 years or more of experience in the information security field or information security risk in Saudi Arabia. A reminder email was sent to the participants to motivate the non-respondents to indicate their intent to participate after ten days. The researcher received only two responses. The researcher then distributed another invitation letters through LinkedIn and via the university's email to approximately 31 information security specialists who had five years or more of experience in the information security field or information security risk in Saudi Arabia. The researcher received six responses from this outreach attempt. Other participants referred another two participants who showed interest in participating.

The researcher then requested participants who agreed to participate in the research to indicate a convenient date and time to conduct the interviews. All participants provided this data with a few rescheduling requests from some participants later on.

Before the beginning of each interview, a copy the consent form was sent to each participant as attached in Appendix 2. Each interviewee was requested to read and sign the consent form, thereby agreeing to participate in the interview and having it recorded. All eighteen interviewees were positive in their responses to the interview. They shared with the researcher their knowledge and experiences regarding ISRM in their organisations.

Ten participants were interviewed during a total of ten interviews, with each interview lasting between 45 minutes and 75 minutes. All ten interviews conducted were single-participant interviews. The interview script of questions was developed to guide the interview. Therefore, deviating from the script was allowed; some participants deviated from the script to provide additional information. Therefore, the researcher had to omit or re-phrase questions based on the participants' answers to previous questions.

Interviews were conducted via a university-provided online conferencing platform called WebEx. The reason why this medium was chosen is that "with face-to-face groups, it can be difficult to locate the participants for topics that seek specific populations" (Barbour and Morgan 2017, p. 240). In addition, recruitment of the participants was limited by geographic locations when searching for the appropriate participants through social network or snowball sampling in order for them to meet in the same place (Barbour and Morgan 2017). In addition, online interviewing ensures a high degree of anonymity in which participants are identified by their online service names. This potentially increases openness and honesty during focus group discussions as participants may not feel self-conscious because they are not recognizable (Edmunds 1999). Therefore, recruiting participants online for the focus group was considerably easier and more diverse because it provided the researcher the advantages of the face-to-face interview without travelling to participants' locations (Edmunds 1999; Barbour and Morgan 2017). In this research, two interviews were conducted via phone and the remaining sixteen interviews were conducted using WebEx online platform. Interviews were audio-recorded with the permission from the participants using WebEx recording tool and mobile phone voice recording to be used for transcription. Interview

recordings were saved on the researcher's personal computer, and a backup copy was stored on the university backup "Research R" drive. The transcriptions were stored in both hard and soft copy format.

At the beginning of each interview, the researcher informed the participants about the purpose of the research for them to gain a better understanding. After that, each participant was asked to talk about their experience and their organisation' working industry, and the organisation's IT structure to understand how IT security is managed within the organisation. Next, the concept of ISRM was discussed in order to gain a common understanding of its definition and scope. Participants were asked to define ISRM and whether or not their organisation complies with any ISRM standards. Finally, participants were asked about factors that could improve ISRM standards to best fit their organisations. Interview questions are available in Appendix 4). Data collected during the interviews were audio recordings of interviews and hand-written notes during interviews taken by the researcher.

The second group, Group B on the other hand, which involved eight participants representing IT security and consultation service providers or information system integrators who provide their services in Saudi Arabia. Those participants were individuals who have provided their services to Saudi Arabian organisations and possess the experience and perspective in information security that this research was exploring. They were a variation from nine years to more than twenty years of experience in different levels of positions, and they provided their services to different Saudi organisational sectors as shown in Table 3-5.

The same approach with Group B, eleven invitation letters were sent through LinkedIn and via university's email and personal email to IT security solution vendors, IT security consultation services providers, or information system integrators who had ten years or more of experience in the information security field in Saudi Arabia. The researcher received five responses. The remaining three participants were referred by previous participants. The characteristics of Group B participants are summarised in Table 3-5.

Table 3-5 Group B Participants Details

Participant ID	Job Title	Years of Experience	Customers Sector/ Classification
P11	Co-founder and Research and Development Manager	17	Private/SMEs and Large Organisations
P12	Cybersecurity Services Vice President "VP"	16	Private and Public/Large Organisations
P13	Network Automation and Security Specialist	9	Private and Public/SMEs and Large Organisations
P14	Co-founder and Senior Information Security Consultant	22	Private and Public/Large Organisations
P15	Security Solutions Sales Team Leader	12	Private and Public/Large Organisations
P16	IT Governance Specialist	12	Private and Public/Large Organisations
P17	Security Solutions Consultant	10	Private and Public/Large Organisations
P18	Security Solutions Sales Account Manager	9	Private and Public/Large Organisations

Eight participants were interviewed for a total of eight interviews, with each interview lasting from 20 to 55 minutes. Similar to Group A, all eight interviews conducted were single-participant interviews and the interview script of questions were developed to guide the interview and deviating from the script were allowed.

Figure 3.3 shows Groups A and B's timeline in which the researcher has started interviewing Group A and gathering initial data and then started interviewing Group B in the same matter. This allowed the researcher to overlap the two groups for a better understanding of the results.

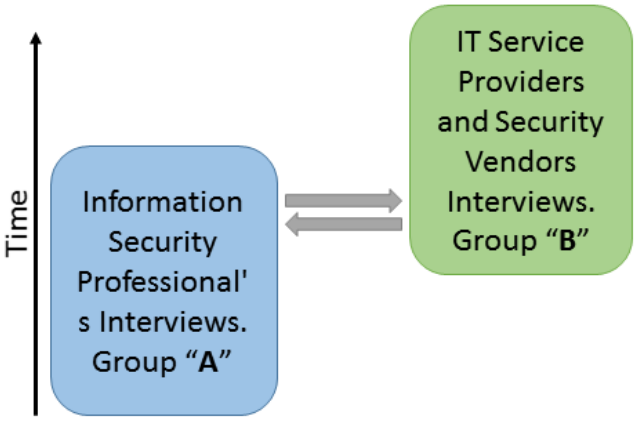

Figure 3.3 Group A and B Interviews Flow

Group B's interview questions were altered from the main interview questions for Group A. The reason is that Group B participants had different roles and therefore different perspectives and points of view of the research phenomena that support the data triangulation. Table 3-6 shows example of Group A questions and the related Group B questions.

Table 3-6 Group A and B Related Interview Questions

Group A	Group B
Does your organisation comply with any information security risk management (ISRM) standards or best practices?	Does your organisation comply with any international ISRM standards or best practices while implementing your systems for your customers?
	Do you have to comply with customers' standards and policies, and procedures?
How does your organisation ensure an adequate and appropriate level of information security over third parties?	Do your customers do regular audit for their IT systems?

Data collected from interviews are summarised and analysed afterward in Chapter 4.

3.5.3.4 Ethical Procedures

The nature of this research required the collection of information that security professionals might have considered confidential because this could potentially outline their organisation's security procedures and measures. Participants were assured of the confidentiality of the information they provided and the anonymity of their identity as well as that of their organisations. Therefore, all gathered data and information were kept confidential and have not been used for any purpose other than the scope of this research. In addition, the participants were requested to sign a voluntary consent form that has been approved by Curtin University's Ethics Committee. For future research requests, all gathered documents and data are securely locked in Curtin University's (R) drive.

The interview and focus group questions and protocols were examined and approved by the Curtin University Ethics Committee. The researcher informed the participants of their rights at the beginning of each interview as well as the information in the consent form. It was explained that their participation was voluntary and they had the right to withdraw from the research at any point during the interview without the need to explain the reason (see Appendix 1 and Appendix 4). The researcher's contact information and that of his supervisors were provided to the participants in case clarification was required.

3.5.4 Research Quality

In order to maintain the quality of this research, validity and reliability must be ensured (Creswell and Poth 2018). Golafshani (2003) stated that "trustworthiness of a research report lies at the heart of issues conventionally discussed as validity and reliability" (p. 601).

3.5.4.1 Validity

Unlike exploratory studies, validity is applicable to the explanatory studies of the semistructured interviews (Yin 2003). It ensures that the correct measures for the research concepts are utilised by using various data sources, individuals, and/or revisions. It is also very important to the research's trustworthiness.

In this research, validity is achieved through data triangulation. In this regard, Creswell and Poth (2018) highlighted that:

> In triangulation, researchers make use of multiple and different sources, methods, investigators, and theories to provide corroborating evidence. Typically, this process involves corroborating evidence from different sources to shed light on a theme or perspective. When qualitative researchers locate evidence to document a code or theme in different sources of data, they are triangulating information and providing validity to their findings. (p. 260)

To achieve triangulation, the researcher considered two different groups, A and B, for the semistructured interviews as described in section 3.5.3.1. Both groups' participants were experts in information security field and involved in security programmes from different Saudi Arabian organisations. However, they look at the problems from different angles. By doing so, the researcher enhanced the validity of the research, provided further interpretation of the research findings, and reduced the risk that the conclusions reflected limitations or biases of a single or specific source. In addition, it provided a broader understanding of the subject in its context.

In addition to triangulation, the researcher verified the data through the participants' feedback. Upon the completion of the interview, each participant had the opportunity to review their interview content in order to address any concern.

Finally, participants were provided an assurance of confidentiality and anonymity in which it would not be possible for anyone other than the researcher to identify the participants or their organisations. By doing that, participants were able to discuss their organisations' information security matters in a candid manner.

3.5.4.2 Reliability

Research reliability is the extent to which the research is consistent and stable and the output can be repeated in ways that results in the same output each time the research is repeated in the same framework, with the same population samples, and with the same

methods (Yin 2003; Creswell and Poth 2018). The reliability of data in the research is ensured by means of the following:

- The research design and processes and its implementation are explained in detail. This allows the research to be repeated to provide a similar result.
- The semistructured interview protocol was developed to ensure the reliability of the data gathered. The consistent use of the same interview protocol across all participants assists in providing consistency of data collection, thus increasing the reliability.
- All interviews were conducted in English after ensuring that all participants were fluent in the English language to minimise translation errors.
- Continuously comparing data to extract meanings and checking themes after each interview.
- Each interview was recorded, transcribed, and reviewed by the researcher. All interview recordings, transcriptions, and notes were stored in university's database as per the data management plan.

3.6 Data Analysis

Saldaña (2015) stated that analysis is "the search of patterns in data and for ideas that help explain why those patterns are there in the first place" (p. 8). Thus, data analysis involves preparing and organizing collected data, reducing the data into themes and categories through the coding process, and representing the results in a discussion, tables, and/or figures (Creswell and Poth 2018).

The data collected from the semistructured interviews were analysed to identify the main factors that influence, constitute, and reflect ISRM in the Saudi Arabian large organisation that contributed to the developed ISRM model in order to improve the information security posture in large Saudi Arabian organisations, to build the theory, and to identify gaps. Conversely, data from the focus group data collection phase were analysed to

enhance and confirm the developed ISRM model for Saudi organisations. Figure 3.4 illustrates the process of the data analysis adopted from Akinyode and Khan (2018).

Figure 3.4 Interview Analysis Process

Source: (Akinyode and Khan 2018)

The data collected in this research were analysed using content analysis approach. Content analysis is "a research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use" (Krippendorff 2018, p. 24). The researchers are able to study human behaviour through an analysis of their communications (Krippendorff 2018). Content analysis for qualitative data is an iterative process through which patterns and trends emerge (Strauss 1987). It enables researchers to analyse unstructured data for their meaning, qualities and expressive content in its original context and to move between the developed themes and the data collection that may guide the collection of data towards more useful information that address the research questions (Krippendorff 2018). Data were analysed by classifying or coding data into categories. Saldaña (2015) stated that qualitative research code is a word or short phrase that summarises, captures, and/or expresses attributes for a specific part of visual or language based data. Coding is a method that enables the researcher to organise and group similar data that may share similar characteristics (Saldaña 2015). Coding is also defined as categorical indexing (Mason 2017).

Figure 3.5, adopted from Krippendorff (2018), shows how the researcher drew distinctions within the collected data from the interviews and apply the content analysis to each interview individually to answer research questions. After that, the next step was to compare inferences drawn from texts for all interviews for each research question that yielded a conclusion (Krippendorff 2018).

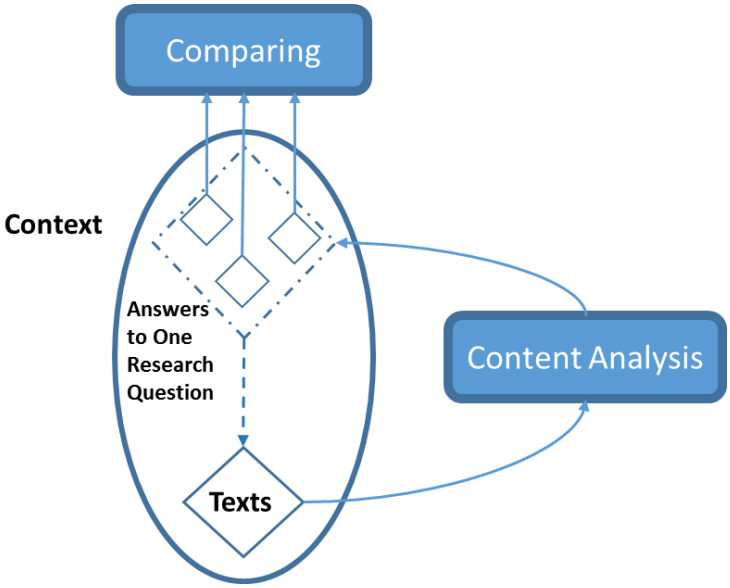

Figure 3.5 Comparing Similar Phenomena from Different Texts

Source: (Krippendorff 2018)

Each interview audio file was transcribed into text. After that, the researcher started the analysis process by listening to audio tapes and highlighting key elements for each interview in the interview transcription document. Thereafter, the transcribed text was coded using an iterative process that involved revisiting the categories and linking data to the research questions. Structural coding method by Saldaña (2015) was adopted to carry on coding for each interview. The structural coding method "applies a content-based or conceptual phrase representing a topic of inquiry to a segment of data that relates to a specific research question used to frame the interview" (Saldaña 2015, p. 130). The researcher utilised NVivo12 Pro to code the data under their categories.

Thirty-eight initial categories were created based on the coded data, which were linked to related research questions. Some data were coded into more than one relevant category if there seem to provide multiple and related ideas. The next step was developing themes according to the pre-defined categories. Saldaña (2015) stated that theme is the resulting set of elements from the data coding, categorising, and analysis. It guides to the development of theory when themes can be clustered together (Saldaña 2015). In order to allow the development of new themes, data and created themes were repeatedly reviewed and compared. This process was applied to each interview group.

The final stage was the cross analysis of both Groups A and B. Similar themes were combined and new themes merged in case of conflicts. After that, the researcher analysed the updated themes to achieve data triangulation. This resulted in the key findings of the research.

3.6.1 Ethical Considerations

Participants are the key data source in qualitative research. Thus, the treatment of the participants is a crucial issue. Consequently, ethical considerations become more important in qualitative research. Researchers should safeguard their participants against any damage and loss and strive to maintain their emotional well-being and dignity (Hossain 2011; Creswell 2014). The following basic ethical considerations apply to the treatment of this research participants in this study:

- Informed consent: Before information collection takes place, the researcher should guarantee that participants are clearly aware of the research process and give their permission to be part of it.

- No deception: Participant deception must be prevented entirely. The only reason for the deception is when there is no other way to address the research question and the research's prospective advantage far exceeds the respondents' risk.

- Right to withdraw: The researcher must ensure that participants are free to withdraw without fear of being penalised during data collection.

- Confidentiality: The researcher should keep all information and data obtained about the participants during the study completely confidential (Hossain 2011).

3.7 Limitations

Because of the nature of the research of information security, most participants were not open to discussing their security issues in a candid manner. The research designed the research question to be general security question that did not request exposure of any sensitive or confidential data of the participants' organisations.

3.8 Summary

This chapter examined and described the methodological approach and the design employed by the researcher to conduct this research. It discussed the research approach, research design, and the justification for the research approach design employed. In addition, the participants' sampling technique and data collection process were clarified. Finally, the methods of the data analysis and the processing of each data group were discussed in detail.

The next chapter presents the findings of the phase one data collection, the semistructured interviews, and analysis of the data that led to the development of the enhanced ISRM model.

CHAPTER 4. RESEARCH FINDINGS

4.1 Introduction

The previous chapter covered a range of research approaches and paradigms and explained in details the methodology adopted for this research. This chapter discusses the research findings from an interpretive, qualitative study that was conducted by interviewing participants who have been involved in ISRM activities in their organisation throughout their careers by presenting the phase one data, semistructured interviews, and analysing the collected data using thematic coding. In addition, it presents the ISRM implementation challenges, ISRM standards compliance, and factors that were incorporated to the initial ISRM model that resulted in the enhanced ISRM model.

4.2 Main Findings

All participants were asked the same questions and were encouraged to discuss their experiences, views, and opinions through open-ended questions. According to Weller et al. (2018), open-ended questions "explore topics in depth, to understand processes, and to identify potential causes of observed correlations" (p. 2). It allows participants to provide details necessary to understand the phenomenon.

To achieve data triangulation, the semistructured interview participants were divided into two different group of participants, A and B. Group A participants were information security specialists who were prequalified from the top 100 companies in Saudi Arabia 2018, while Group B participants represented IT security and consultation service providers or information system integrators who provide their services in Saudi Arabia.

Group A Data Analysis

The respondents from Group A were asked 22 questions, as shown in Appendix 4, which were divided into five categories. The categories into which questions were divided included:

- Demographics questions
- Information security team structure
- ISRM standards compliance
- Factors influencing ISRM standards effectiveness
- Factors improving ISRM standards to best fit Saudi organisations

4.3 Demographics Questions

The data collected from participants that related to demographics included their gender, experience, organisation type and industry, and their job title. All the participants were males, except one female participant, with five to 15 years of experience in the information security field as shown in Table 3-4 in previous chapter. This information allowed the researcher to determine their appropriateness for being an interview participant.

4.4 Information Security Team

Another set of information collected from respondents which related to information security team members number, to whom they report, and the actual organisation size is presented in Table 4-1.

It is clear that the oil and gas organisation has the highest number of information security team members. Following these organisations are education and financial institutes, where the least number of information security team members is the private “non-financial” sector.

Moreover, it indicated that financial institutes have more dedicated information security team members per organisation size compared to other sectors, while the least number of information security team members per organisation size is the non-financial private sector. Examples of participants answers as shown below:

"Security is outside the I.T department its independent function and independent department almost 8" P2

"My department which is related to any operational security things. We have more than 200 people" P3

It can be seen that the information security teams in financial institutes as well as oil and gas report to the chief of information security officer (CISO), while other government agencies, educational, and private sector information security teams report to their IT manager or head. There is one exception for one government agency where the information security team reported to the CISO. This particular government agency is a financial government agency. It is clear that financial institutes, including government financial agencies, are more mature in terms of information security team structure because they have a dependant information security department that is managed by an information security head. This would provide direct access to leaderships and decision-makers, resulting in management support, aligning information security initiatives with business objectives and programs, and less conflicts of interest with IT team.

Table 4-1 Information Security Team Members

Participant ID	Number of Information Security Team Members	Reporting to	Organisations Size	Organisation's Industry/Classification
P1	1	IT Head	5,000	Manufacturing/Private Sector
P2	8	CISO	2,000	Financial Institute/Private Sector
P3	200	CISO	65,000	Oil and Gas/Semi-government
P4	4	CIO	10,000	Education/ Public Sector
P5	0	-	5,000	Retail/Private sector
P6	8	IT Security Head	3,000	Government Agency/Public Sector
P7	14	CIO	10,000	Education/ Public Sector
P8	6	CISO	1,000	Financial Institute/Private Sector
P9	11	CISO	2,000	Financial Institute/Private Sector
P10	8	IT Manager	12,000	Health/Public Sector

4.5 ISRM Practices in Saudi Arabian Organisations

The researcher began the interviews by asking the participants several general questions regarding their perspective and experience about ISRM that include:

- Their understanding of ISRM
- Whether their organisation complies with any ISRM standards
- Whether their organisation is ISRM certified
- ISRM standards effectiveness

Each participant defined ISRM from a different angle; however, all of them made almost the same point that show their understanding and knowledge about ISRM. For example, **P1**

stated that:

> *"Identifying your assets, identifying your data, the most important data you have. Categorizing that data, knowing what it is, where it moves and the threats, identifying the threats to each of your assets holding your system's data" P1*

Similarly, **P2** related:

> *"Is a cycle to start identifying your risk, create risk register so You start and identify the risk then you of course information security risk. Then you have to do the risk assessment exercise and you have to come up with risk treatment plan" P2*

Also, **P3** said:

> *"It is the way of assisting the environment, the periodically assessment of the environment, and identify the threats that can't be removed or it is not acceptable. It is not in the acceptable level. And identify the impact and the weaknesses, and probability of it, and then treat the stress until it is accepted, and decrease the impact as much as possible" P3*

It is clear that all of the participants have had sufficient ISRM and information security-related experience throughout their working life. This information allowed the researcher to determine their appropriateness for being interview participants. Therefore, from the information provided in this section and in Section4.3 the selected sample, phase one participants, appear to have relevant experience to this research.

4.5.1 ISRM Standards Compliance

In responses to questions 7 and 8 with regard to complying with ISRM standards and ISRM certified, the data revealed that most of the organisations comply with one or more of different international ISRM standards or best practices such as ISO27001, NIST, COBIT, ITIL and PCI. For example, P2 and P4 stated that:

> *"NIST in one of the things we are using" P2*

> *"Yes, we comply with ISO27001/2013" P4*

Other participants declared that they comply with more than one ISRM standards as

indicated by P1 and P6:

"Yes. It's a mix of ISO and COBIT and ITIL" P1

"Yes, we do have an international best practice with us, and we do rely on our rules and regulations… We do not follow an independent module function, we follow both" P6

"Actually, we have to comply with many standards across the international or regulation here in Saudi Arabia, so we have to follow PCI, ISO. So, PCI, it's focused about the governance, documents, such as policy, security risk, like that and we have to follow also the international standards" P8

Table 4-2 provides an overview of ISRM standards and best practices compliance as well as whether they are certified or not. It is apparent from this table that nine out of ten of the organisations comply with one or more ISRM international standard and best practices. Moreover, seven out of those who comply with ISRM standards and best practices are ISRM certified. Closer inspection of the table shows financial institutes are the ones who are indeed concerned about ISRM compliance with at least two or more ISRM standards and being certified by two standards.

Table 4-2 ISRM Standards Compliance and Certification

Participant ID	ISRM Standard Compliance		ISRM Standard Certified		Organisation's Industry/Classification
P1	Yes	ISO27001 COBIT ITIL	No	-	Manufacturing/Private Sector
P2	Yes	ISO27001 PCI NIST COBIT	Yes	ISO27001 PCI	Financial Institute/Private Sector
P3	Yes	ISO27001 PCI	Yes	ISO27001	Oil and Gas/Semi-government
P4	Yes	ISO27001	Yes	ISO27001	Education/ Public Sector
P5	No	-	No	-	Retail/Private Sector
P6	Yes	ISO27001	No	-	Government Agency/ Public Sector
P7	Yes	ISO27001	Yes	ISO27001	Education/ Public Sector
P8	Yes	ISO27001 PCI	Yes	ISO27001 PCI	Financial Institute/Private Sector
P9	Yes	ISO27001 PCI	Yes	ISO27001 PCI	Financial Institute/Private Sector
P10	Yes	ISO 27001	Yes	ISO27001	Health/Public Sector

Interestingly, only one participant declared that his organisation, one in the private sector, do not comply with any ISRM standards:

"In fact, we don't have anything as of now. As I did mention, since I am the IT auditor as well for this company, so I am deriving the security aspect to start with" P5

Finally, what stands out in **Error! Reference source not found.** is that ISO27001 is the d ominant ISRM standard as all of the nine organisations comply with ISO27001, or it is amongst the standards they comply with.

4.5.2 Selecting Applicable ISRM Standard

Answers to question number 8 regarding the reasons of selecting ISRM standards to comply with showed different attitudes. The data indicated that there are many reasons for

selecting the applicable ISRM standard as revealed by participants when they were asked why they comply with certain ISRM standard, among others. For example, participant 2 stated that ISO27001 standard was selected because it is well documented and easy to manage in its implementation, while other standards are more technical:

"The beauty of ISO is that's its more focus on the documentation, so you have to build this documentation you have to make your organisation a bossy driven organisation…. The other standards is more technical standards or let's say, mainly focus more on technical operation" P2

Another participant reported that decision was driven by the availability of the ISRM standard consultation services, support, and popularity, which are the main reasons of selecting the right ISRM standard:

"At first you can see the market, the companies who provide services, ISO 27001 is very popular. A lot of consultation you can get. It's effective" P8

One participant declared that the selection of the ISRM standards was based on the nature of work and culture, as stated by participant 9:

"A committee combined between the business and the risk team decide based on the nature of work, the nature of culture and the country" P9

Participant 6 revealed that a third-party consultant was assigned to select and implement the ISRM standard:

"I don't know, many years ago there was a consultant who implemented this methodology" P6

Other participants revealed that they follow their organisation policy that has been set earlier and cannot be changed, as stated by participants 1 and 10:

"This was part of the whole IT policy. The whole IT policy was meant on these standards" P1

"It's a standard that we have to follow" P10

In summary, the data show a lack of proper methodology for selecting the applicable ISRM standard for most of the organisations. Almost each organisation has its own methodology, if any, to select an ISRM standard. Only one organisation considers the nature

of business and culture when selecting the ISRM standard. Another organisation focussed on the standard documentation, and another is driven by the market regardless of the appropriateness of the standard.

4.5.3 ISRM Standards Effectiveness

The data from the interviews showed that most of the organisations comply with one or more international ISRM standards and some of which are ISRM certified as well. Table 4-3 shows that two participants indicated that complying with international ISRM standards are effective and improve their organisations' information security posture because it provides guidelines which cover all risks and manage resources, budget, time, and effort as related by P2:

> *"I think it's effective because gives you the time to focus more, you know you cannot you will not be able to cover all risk from the organisation or security threats in the organisation. So, we have to manage your resources your efforts your time, your budget, you management support. So going with the risk-based approach or risk management approach, it helps a lot to focus more prioritising risk and to maintain these lists and update it in regular basis. So, it helps to utilise your resources, budgets, your time, your effort in the right direction" P2*

Three participants emphasised that the international ISRM standards are not effective and have limitations. For example, P7 argued that cultural differences influence ISRM effectiveness, and P4 indicated that it is not effective because the management is only concerned about being ISRM certified:

> *"Well, I would say still the culture is not the same, so I cannot see the value for that… I would say it's helping out a little bit but it's not that much." P7*

> *"Not effective at all to be honest… I feel like they just want to get the certificate, they get it and that's it" P4*

The remaining four participants stated that complying with the international ISRM standards is partially effective; for example, one participant indicated that complying with any standards is better than non-compliance with any, as stated by participant P1:

> *"Any known credited framework is better than having none" P1*

Another reason of the limitation of effectiveness of the international ISRM standards is its generic purpose of use as indicated by P9:

"Global standards usually talks generally about general organisation" P9

Table 4-3 ISRM Standards Effectiveness

Participant ID	Effective	Partially Effective	Not Effective	Certification	Organisation's Industry/Classification
P1		√		-	Manufacturing/Private Sector
P2	√			ISO27001 PCI	Financial Institute/Private Sector
P3		√		ISO27001	Oil and Gas/Semi-government
P4			√	ISO27001	Education/ Public Sector
P5	-	-	-	-	Retail/Private Sector
P6		√		-	Government Agency/Public Sector
P7			√	ISO27001	Education/ Public Sector
P8	√			ISO27001	Financial Institute/Private Sector
P9		√		PCI	Financial Institute/Private Sector
P10			√	ISO27001	Health/Public Sector

Table 4-3 shows that the only two organisations who agree that the international ISRM standards they comply with are effective are financial institutes. On the other hand, the three organisations who do not see the value of the international ISRM standards and believe that they are not effective are mainly public sector. Two of these three organisations are educational institutes, namely universities, and the other is a health institute, namely a hospital. The remaining four organisations agree that the international ISRM standards they comply with are partially effective. Three out of four organisations are classified as being in the private sector.

In summary, nine out of ten organisations comply with one or more ISRM standards with six organisations being ISRM certified. The most commonly adopted ISRM standard is ISO27001 as all of the nine organisations comply with the standard solely, or it is one of the ISRM standards that they comply with. Also, seven out of nine organisations are ISRM certified where ISO27001 is the most common certification. Finally, only two participants agree with

the value and effectiveness of the international ISRM standards, whereas the remaining participants either they partially agree or entirely disagree.

4.6 Factors Influencing the Effectiveness of ISRM Standards

In seeking to investigate the factors influencing the effectiveness of ISRM in Saudi organisations, this section presents the participants' feedback on the ISRM standards contributing factors to ascertain whether these factors influence the effectiveness of ISRM standards. From the literature, it was clear that ISRM standards are generalised and not regionally specific, which make them less effective (Al-Ahmad and Mohammad 2012; Al-Ahmad and Mohammad 2013; Flores, Antonsen, and Ekstedt 2014). P9 confirmed that international ISRM standards are generic and there are factors influencing its effectiveness:

> *"Global standards usually talks generally about general organisation…. The most important factor that I usually see in order for me to implement any framework is to understand with whom I'm working" P9*

Therefore, understanding the context of Saudi organisations business is crucial to develop an effective ISRM model.

4.6.1 People

4.6.1.1 National Cultural

From the interviews, the researcher observed that most of the participants agreed that national culture has direct influence on the effectiveness of ISRM. The data show there were different views regarding the national culture contribution to the successful of ISRM. For example, most of the participants agree that it is a major factor influencing the information security in Saudi organisations. This is illustrated by the following participant's comments answering whether Saudi culture influences ISRM effectiveness:

> *"I think culture impacts a lot on the environment; I have worked in different entities within Saudi Arabia, culture within the organisation makes a big difference. So, culture is important… Because we have certain set of culture, mentality, bureaucratic culture" P2*

Moreover, national culture has been linked to employees' behaviour and attitudes such as trust that may negatively influence organisations' information security, as commented by P5:

"Yes, very much. I'd say the first thing is the trust. A little bit which is nice. You trust people which is very nice but right now we are dealing with someone whom we don't know at all… but in Saudi Culture mainly micromanagement, following up closely what is happening, so, I think that is also sometimes blocks it" P5

The comment below illustrates that culture must be considered while managing information security risks because cultural differences may cause major conflicts in processing simple work tasks such as privacy control.

"The view and opinion about the privacy is defer from culture to another. So, when I consider so for example, let's say in Saudi, women consider their pictures very private things for them while other team member from another nationality or another culture, they didn't consider it as a very critical or very sensitive" P7

"It's not indirect… it has direct effect… We are behind the world. We are behind the world…. we know the culture and we know the global standards" P9

"Actually, yes, I agree with you… they don't care about the rules, about awareness…" P10

As discussed in Section 2.9, management theories and practices are culture-bound; therefore, management practices are not necessarily applicable to Saudi culture. P9 confirmed that due to the cultural difference, the international information security standards cannot provide a comprehensive solution for all security risk-related issues, resulting in a culturally modified standard as expressed in his comments below:

"… based on the global security framework, they say that it is the responsibility of the employee not to print screen something confidential, but with Saudi culture this is wrong. Usually, people rely at their work using print screens, so for them, it's a low risk; for us, it's critical. That's why we disable that in Saudi Arabia" P9

"The password complicity. In the global framework, usually, the password complicity contain special characters, capital letters, the small letters, numbers, minimum of 12 characters password which has to be changed every 3 months. In Saudi Arabia this is not practical because

people don't memorise their password, so in order for us to comply with this, we have to use the level of complexity but we add another encryption methodology which is the OTP, one-time-password. So, okay, I'm going to give you a space which you will view the password but also, I'd force you to follow the one-time-password, which is the password that will come to your mobile device" P9

Only one participant, however, did not see a direct impact of Saudi culture in ISRM effectiveness when they were asked whether culture has direct impact on ISRM effectiveness:

"No, I don't think…" P6

In summary, the data indicated that cultural factors influencing the effectiveness of ISRM standards in Saudi organisations were supported by 90 per cent of the participants. Some argued that it is the main factor that affects information security in Saudi organisations. Other participants agreed that it is one of the factors that affect information security in Saudi organisations.

4.6.1.2 Management Support

Table 4-4 below illustrates that 70 percent of the participants considered management support as an information security issue. Top, or upper, management was cited approximately 39 times throughout the interviews. Participants stressed that management support is essential when it comes to successful ISRM as indicated by the participant comments below:

"Top Management in all enterprises need to know the value of having a proper information security risk framework and investing in the correct people and technologies to achieve these goals" ***P1***

"The most important thing is management commitment and top management support" ***P7***

"Getting support from top management, that's it" ***P8***

Table 4-4 Management Support

Participant ID	Lack of Management Support	Organisation's Industry/Classification
P1	Yes	Manufacturing/Private Sector
P2	No	Financial Institute/Private Sector
P3	No	Oil and Gas/Semi-government
P4	Yes	Education/Public Sector
P5	Yes	Retail/Private sector
P6	Yes	Government Agency/Public Sector
P7	Yes	Education/Public Sector
P8	Yes	Financial Institute/Private Sector
P9	Yes	Financial Institute/Private Sector
P10	No	Health/Public Sector

The data indicated that top-down approach is the key for the successfulness of ISRM implementation, as stated by P5:

> *"Spread the knowledge by getting the buying from the top management. Tell them what is important; what is critical for an organisation. The top-down approach is very important" P5*

It is clear that the high level of management support would facilitate a proper investment in people and technologies, resulting in an improved information security posture.

One participant considered top managements' mindset is very critical because it directly influences their view regarding critical decisions. For example, if the top management have a certain beliefs, it is difficult to convince them to invest in information security because they do not see the value of such investment, as explained by P5:

> *"So, if I have a mindset that I am running a business for the last 80 years and it is doing well, why should I complicate my process? So, basically, no one is able to sell that idea" P5*

P4 stated that top management tends to comply with certain information security standards for the purpose of having the compliance certificate and to be the first certified

university in Saudi Arabia. They are not concerned about the real outcome of the compliance and whether the organisation has really improved its information security posture, as stated by P4:

"They want to be certified, we want to be one of the first certified universities" P4

P4 added that management do not give information security the appropriate attention or priority, which may lead to incorrect investment decisions resulting in a tremendous shortage in information security professionals in the organisation:

"We need more than 10 or 20 people to work in a security environment. The limitation of some management they don't take care much about security" P4

It was emphasised that management considers business operation over security, regardless of the severity of the risk they might be exposed. Moreover, realising the need for information security by the management and understanding its important was indicated as a major issue, as expressed by P5 and P7:

"The first thing, the biggest risk, to any organisation across Saudi Arabia is realising that information security is a need. I think that's the biggest risk… So, the sense of knowledge has to come in, the sense and urgency has to come in, and people have to realise that we need to make sure we are there to security practices" P5

"Well, they don't consider the threats… the new risk events that's going on in the cyber, so they didn't consider it as very critical for them. So, they consider the operation more than security" P7

One participant declared that management do not see the value of managing organisations' security risk, and, more importantly, the management considers the risk management practices as a stumbling block that hinders the business as stated by P9:

"The management and the business, usually pushes back when we come to identify risk with them, because again as I say, they always look at us as a show stopper. Whenever we come to them, they think that they we are trying to make their work complicated" P9

Moreover, the data show that the management reactive actions related to information security instead of proactive actions is a major concern in Saudi organisations.

Some participants believed that the management take an action only if something happens, as commented by P1, 4, and 5:

"They're mostly reactive. If something comes up in the news, then it becomes a concern" P1

"They are reactive for example unless something happens, they don't see the value" P4

"These are all the basically firefighting issues" P5

Reactive managers have greater likelihood of making costly mistakes because they react after a crisis occurs (Proactive Vs Reactive Task Management 2020). A reactive mindset which ignores warnings and dangers could produce severe consequences for the competitive status of the business. It has been found that proactive information security investments are more effective at reducing security failures than reactive investments (Kwon and Johnson 2011). Thus, a management with a reactive mindset toward developing a strategic information security program could lead the organisation to catastrophic consequences.

On the other hand, a few participants indicated that top management are becoming more supportive especially in the recent years as shown in the comments below:

"I think in the last years, the top management become more supportive in terms of information security project and information security initiatives. So, they are more supportive" P6

"So, we have also the buy in and the commitment from the management" P2

In summary, the data indicated that top management support is vital for the success of ISRM implementation in Saudi organisations. It was revealed that top management do not consider information security to be a priority when it comes to planning and investment for the favour of operations. Further, it was concurred that top management's proactive mindset and behaviour is vital for an effective ISRM resulting in improved information security posture for the organisation. In addition, understanding the value of the risk management of information systems by top management is the key to a top-down approach for successful information security management.

4.6.1.3 Education and Training

The data showed that 70 percent of participants emphasised that there is a serious shortage in specialists, experts, and highly qualified ISRM Saudi professionals as expressed by the participants:

"We don't have expertise… one of the main issues that I've seen in this company or other companies… once they found any risk in the company, they don't find the solution to mitigate the issue… we don't have that expertise" P3

"Still there is a lack of the human resource coming into the IT security" P5

"And you can see that a lot of non-Saudi work in information security, because of the lack of resources" P6

"The problem is the lack of information security specialist" P7

"A very few people in Saudi, they know risk management" P8

It was indicated that the most challenging step in ISRM implementation in Saudi organisations is finding skilled information security risk professionals who are able to perform the ISRM tasks. The data also showed that this problem has become serious because they are required to hire Saudi nationals in information security positions in most Saudi organisations:

"To find the right experienced and eligible guy to conduct that risk assessment. Once you have this this kind of resource or qualified resource you would be able to complete the cycle smoothly" P2

"It is not allowed to hire non-Saudis specialty in security division" P10

P4 stressed that his organisation needs at least 10 more information security specialists in order to cover the shortage. Referring to Table 4-1, P4 organisation information security team are 4 members; therefore, they need to increase the team by at least 250 percent:

"We need more than 10 or 20 people to work in a security environment" P4

It was argued that the reason of the shortage in Saudi national information security and risk management specialists is the unavailability of information security and risk

management-related educational programs as expressed by the following comments:

"We should have proper education and awareness, then you can have a successful project" P1

"First of all, maybe we don't have in our universities or an education here, of course, it's about risk management. We don't have that sort of thing" P8

P6 revealed that the lack of specialised information security and risk management training centres is another reason for the shortage information security and risk management specialists as noted by the following comment:

"There is no master's degree in information security, there is no bachelor degree in information security. Even training, you cannot find adequate training centres" P6

It can be understood from P7's comment that the lack of the risk management education could contribute to the lack of understanding of ISRM processes resulting in hindering the risk management tasks progress.

"Well, the lack of understanding, the value of risk assessment… they don't have some knowledge in risk assessment, they don't understand it" P7

The data revealed that top management's lack understanding of the importance of the risk management education value, which affects the success of ISRM projects as stated by P1 below:

"I think the most important thing is education, top management and all enterprises need to know the value of having a proper information security risk framework. If it comes from top with upper chain management with proper education and awareness, then you can have a successful project" P1

Moreover, misunderstanding risk, which can be related to the lack of education, was repeatedly mentioned by some participants. P6 emphasised that employees as well as some managers do not understand risk and its importance for the organisations. It was confirmed by P8 and P7 that the risk management concept is misunderstood. Further, it was highlighted that some employees would think that risk is something harmful, and therefore they try to

avoid dealing with any risk tasks. It also indicated that there is a common misconception that risk management is the risk department or IT responsibility. This is probably a consequence of the lack of education:

"You know, when you come up with those ideas… even the management will not understand why you are doing that" P6

"They don't know what risk is… People doesn't understand what risk is. They think risk is something bad…They don't want to spend money for risk management… Risk management is the responsibility by everybody, not by risk department or security department alone" P8

"It is the understanding of the people, so the culture, the employee culture is still not mature to understand risk assessment and to analyse risk" P7

The data indicated that that the risk rating task is quite challenging. Risk ratings are typically used to evaluate the likely impact of an event on an organisation's critical data and also be used as part of the decision-making process. The data revealed that the process of assigning a risk rating by the risk owners lacks realistic reasoning due to the lack of risk management needed skills. It was indicated that the consequences of the improper risk rating of the data assets could negatively affect the risk management activities. For example, some of the risk owners who are involved in assessing their data assets risks believe that all of their data assets are very critical and therefore they do not provide the actual risk value by scoring their data assets with a high rate while in reality they are not, as stated by P7 below:

"Well… people there don't understand let's say qualitative risk. The issue is they don't see numbers between safe values, so they thought that it is hard to convert it to numbers. So, one of issues we face if we ask, let's get a value or classify your assets based on criticality and the integrity and ability… they always say their systems or their assets or data they consider it always 5, 5, 5… five for confidentially, five for integrity, five for criticality. So, while we as security governance we thought that this is very critical since we experience that, we have on good knowledge, so we thought that this is not the real value. So, every asset owner see his asset as very critical and very confidential and very sensitive" P7

Another example of improper risk rating due to lack of risk management skills is expressed by the following comments:

"If I see one of the machines try to spread some virus over the network… So, we do not we have the equipment that can rate the level of risk so we

rate based in our experience" P4

"The other challenge its during risk rating and acceptance from the risk owner because you sometimes come up with certain risk and if there is a disagreement with the risk owner it would be hard you know to do the risk rating and to implement that recommended risk control" P2

Moreover, the data shows that unrealistic risk management assumptions and decisions could be due to the lack of risk management skills as indicated by the following comments:

"Some companies are afraid of taking risks because they don't want to be exposed to the outside" P3

"These people who have been working for the company for the past two or three decades, they are hesitant to move to a different technology or they are hesitant to implement the controls?" P5

It is clear that the lack of proper training and education seems to contribute to this issue. This is true for all level of employees as expressed by P7:

"Although we have employees from different education background let's say the from a technician up to a professor, let's say, they're always involved in informed risk assessment and we don't have some knowledge in risk assessment, they don't understand it" P7

One participant suggested that culture could be the reason for lack of risk management practices understanding as indicated by P7 below:

"The employee culture is still not mature to understand risk assessment and to analyse risk" P7

In summary, the data revealed that the shortage of information security and risk management specialists due to the lack of educational programs in information security and risk management. It was indicated that all sectors encounter this problem. Proper education programs seem to be the solution to overcome the shortage of Saudi of information security and risk management specialists.

4.6.1.4 Ethical Culture

There were some participants who indicated that unethical behaviour can be a factor that influences ISRM effectiveness in Saudi organisations. Unethical behaviour can be related to ethical culture (Kaptein 2011). Ethical culture is defined as the characteristics that stimulate

employee's ethical conduct (Riivari et al. 2012). It is considered "an important if not the most important component of the organisational context to account for unethical behaviour" (Kaptein 2011, p. 844).

One participant reported that some employees are not responsible when dealing with confidential data and may perform unethical behaviour. For example, some employees misuse confidential data by taking a screenshot or printing a screen displaying confidential data and then sharing this data with others. The participant indicated that the only solution for this behaviour is to disable the screenshot feature on the organisation's computers as commented below:

> *"In a global low, print screen is something normal, everybody can do that... In Saudi Arabia, a huge number of information leakage come from the print screen, so based on the global security framework, they say that it is the responsibility of the employee not to print screen something confidential, but with Saudi culture this is wrong. Usually, people rely at their work using print screens, so for them it's a low risk, for us it's critical. That's why we disable that in Saudi Arabia" P9*

Another participant indicated that behaviour related to privacy is a concern in his organisation. The participant claimed that some employees could intentionally access business related data for personal purposes as stated by P8:

> *"Privacy is an issue when it comes to users behaviour, some are not really aware of the data privacy… they access data for personal purposes… this is a serious issue to be honest" P8*

These results suggest that unethical behaviours could contribute ineffectiveness of the ISRM. It was suggested that imposing new controls such as blocking screenshot feature is one of the solutions to this behaviour.

4.6.2 Process

4.6.2.1 Information Technology Audit

Table 4-5 illustrates participant's response regarding information technology audit. That data indicated that the majority, or ninety percent, of the organisations perform information security audit on their IT systems to assess the effectiveness of the existing

information security measures and to identify potential risks.

Table 4-5 Information Technology Audit

Participant ID	Information systems Audit	Internal/External	Organisation's Industry/Classification
P1	No	-	Manufacturing/Private Sector
P2	Yes	Both	Financial Institute/Private Sector
P3	Yes	Both	Oil and Gas/Semi-government
P4	Yes	Internal	Education/ Government
P5	Yes	Internal	Retail/Private sector
P6	Yes	External	Government Agency/Public Sector
P7	Yes	Both	Education/Government
P8	Yes	Both	Financial Institute/Private Sector
P9	Yes	Both	Financial Institute/Private Sector
P10	Yes	Internal	Health/Public Sector

Only one participant stated that his organisations do not perform information technology audit although they conduct other audit practices such the financial audit as stated by P1:

"Audit do not take place… the only other that takes place are the financial audits" ***P1***

It is clearly understood from participant feedback that the top management do not see the value of information technology audit.

Moreover, Table 4-5 illustrates that fifty percent of the organisations conduct both external and internal information technology audit, while three organisations conduct internal auditing and the remaining organisations conduct external audit as related below. It is clear that all financial institutes, along with oil and gas organisations, are concerned about their information technology audit as they do external and internal audit exercises.

"Our internal team they are able to conduct these exercises but in

certain cases we might invite someone from outside for example in annual basis" P2

"So, we invite different companies sometimes based on Riyadh but sometimes outside the country you know, regions, because at the end of the day we're trying to get the most value out of this exercise so having different fresh eyes every day, every time has a lot of value." P8

Overall, the data revealed that the majority of Saudi Arabian organisations conduct information technology audit with half of the organisations conduct external and internal information technology audit. It was indicated that top management in some organisations are not concerned about the information technology audit practices because they are not aware of its value.

4.6.2.2 Roles and Responsibilities

Unclear roles and responsibilities were highlighted by 30 percent of the participants as a factor that influence ISRM effectiveness in Saudi organisations. Many organisations, especially governmental agencies, encounter these problems. One participant stated that a clear organisational structure as well as roles and responsibilities is crucial to improve ISRM effectiveness in Saudi organisations. It was indicated that poor job description details, organisational structure, and roles and responsibilities can influence ISRM effectiveness as expressed by P4:

"There is no clear structure for most of the government sector agencies… The system is old and everything is centralised. No clear organisation structure… Reporting problems and structural problems" P4

This participant stated that the lack of clear roles and responsibility is due to the lack of proper organisational structure and centralisation as well as outdated policies and procedures. Further, P2 suggested that the lack of understanding of the roles and responsibilities is another factor that can influence ISRM effectiveness:

"Understanding their roles and responsibilities" P2

Meanwhile, it can be understood from P3's comment that some employees' behaviour towards risk is directly affected by their understanding their responsibilities. For example, if an employee believes that this risk is their responsibility, they would act

accordingly to mitigate it and be held accountable. However, from P3's statement below, it seems that due to the lack of understanding of roles and responsibilities, tasks such as risk mitigation are not performed due to unclear responsibility:

"This is a risk, and this is how to mitigate. No one say it because no one want to be responsible" P3

In summary, the data revealed a new finding that influences ISRM in Saudi organisations. It was indicated that unclear roles and responsibilities could affect the risk management progress due to lack of clarity. This role ambiguity can lead to many problems, such as poor communication, missed deadlines, and more. This can affect the quality of work being produced because employees will not be able to provide their best work.

4.6.2.3 Information Security Knowledge Sharing

Table 4-6 shows that 70 percent of the participants stated that they do not share information security knowledge with other organisations:

"Outside the organisation, no" P6

"Not that much, I would say. I just check with my colleagues and the same with my team, but formally, no" P7

"Actually, no" P8

"We are sharing the security between us only" P10

"For government sector, no…"

It can be understood from the data that financial institutes and oil and gas are the only sectors which adopt the information security knowledge-sharing practice. However, the data indicated that they neither have a formal policy nor a clear procedure to follow as expressed by P2:

"The central bank communicate with all banks… for anything that could be happening… But we do not have clear methodology" P2

Table 4-6 IS Knowledge Sharing

Participant ID	Sharing of IS knowledge	Organisation's Industry/Classification
P1	No	Manufacturing/Private Sector
P2	Yes	Financial Institute/Private Sector
P3	Yes	Oil and Gas/Semi-government
P4	No	Education/Public Sector
P5	No	Retail/Private sector
P6	No	Government Agency/Public Sector
P7	No	Education/Public Sector
P8	No	Financial Institute/Private Sector
P9	Yes	Financial Institute/Private Sector
P10	No	Health/Public Sector

The results confirms the findings of the previous work discussed in section 2.8.2.1 by Almuqrin et al. (2020) and Chandran and Alammari (2020), who examined the knowledge-sharing behaviour in Saudi organisations. The results show that there is a low level of knowledge sharing in the country.

In summary, the data revealed that there is a low level of information security knowledge sharing adoption among many Saudi Arabian organisation. Oil and gas and financial institutes are an exception as they tend to practice knowledge sharing. However, there is no clear policy and procedure to follow.

4.6.2.4 Cross-Departmental Collaboration

Cross-departmental collaboration involves joint activities between departments in an organisation by working together rather than separately. It employs sharing public authorities, information, goodwill, activities, and resources to improve capabilities or to resolve issues utilising public policies (Liu and Zheng 2018).

The data revealed that thirty percent of the participants indicated that the lack of

cross-departmental collaboration could influence ISRM effectiveness. It was indicated that poor communication, dependency, and delay in response between departments are major issues that security specialists face in Saudi organisations. More importantly, culture contributes to this behaviour that could lead to major delay, which could be for years, in replying to information security requests as commented by P2:

"There's a dependency on other departments and it takes time… So usually, these kind of cycles take at least two years because it's a cultural thing so it's not something fully controlled by our department" P2

P6 confirmed what P2 stated regarding communication issues among departments and added that risk management activities—especially risk assessment—could be negatively affected by the lack of proper communication between departments.

"There is lack of communication between the departments, for example, got a new technology which you were not aware of it, and it was not a part of assessment scope Think this is the main things, the problem with the communication" P6

Lack of cooperation between departments due to unclear roles and responsibility at departments level was highlighted by P4 as one of the major issues that influences ISRM. P4 emphasised that there is a huge gap of knowledge between departments teams in terms of services provided from one department to another and related procedures. This gap of knowledge seems to affect the cycle of risk management process, especially risk assessment as commented below:

"There is no cooperation between departments… departments should know how to communicate and present the service to other departments and which task is the responsibility of which department… how they're going to present the service to other department and which task That is required from other departments to specific department… there is no agreement between different departments with the organisation to resolve any security issues within a time frame for example, in order to run these security technologies we need other departments to cooperate" P4

This suggests a different perception of factors that influence information security in Saudi organisations from what the researcher founds in the literature. Poor communication, dependency, lack of cooperation, and delay in response between departments are results of lack of cross-departmental collaboration. It is clear from the responses that the lack of cross-

departmental collaboration could negatively influence the ISRM effectiveness and therefore expose the organisation to information security risk.

4.6.2.5 Information Security Policy (ISP)

The results, as shown in Table 4-7, indicate nine out of ten organisations have an information security policy in place as indicated by the following statements:

"Yeah, we have a security, we follow the ISO 27001 standard, information security, it's required in many offices" P8

"Yeah, we have our private policy… It came from the top management" P10

Table 4-7 Organisations Public Information Security Policy

Participant ID	Corporate Information Security Policy	Regularly Updated	How Often	Organisation's Industry/Classification
P1	Yes	No	-	Manufacturing/Private Sector
P2	Yes	Yes	Annually	Financial Institute/Private Sector
P3	Yes	Yes	Annually	Oil and Gas/Semi-government
P4	Yes	Yes	Annually	Education/Public Sector
P5	No	-	-	Retail/Private sector
P6	Yes	Yes	Annually	Government Agency/Public Sector
P7	Yes	Yes	Annually	Education/Public Sector
P8	Yes	Yes	Annually	Financial Institute/Private Sector
P9	Yes	Yes	Quarterly	Financial Institute/Private Sector
P10	Yes	Yes	Biannually	Health/Public Sector

One organisation does not have an ISP and represents private retail sector. Another private sector organisation has an ISP; however, it does not regularly update it.

Moreover, the results shows that six out the nine organisations update their policy

annually while the remaining two organisations update their policy biannually and quarterly. It is clear that almost all of the organisations in Saudi Arabia already have a published ISP and it is regularly updated. However, private sector organisations have less of a concern about having a published ISP or update it in regular basis.

4.6.3 Technology

4.6.3.1 Information Security Awareness

The data indicated that the low level of information security awareness was repeatedly mentioned as a major factor that influences information security in Saudi organisations. Ninety percent of the participants commented that awareness directly influences ISRM in their organisations as commented below:

"Proper education and awareness, then you can have a successful project" P1

"In general, I think, there is a problem with the awareness" P6

"Awareness is the keyword… it depends on the awareness level" P7

"The low level of awareness, people doesn't understand what is risk" P8

"They don't care about the rules, about awareness" P10

To show the importance of the information security awareness, Participant 9 stated that his organisation's greatest security risk is:

"Lack of awareness" P9

Other participants believe that the low level of awareness among employees could lead to underestimating existing risks and their consequences and, therefore, make it more difficult to react against potential risks in a timely manner, as indicated by the following comments:

"Sometimes we detect malwares in other departments system and we notify them to react immediately but they don't respond or give it a low priority" P4

"In general, across the Saudi Arabia IT security is the least important. IT operations is the top priority" P5

"They don't want to invest time to classify the data because they don't see the value" P7

"Usually staff want to generate money, bring more business, but they don't care about security, which lead to a lot of issues within the security module" P9

Three participants revealed that the low level of information security awareness exists not only among non-managerial employees but also among the top management as expressed in the following comments:

"The issue is that most of the managers they think the security is only antiviruses… They just want to be certified; they want to be one of the first certified university" P4

"Awareness, awareness to the top management…" P5

"…they think that security is a tool" P8

Further, P5 indicated that top management lack of awareness hinders a proper information security investment including the adoption of an ISRM program which could potentially lead to high risk of information security incidents. He stated that awareness is the key to convince top management to consider a proper investment in information security programs and solutions:

"Awareness to the top management… Basically, awareness to the top management" P5

As a consequence of low awareness, security risk professionals face obstacles that hinder them in performing certain risk-related tasks. For example, P9 stated that as information security risk professionals, other employees within the organisations consider them "show stoppers" that complicated work:

"Usually treats us in a way that we are the show stoppers for them, we usually make their work complicated. They don't look at us comfortably" P9

Moreover, it was revealed that top management considers acquiring technology solutions as the solution for information security. Therefore, they invest in the advanced

and expensive technology without considering other related factors. It is believed that once these technologies and tools are purchased and put in place, they would provide a full protection. This behaviour can be related to the lack of awareness on information security. P1 stated that when they have information security risk issues, their decision-makers tended to invest in tools and technologies rather than people although these tools will not solve the problems.

"There is a lot of interest in technologies and technologies won't solve existing problems and they're not replacements for an actual risk management framework…. So, what I see is that there is more investment in technologies than in people which is, I think, not a solution" P1

"It's a lot of money; it's a lot of money… basically, they spend a lot of money in tools, new tools and technology" P3

P4 emphasised that the public sector does not have proper technology management teams which can utilise the information security tools and technologies to achieve the desired results. The management concern ends by acquiring the best tools and technologies that even some financial institutes cannot afford.

"The problem with government sector is that they purchase all new technologies but the problem is how to manage them afterward…They care about spending and buying the tools but they don't care about how to make this tool effective…We spend a big amount of money on technologies but we don't manage them well…We have some technologies that some banks cannot even afford but they are not utilised well" P4

Similarly, P5 stated that they invest in the best technologies; however, they do not practice proper management such as device monitoring and vulnerabilities analysis to address risks and therefore assess them accordingly.

"We have the best of the best devices, but to monitor the devices to make sure the vulnerabilities are addressed, we don't' have anything else after at all" P5

To overcome this issue, P3 believes that their organisation should provide proper training and awareness programs for their employees. This results in better information security awareness and improves ISRM effectiveness as expressed by the following comments:

"Employees must take training regarding security, how to survive

phishing emails or phishing SMS that comes to your cell phones" P3

In brief, the data indicated that the low level of awareness is a main concern in Saudi Arabian organisations. Culture and education play a major role on the awareness level on the entire organisations. It is clear from the responses that a low level of awareness influences executives in making poor information security investment decisions, and employees to make actions that could expose their organisations to higher information security risks.

4.6.3.2 Third-Party Management

The data show that six out of ten participants confirmed that they outsource one or more of the IT-related activities and operations to a third-party as shown in Table 4-8 and expressed below:

"We have some, some tasks already outsourced" P2

"Yeah... Mostly we outsource the IT operation completely to the contractor" P7

Table 4-8 ICT Outsourcing

Participant ID	ICT Outsourcing	Organisation's Industry/Classification
P1	No	Manufacturing/Private Sector
P2	Yes	Financial Institute/Private Sector
P3	No	Oil and Gas/Semi-government
P4	Yes	Education/Public Sector
P5	Yes	Retail/Private sector
P6	Yes	Government Agency/Public Sector
P7	Yes	Education/Public Sector
P8	No	Financial Institute/Private Sector
P9	No	Financial Institute/Private Sector
P10	Yes	Health/Public Sector

It was revealed that ICT outsourcing includes information security operations, risk

management, and auditing activities as stated below by the following participants:

"We have our DDOS mitigation service is already provided by one of our external consultants. You know the DDos part of our SAC It's already outsourced so we have… They monitor 24/7 any abnormal or suspicious activity in our intranet interface" P2

"Yes, we do for penetration testing and the audit… we do the IT audit from the external auditors" P5

P4 revealed that his organisation outsources all of the IT operations and related activities to third parties, such as information security management activities, which indicates that P4's organisation's IT operations and related activities such IT security are fully controlled and managed by a third-party. This is accomplished by signing a contract with a third party to provide the organisation with IT teams, as shared below:

"All the security stuff are not a university staff… Even the chief information security officer" Participant 4

All participants confirmed that they had policy and procedures to follow when dealing with third parties to ensure adequate level of information security regarding third parties. It was indicated that some organisations enforce their policies through third parties by signing a contract or agreement that ensure an adequate level of information security, as stated by the following participants:

"We do have a policy regarding third parties…. we have an NDA a nondisclosed agreement… we have also a certain policy they have to comply and provide their confirmation" P1

"They must obey to the information protection manual, so anything has to be by the book" P3

"One of our policies is mainly for vendor management from security point of view… So usually we have a contract" P2

"Yes, we do. In fact, in every contract there is information security clause as well which we sign it across with our suppliers" P5

Some organisations perform a third-party security assessment prior to commencing any job as a pre-requirement for awarding contracts to ensure an appropriate degree of information security compliance. It was indicated that this would provide clear image of the third-party information security compliance and capability and therefore supported the

decision whether to work or continue working with the same third-party or not as expressed by P6, P7, P9, and P10:

> *"We do a third-party assessment. This include an access control review including the VPN, including the non-disclosure agreement. The third-party also, there should be a policy for handling the third-party. That should be shared before doing any kind of IT projects" P6*

> *"Usually, we do a third-party security assessment quarterly basis and we do vendor management reviews…. based on these certificates the third-party would be eligibly work with us or not" P9*

> *"Yeah, actually, we don't give access for a third-party until, I mean, they bring some papers and fill the forms and do many things to be sure they're responsible for these things… we have like a form, with the policies and they have to sign it before we give them access or admin or anything related to security" P10*

> *"Yeah, we do. We have signing NDAs and we do risk assessment in a quarterly basis. And also, part of the main contract with the vendors we have them our SLAs between the organisation and the contractor" P7*

However, P1 revealed that some of the third parties do not adhere to rules that they have been requested to follow. The participant stressed that they need to monitor the third parties to make sure that policy and procedures are followed by continuing to audit and enforce procedures, even if they claim that they follow the rules:

> *"Vendors don't follow these practices, from what I've seen… only if you ask them and only if you can enforce it and audit it because maybe they tell you, ok we don't share passwords, we don't do this or that, and you might find out that they do" P1*

Moreover, it is clear that third parties are not aware of the security policies and have a lack of information security awareness as well. P5 argued that they are not concerned about the security aspects of the job they work on. These vendors just want to complete the task and deliver without following the security policy and procedure. It was indicated that third parties seem to have staffing shortage issues in skilled information security professionals as well. This action could potentially expose Saudi organisations to a potential security risk.

> *"Most of the times, the vendors come to configure the firewall, configure the servers, and they themselves they are not aware of the security aspects. They just configure it from point A to point B and the traffic has to flow, that's it. But they don't look it from the auditor's eyes.*

They don't look at form the security eyes. Like, traffic flowing and can be exploited. What is the best way to configure a device? How a device can be hardcoded. There is a very shortage of the skill set of the knowledge" P5

In summary, the data showed that many organisations outsource their ICT and information security services. The level of outsourcing varies from very limited services such as auditing and penetration testing to full ICT services outsourcing, including ICT and information security staff. Moreover, the data revealed that all organisations perform a level of information security check to ensure third-party eligibility. Some organisations are very strict and perform security assessments prior to start working with third parties as well as signing non-disclosure agreements or/and contracts. They continue to monitor the third party by conducting a regular security assessment to ensure their adherence to the provided rules and also enforce their policies which have been shared previously with the third party. On the other hand, other organisations are less concerned about third-party management. They might just request a non-disclosure agreement to proceed with a job. This low level of third-party management is not adequate to ensure that the third party is eligible to complete the job from information security point of view and could potentially expose organisation to unexpected security risk.

4.6.3.3 Risk Management Process Automation

Complicated risk management processes were revealed as a factor that influences ISRM effectiveness in Saudi organisations. The data revealed that performing manual risk management activities such as utilising spreadsheets may complicate the risk management process as commented below:

"We use spreadsheets… we perform the first life cycle of risk management manually" P8

It was suggested that simplifying the risk management process is may help overcoming its complexity as commented by P7:

"Simplifying the process itself is the key" P7

Further, P2 argued that the automation of the risk management process may simplify the process to overcome this problem and improve the risk management effectiveness

tremendously. It was indicated that a full risk management automation lifecycle, starting from risk identification to risk closure, provides more insight of organisation current risk status and management can track risk process, generate reports, and set deadlines for certain risks as indicated below:

"I think automation… if we automate the risk management life cycle form identification until the closure of the risk assessment it will be very helpful… track and report and dashboard, follow up in automated way and also to escalate in case certain controls not implemented in certain time frame it would be escalated to top management so top management in any time they would be aware of the risk status and posture of the organisation" P2

P2 added that managing the information security risk should be integrated with all the organisation risk management activities in order to have centralised risk management as commented below. This indicated the importance of risk management automation.

"Integrate all risks so to move from all the information security risk to be corporate or enterprise risk management. So, in this case we'll be able to aggregate all the risk on the organisation in one central register" P2

The data revealed that assets management is challenging in some organisations in Saudi Arabia. It was indicated that due to poor assets management, some organisations cannot locate their IT assets and their actual users. Additionally, it is difficult to backtrack the assets arrival date. Therefore, when a security vulnerability has been detected as such, either the asset cannot be located timely to be rectified or cannot be located at all.

"It's hard to identify who's the user and where's location of this machine or this PC" P4

"We don't know when assets actually come" P6

In sum, the data showed that some Saudi Arabian organisations encounter the issue of the complexity of risk management process such as IT assets management which may influence ISRM effectiveness. It was suggested that there is a need to simplify the entire risk management process. It was therefore indicated that automation is the solutions to simplify the risk management process resulting in better ISRM effectiveness.

4.6.3.4 Measuring Information Security Awareness

Table 4-9 below shows that sixty percent of the participants confirmed that they practice measuring information security awareness in their organisation. It is clear that private sector, excluding the financial institute, are less concerned about measuring employees' information security awareness followed by the public sector.

Table 4-9 Measuring information security awareness

Participant ID	Measuring ISA	Organisation's Industry/Classification
P1	No	Manufacturing/Private Sector
P2	Yes	Financial Institute/Private Sector
P3	Yes	Oil and Gas/Semi-government
P4	Yes	Education/Public Sector
P5	No	Retail/Private sector
P6	Yes	Government Agency/Public Sector
P7	No	Education/Public Sector
P8	Yes	Financial Institute/Private Sector
P9	Yes	Financial Institute/Private Sector
P10	No	Health/Public Sector

The data revealed that the level of awareness measurement program is different from one organisation to another. P3 indicated that measuring the awareness level is a serious practice, and that all employees must perform awareness tests regularly. The test results reflect on employees' yearly key performance indicator (KPI) achievements as shared below:

> *"It is a part of yearly achievement… Any employee must take training regarding security, how to survive phishing emails or phishing SMS that comes to your cell phones and also that is included in their yearly KPI achievement. How many times you open a phishing e-mail and all this stuff" P3*

Another participant revealed that if an employee passes the measurement program test, a security awareness certificate will be awarded. However, since this test is not mandatory, only a small number of employees conducted this test—as low as two percent of the total number of employees, as commented by P4:

> *"Yes, we do it. We have online programs so all that stuff they can*

access even from their house. They can do small exam after they watch all the videos. So, if he passes, he will get security awareness certificate. However, it's less than 1 percent or 2 percent do the test" P4

P8 confirmed that they measure employees' information security awareness by conducting awareness tests regularly by sending fake phishing email to analyse employee reactions, but do not follow up with further action:

"We have… a lot of time, a lot of time. We made like a test, they provide basic email for employees, it's a phishing email to ask them, please change your password, just to see their reaction" P8

The remaining forty percent of the participants, which mainly represents the private sector, revealed that they do not have any kind of information security measurement programs as expressed by the following comments:

"No. There is an assessment" P5

"Unfortunately, we have nothing like that" P7

Overall, these results indicated that measuring information security awareness is conducted by many of the Saudi organisations; however, the level of measurement varies from organisation to another. Only a few organisations, such financial institutes and oil and gas, are concerned about measuring their employees' awareness in which it is part of employees yearly KPI achievements. Private sector organisations, excluding financial institutes, and the public sector are not expressly concerned about measuring their employees' awareness level.

4.6.4 Summary of Group A Findings

The current analysis of the Group A suggests that there is a high level of understanding of ISRM concepts. In addition, it was indicated that the majority of organisations complies with one or more ISRM standards from which many are certified. However, there is no consistent methodology to select ISRM standards in most of the organisations. Moreover, ISRM standards effectiveness were controversial in that only financial institutes believe that ISRM standards are effective.

The data revealed that there are many factors that influence ISRM effectiveness in

Saudi organisations, which can be classified according to PPT dimensions as discussed in Section 2.8. It was indicated that national culture, management support, education and training, and ethical culture are the main factors, classified under People dimension, which must be addressed in order to enhance ISRM effectiveness in Saudi organisations. Moreover, information technology audit, roles and responsibilities, information security knowledge sharing, cross-departmental collaboration, and information security policy are the main factors, classified under Process dimension. Finally, technology dimension factors that have been demonstrated are information security awareness, third-party management, risk management automation, and measuring information security awareness.

Group B

4.7 Demographics Questions

The information collected from Group B respondents related to demographics included their gender, experience, and their current job title. All the participants had from nine to 22 years of experience in the IT security business from both local and international companies based in Saudi Arabia as illustrated in Table 4-10.

Table 4-10 Group B Participants Details

Participant ID	Job Title	Years of Experience	Organisation Headquarter	Customers Sector/ Classification
P11	Co-founder and Research and Development Manager	17	Local Company	Private/SMEs and Large Organisations
P12	Cybersecurity Services Vice President "VP"	16	Local Company	Private and Public/Large Organisations
P13	Network Automation and Security Specialist	9	International	Private and Public/SMEs and Large Organisations
P14	Co-founder and Senior Information Security Consultant	22	Local Company	Private and Public/Large Organisations
P15	Security Solutions Sales Team Leader	12	International	Private and Public/Large Organisations
P16	IT Governance Specialist	12	Local Company	Private and Public/Large Organisations
P17	Security Solutions Consultant	10	International	Private and Public/Large Organisations
P18	Security Solutions Sales Account Manager	9	International	Private and Public/Large Organisations

Because the researcher had to assure that all participants had the correct amount of experience and interaction with Saudi organisations to ensure the quality of the participants, the researcher asked the participants several general questions regarding their involvement in IT/IS solutions implementation at Saudi organisations. All of the participants had sufficient IT or information security experience and were providing IT or information security services. For example, P11 and P12 stated:

"Yes, I'm making the architect and security layers" P11

"Mostly working in networking and security roles" P12

In addition, all participants stated that they worked with large organisations or government agencies in Saudi Arabia. For example, P13 and P14 stated:

"We manage the network for Saudi Telecom, operated for them in terms of network surveillance, fault management and all stacks of operation for Saudi Telecom service provider" P13

"Mainly, the petrochemical companies" P14

4.8 ISRM Practices in Saudi Arabian Organisations

The researcher asked the participants several questions regarding their perspectives and experience about ISRM in Saudi organisations customers which included:

- Whether they comply with ISRM practices for services or solutions provided to their Saudi organisation customers, and
- Whether their customers enforced information security policy and procedures with their vendors or service providers

The following sections discuss the ISRM practices in Saudi organisations as revealed by IT, information security vendors, and service providers.

4.8.1 Organisation's ISRM Standards Compliance

The data revealed that the majority of Saudi organisations comply with ISRM standards such as ISO and NIST as shared below:

"In large enterprises they have their procedures and standards…" P11

"Most of our clients we work with follow standards and best practices" P17

"I would say 90 percent they follow the international information standard when it comes to risk, when it comes vulnerability assessment, when it comes to sometimes even awareness and, when it comes to information security framework. So, they follow the international standards NIST, ISO, OCTEV" P12

It was confirmed that government agencies, financial institutes, and telecom companies in Saudi Arabia are required to comply with other standards issued by local regulators along with the international ISRM standards as commented by P12:

"Some government agencies besides following the international standards, they do follow some… regulations from the domain... For example, for Saudi Telecom Company, they follow the regulations that are set by… MCITC for example, The Ministry of Communication and Information. When it comes to government agencies, pure government agencies, they follow the standards that was set by the Ministry of Interior because ministry of interior has created an entity for national cyber security centre" P12

On the other hand, only one participant revealed that not all Saudi organisations comply with ISRM standards as stated by P15:

"Normally, not all the customers knows about the standards and the procedures" P15

In summary, most of the participants agreed that Saudi organisations comply with at least one ISRM standard. Also, it was indicated that the regulator requires some organisations such as government agencies, telecom companies, and financial initiates to comply with certain ISRM standards.

4.8.2 ISRM Standards Compliance

What motivates Saudi organisations to comply with standards could provide an insight to the problem. One participant revealed that compliance motives in Saudi organisations are enhancing security postures as stated by Participant 14:

"Some, are interested in the regulation just to enhance their security posture" P14

Other participants revealed that most Saudi organisations comply with ISRM standards with no clear idea why they do it, or just for the sake of being certified. This supports the discussion in subsection 4.6.1.2. For example, Participants 14 and 12 stated:

"Some are very, very much insisted because they need to just comply" P14

"They just encourage to finish it and that's it…. In some cases, companies do just for the sake of the certification. So, they just want to have this certificate hanged in the wall, drag about it without, you know, without considering the security aspects of it" P12

On the other hand, other participants revealed the reasons of non-compliance for

other Saudi organisations. For example, Participant 12 stated that some organisations find ISRM standards not practical and Participant 17 stated that ISRM standards available are very generic, as stated below:

"I think because sometimes it's not practical to follow these standards" P12

"Because, take for example ISO, ISO is very generic" P17

Also, Participant 12 added that government organisations do not have a strong financial motivation to comply with ISRM standards:

"The government however is less… I think there is no strong financial business motivation" P12

To summarise, the data revealed that the motivations for ISRM standards compliance in Saudi Arabia are improving security posture or to obtain certificates and accreditation. On the other hand, the reasons of ISRM standards incompliance are ineffectiveness, the standards being too generic, or no financial benefit.

4.8.3 Policy Enforcement by Saudi Organisations

The data revealed that most of Saudi organisations enforce their policy and procedures over third parties. Most of the participants indicated that each organisation is different from others in terms of the level of the policy and procedures enforcement as shared below:

"Usually, we comply with their procedures. In SME's, they don't have any standards or procedures" P11

"I cannot generalise because each environment is quite different… some clients have their own policy that we must comply… some clients again have it but they do not enforce it… they say it in the contract but they don't follow it" P17

P11 revealed that some Saudi organisations enforce their policy and procedures, such as financial institutes, because it is a mandatory requirement by the regulator:

"Yes, some of them do it from compliance perspective, like banks, we're doing what we call internal audit asking to do so because SAMA is

asking to do so" P11

P12 also added that Saudi organisations consider partial compliance; for instance, when it comes to services a third-party is required to comply with the policy and procedure. However, with solutions, it is not required.

"Here in Saudi market, they don't consider a compliance part when it comes to solutions… for services, no, they do require, you know, compliance with standards, for example, for risk assessment, if you want to go with for example the ISO270001 for security architecture, they will go SABSA and when it comes to maybe risk assessment or risk management framework, they understand that there are present requirements" P12

It was indicated that Saudi organisations would not enforce their policy and procedures unless an incident occurred, as stated by P11:

"It's not a continuous procedure. Once they find an issue then they will do the audit and will ask for corrective action for security issue. But it's not continues at all" P11

P13 stated that third parties do not comply with their customer's policy and procedures most of the time because the policy and procedures of Saudi organisations are loose and, rather, they follow their own strict policies and procedures.

"They do not enforce their own policies as much as they preach it, so it's – they have their procedures, they have their own policies, they have their own unit for cyber security which ties to the executive managers not under any other unit to give them the power. But it's – the organisation is too big to be able to enforce these policies" P13

P13 also added that some vendors choose not to comply with their customers' policy and procedure and instead comply with their own, which can be accepted by some of their customers as shared below:

"Actually, we do have our procedures in terms of privacy and where do we share information, where to install them, how do we share it to STC, and they have their own standards as well which is rather too loose compared to ours. So, we have some restrictions on where do we store information. We cannot, for example, if we want to share a large file through email, we cannot send it through email, so we are not allowed to put it in in Dropbox for example" P13

A few participants revealed that it is not a common practice to comply with customers'

security standards because some organisations do not comply with standards at all:

> *"Normally not all the customers know about the standards and procedures… honestly speaking, I am one of the vendors and I am not Saudi. Only one time I signed an NDA during an incident happened. So, I cannot say this is common. It happens once in Saudi Arabia only with me at least" P 15*

In summary, the data revealed that a few Saudi organisations enforce their policy and procedures on third parties. Further, some organisations have no enforcement mechanism to check whether or not vendors follow the policies and procedures. Moreover, it was indicated that some of the third parties may not adhere to their customers' policy and procedures because these are not clear and instead they follow their own standards. Finally, a few Saudi organisations—especially the small- and medium-enterprise SMEs—do not require their third-party vendors to comply with any policies and procedures.

4.9 Factors Influencing the Effectiveness of ISRM Standards

In investigating the factors influencing the effectiveness of ISRM in Saudi organisations similar to Group A, this section presents the Group B participants' feedback on the ISRM standards contributing factors to ascertain whether these factors influence the effectiveness of ISRM standards. From the literature and Group A data, it was clear that ISRM standards are generalised and not region-specific, which make them less effective. P14 confirmed that the international ISRM standards are generic and there are factors influencing its effectiveness:

> *"Take for example ISO, ISO is very, very generic and it describes best practices" P14*

Therefore, the data revealed that understanding the context of Saudi organisations business from a third-party point of view could provide another insight of the problem and may assist in developing an effective ISRM model.

4.9.1 People

4.9.1.1 National Cultural

From the interviews, the researcher observed that the majority of the participants agreed that national culture has an influence on the effectiveness of ISRM. It was indicated that it is not clear how national culture influence ISRM; however, it is still believed that it should be considered as expressed below:

"Yes… our culture is different… we think about security differently… that's why we need more awareness to prevent disasters" P11

"Yes, it could be… it could have some influence on following the procedures… sometimes they would maybe ignore some policies because they think they are not important, not necessary. So, I think the culture would affect the enforcement of the policies." P13

"Yes, yes, I do… if we are talking about security… everyone nowadays in the US are talking about the cloud-based security. The local market is against this concept until this moment." P15

"I think culture is an important issue when we talk about security in government sector" P16

Only two participants argued that national culture does not influence ISRM or security in Saudi organisations. P12 indicated that the IT environment is identical everywhere and accordingly, the challenges should be the same:

"No, I don't think so. The IT environment and challenges are the same, the type of efforts and interpretation of maybe like, you know, of the challenges, different challenges and incidents and risks, it should be everywhere" P12

"No, I wouldn't say that… It's basically the same" P14

In summary, the data revealed that the majority of the participants agree that ISRM and information security effectiveness in Saudi organisations can be influenced by the national culture. It is believed that the public sector is more influenced by the national culture. On the other hand, it was indicated by a few participants that national culture does not influence ISRM or information security in Saudi organisation due to a similarity in IT

environments and existing challenges.

4.9.1.2 Management Support

The data revealed that three participants suggested that management support may influence ISRM effectiveness in Saudi organisations. It was indicated that management support is challenging due to the lack of information security strategic planning as commented by P12:

> *"So, that's why I think there are some challenges, the level of commitment from management… so, the strategy and the management support is different, so in the US, for example, strategies implemented and followed and everybody is taking his stake seriously. In Saudi organisations you can find this but in ad-hoc basis. So, you can find security initiatives that are not part of the security program, that are not part of an information security strategy, so there's duplication efforts, there's wasted money, wasted time sometimes in projects that are not under certain program." P12*

P13 indicated that the management-reactive actions related to information security is one of the issues in Saudi organisations. The participant believes that the management take action only if something happens, as commented below

> *"They lack on the awareness side… they would do it after a shock or after an issue that happens as a reactive action" P13*

Further, it was suggested that the lower management support could be related the low level of awareness of the importance of information security activities.

> *"I would say understanding the real value of security by senior management is low… it's not usually a priority" P16*

To summarise, the results showed that that top management support and proactive mindset and behaviour is vital for an effective ISRM. In addition, the awareness of the risk management of information systems' value by top management can contribute to the successful of information security management activities.

4.9.1.3 Education and Training

The data revealed that fifty percent of the participants felt that there is lack of information security and risk management education and training. This results in shortage and low local specialist competency and qualification as indicated by the following comments:

"The first challenge, you know, the level of expertise, skillsets are different, honestly… due to lack of proper security education, training centres, university, programs for information assurance, no as competitive skills and knowledge so I think that's the main reason" P12

"I only see education issues. I only see learning issues" P15

"They are competent enough" P14

"There aren't enough specialised security specialties" P13

"I mean we still have big gap here. I can see only 15 percent Saudi national… it's a big challenge" P15

It was indicated that some organisations do not invest in information security training and education because it is a long-term investment and the management do not see the value. This is true especially with public sector as shared by P12:

"Companies here and organisations in Saudi, they don't invest, they don't spend, you know, their money on training, you know. So, I think that's the main challenge, so they don't see the training investment as a longer term, let's say, success factor for their staff, for their engineers so they can, you know, they get proper training and education and which would pay off very soon… in government sector people are not as competitive skills and knowledge as the private sector" P12

The data indicated that the shortage of the information security and risk management specialists may affect the quality of their work as they become overwhelmed. Further, information security specialists could be assigned to tasks which they are not specialised, which may lead to information security serious issues to overcome this shortage.

"There are some good expertise but maybe they are a little occupied because there aren't enough specialised security specialties" P12

"They are not specialised. So, you will have one who is working in too many fields who is not really specialised on any of them… the main reason is resources" P14

To sum up, the data revealed that there is a shortage of information security specialists in Saudi Arabia due to lack of educational programs in information security and risk management. As a result, some organisations assign some information security and risk management tasks to non-qualified employees, which results in exposing the organisation to increased risks.

4.9.2 Process

4.9.2.1 Information Technology Audit

The data revealed that the majority of the Saudi organisations conduct information security audit to assess the effectiveness of the existing information security measures and identify potential risks as commented below:

"They do some audit, security audit, pen testing audits and on the devices we manage, they audit the configuration of the routers to confirm they are properly locked down" P13

"Yes, they are actually. Nowadays, the variety of the security vendors changes the way they're selling to customers" P15

"They usually do, especially big organisations who don't have big enough team to do this, they outsource audit" P18

The data indicated that information technology auditing is not a consistent practice in some Saudi organisations. It is practiced only if they encounter a serious issue that requires auditing as commented by P11:

"For a lot of companies, it's not a continuous procedure. Once they find about it or they find an issue then they will do the audit and will ask for corrective action for security issue. But it's not continuing at all" P11

Further, it was argued that information technology audit is not properly practiced due to the lack of required techniques and tools that improve its effectiveness:

"Yes, they are interested and they want the audit, but, unfortunately, with the industry is lacking of tools to where they can proximate an audit IT processes and procedures" P14

"They do audit… but it's not a proper audit" P13

Moreover, it was revealed that some organisations do information technology audit because they have to comply with local legislation requirements as revealed by P12

"Some of them do it from compliance perspective, like banks, we're doing what we call internal audit because SAMA is asking to do so" P12

P18 emphasised that the public sector and small- and medium-sized enterprise SMEs are the least of information technology audit as commented below:

"Only big companies do audit, most of government agencies do not have capable teams to do it" P18

Finally, one participant revealed that from his 23 years of experience in the Saudi Arabia information technology market, there is a lack of proper information technology audit that needs to be rectified:

"I'm sorry to say it, from my experience in 23 years, I did not find a special section for security. In large enterprises, they do the security but there is no special security section during the acceptance to make the acceptance based on that" P11

In summary, the data revealed that most of the organisations in Saudi Arabia conduct information technology audits. However, these audits lack consistency and proper techniques and tools, resulting in less effective information security management. Further, it was indicated that some organisations, such as financial institutes, conduct information technology audits only because it a mandatory requirement from the local legislation.

4.9.2.2 Unclear Roles and Responsibilities

A few participants revealed that unclear roles and responsibilities may influence ISRM effectiveness in Saudi organisations. It was indicated that due to the ambiguity of the responsibilities, some of the information security tasks may not be performed in a timely manner and may result in information security projects delays as commented below:

"The clear definition of rules and responsibilities. Sometimes the security is responsibility of the network team while in other organisation, the application team, sometimes it's handled by a third department… So, the rules and responsibilities are not well and clearly defined in most of the organisations" P12

"Understanding job responsibility is missing… I mean when work on some of clients sites and want to take action for example changing firewall settings or request a major change to network design, we end up in loop of wasting time communication… they do not know who is responsible of what in some cases" P17

"Roles are not clear… I think that's the reason" P18

In summary, the data revealed that unclear roles and responsibility is a common issue in some Saudi organisations, and the ambiguity of responsibilities may result in information security project delays.

4.9.2.3 Information Security Knowledge Sharing

The data revealed that information security-related knowledge sharing among Saudi organisations is not practiced. P12 indicated that every organisation works independently when it comes to information security threats as they do not share necessary information that might assist other organisations to prevent information security threats.

"Most organisations work in silos, they don't worry, they don't exchange or share knowledge, experience, threats on certain sectors. For example, like, if you take the -- just an example as an insurance company sometimes they get targeted to some APT groups, like advance persistent threats groups, they target the Saudi insurance companies, for example, they don't share this among each other. They don't have plans to share and explain -- because sharing knowledge is very, very critical, it saved a lot of time and money and it helps" P12

"One of the issues I can see in companies working in the same industry is they face the same challenges and every one of them treat it differently. This is a waste of time and effort. Why don't they cooperate and share the knowledge to help … they do not look interested or they may feel it is improper to ask" P18

In summary, the data showed that sharing of information security knowledge among organisations is not a common practice Saudi Arabia. Most organisations work alone when it comes to information security threats due to lack of legislation and interest.

4.9.3 Technology

4.9.3.1 Third-Party Management

From the data, it can be understood that the third-party management is poor in some Saudi organisations. P13 indicated that they are not consistent in enforcing policy in information technology contractors:

> *"They lack some details, not on everywhere… it's not restricted properly. So, maybe for the huge projects they have NDAs, they have their policies, they have set of rules on the contract, but the day-to-day jobs, there are some new projects, the smaller ones, sometimes they do not enforce" P13*

Further, it was stated that some Saudi organisations enforce policy only at the beginning of the project and after that, oversight is relaxed. Consequently, no employee would enforce and assure that the third party is adhering the policy and procedure. It was also indicated that the smaller the project, the less enforcement:

> *"Yes and no, they require us to comply with their policies at the beginning of a project but after that, no one ask and most of the time they don't care about compliance because they want to close the job and deliver" P17*

One participant revealed that the majority of the organisations in Saudi Arabia do not have third-party management systems in place:

> *"Honestly speaking, I am one of the vendors and I am not Saudi. Only one time I signed an NDA during an incident happened. So, I cannot say this is common. It happens once in Saudi Arabia only with me at least" P 15*

In summary, the data indicated that third-party management is quite poor in most of the Saudi organisations, especially in smaller-sized projects. Further, even in larger projects, the enforcement of policy and procedure reduces as time passes.

4.9.3.2 Lack of Information Security Awareness

Lack of information security awareness was indicated as one of the factors that may influence ISRM in Saudi organisations. P14 stated that the low awareness of the importance

of ISRM may lead to the behaviour of only complying with ISRM standards to satisfy the regulator's requirements without considering the real security benefits as commented below:

"Actually, user education and user awareness is a big part… some companies are very, very much insisted because they need to just comply" P14

Further, it was indicated that due to the low awareness of the importance of ISRM, some organisations may comply for the purpose of certificate issuance and accreditation, which is a document that certifies compliance to particular standards:

"In some cases… companies do just for the sake of the certification. So, they just want to have this certificate hanged in the wall… without considering the security aspects of it" P12

P13 revealed that the low level of awareness may result in focusing on the incorrect problems and ignoring the real risks and vulnerabilities that organisation might face:

"They focus on the wrong problem… I think awareness is the first point to tackle either internally or on a national scale… most people ignore risks thinking they are not risks at all or with minimal risks. So, I think awareness would remove some of that" P13

In summary, the data showed that the lack of information security awareness is considered as a factor that influences ISRM effectiveness in Saudi organisations. It was indicated that focusing on incorrect problems and compliance attitude may be influenced by low awareness.

4.10 Summary of Group B Findings

The current analysis of Group B indicated that that most of the organisations in Saudi Arabia comply with one or more of international ISRM standards and best practices such ISO and NIST. The motivation of ISRM standards compliance in Saudi Arabia are: improving security posture or certificates and accreditation, while the reasons for ISRM standards incompliance are ineffectiveness, standards are too generic, or no financial benefits.

Group B's data revealed that there are factors that influence ISRM effectiveness in Saudi organisations which can be classified according to PPT elements discussed in Section

2.8. It was indicated that national culture, management support, and education and training are factors, classified under People elements, which may be addressed in order to enhance ISRM effectiveness in Saudi organisations. Moreover, information systems audit, roles and responsibilities, and knowledge sharing are factors, classified under Process elements. Finally, technology element factors that have been demonstrated are third-party management and information security awareness.

4.11 Summary

This chapter examined the ISRM practices, implementation challenges, and factors that influence the effectiveness of ISRM standards in large Saudi Arabian organisations. The interview data from Groups A and B were carefully coded and qualitatively analysed. Thematic coding was used on the transcripts of phase one data that unveiled a number of interesting themes that were grouped into PPT dimensions, resulting in producing the ISRM factors that were used to develop the enhanced ISRM model discussed in the next chapter.

The analysis indicated that there are contradictions between Group A and Group B results. The contradiction was very minor and did not affect the final results; however, it provided more information that helped the understanding of how some of the newly revealed factors influence ISRM in large Saudi Arabian organisations.

The next chapter discusses the research findings and presents the enhanced ISRM model emerged from the data.

CHAPTER 5. DISCUSSION

5.1 Introduction

The previous chapter discussed the data collection phase one, the semistructured interviews, and how the data obtained from the interviews were analysed. The resulting data were encoded utilising NVivo software, which revealed the ISRM compliance in Saudi organisations. In addition, it revealed the factors that influence the effectiveness of the ISRM standards in large Saudi Arabian organisations.

This chapter addresses the first and second sub-objectives and research questions. It discusses the ISRM compliance in Saudi organisations and the factors that influence the effectiveness which have been obtained from literature review and the semistructured interviews. All factors, including the factors within the initial ISRM model discussed in Section 2.9, have been combined to construct the enhanced ISRM model for large Saudi Arabian organisations which was then evaluated by the focus groups and the data collection phase two in the next chapter that led to the proposed ISRM model for large Saudi Arabian organisations.

5.2 ISRM Compliance in Saudi Arabian Organisations

This section addresses the first research question:

RQ 1. *What is the level of Saudi Arabian large organisations' compliance with ISRM standards?*

As discussed earlier in Section 2.7.3, the few studies that have been carried out on government agencies, healthcare, defence, financial institutes, and private enterprise have noted that only a few Saudi Arabian organisations comply with ISRM standards. Yet, the Saudi government has started to recognise the importance of information security and has introduced a few initiatives to boost its information security position. These initiatives have introduced mandatory requirements to comply with information security standards including

ISRM standards such as ISO 27005 because it is believed that it is one key element in improving the country's information security.

The results of this study discussed in Section 4.5.1 indicates that there is high level, ninety percent of the participated organisations, of the compliance with one or more ISRM standards such as ISO, NIST, COBIT, PCI, and the ISF Standard of Good Practice. This finding is contrary to previous studies by Alshitri and Abanumy (2014) and Nabi, Mirza, and Alghathbar (2010), which noted that compliance with ISRM standards and best practices is very low. The observed increase in ISRM compliance could be attributed to the fact that Saudi Arabia's government has introduced new information security initiatives discussed in Section 2.7.2 that emphasise the need to comply with information security standards. Moreover, the increased number of cyberattacks on critical and major economic organisations that caused serious loss and affects reputation such as Saudi ARAMCO attacks, could be another reason that has encouraged Saudi organisations to reassess their information security approach and eventually lead to complying with international information security standards such as ISRM standards.

Another important finding was that the dominant adopted ISRM standard in Saudi organisations is the ISO 27005, as part of the ISO27001 ISM standard and certification, with 80 percent of the organisations complying. The reason, as described by a few participants, is that the resources and service providers and certified professionals for ISO standards are more available and more accessible than other standards. Also, the ISO certificates are more recognisable by government and semi-government entities and, in some cases, are a mandatory requirement. Meanwhile, the data show that 70 percent of the organisations are ISO 27001 certified, which contradicts the claims of Nabi, Mirza, and Alghathbar (2010) that only 20 percent of surveyed organisations are certified. One of the possible explanations for this finding is that Saudi government information security initiatives provide organisations with clear guidelines to comply with information security standards and require certifications for governance purposes for critical industries such as financial institutes and government agencies.

The findings also showed that some of the Saudi organisations tend to comply with more than one ISRM standard, mainly financial institutes. It suggests that financial institutes

are more concerned about their security posture as they comply with multiple ISRM standards because it is believed that this approach could assist the organisations in overcoming some of the challenges discussed in Section 2.5.4 by adopting the parts that help achieving the organisation's objectives and therefore minimising the risk.

The findings reveal, however, that most Saudi organisations have no guidelines to select appropriate ISRM standards. Most organisations have general criteria to select their ISRM standards such as the market trend or the most adopted standards among the same industry organisations, well-established standards such as ISO 27001, the availability of proper documentation, and/or the availability of ISRM standards consultation services and support. However, this result has not previously been described. A possible explanation for that may be the lack of information security risk professionals, discussed in Section 4.6.1.3, who have the knowledge and expertise in a wide range of ISRM standards available in the market that support the decision to be made in selecting the most appropriate ISRM standard for the organisation.

5.3 ISRM Challenges in Saudi Arabian Organisations

This section addresses the second research question:

RQ 2. *What are the ISRM standards implementation challenges in large Saudi Arabian organisations?*

The limited research that has been carried out on a few Saudi Arabian organisations that comply with ISRM standards indicated that there are challenges in implementing ISRM standards or best practices in Saudi organisations. Some of these challenges overlap with the ISRM factors, such as national culture and management support and are discussed in great detail in the next sections.

Previous studies showed that the shortage of information security expertise is one of the main challenges in which information security qualifications need to be addressed in Saudi organisations. The shortage has worsened as a result of the increase in the price of oil, investments in mega projects, economic liberalisation, and the higher level of digital maturity

of e-government services (Alshitri and Abanumy 2014). The data confirmed that the shortage of information security expertise as well as risk management expertise is a long-lasting challenge. It was indicated that the education system outcome is poor in terms of quality information security and risk-management education and training programs. This finding is consistent with that of Al-Saud (2012) and Kshetri (2016), who discussed the association between the effect of the education system and the local information security and risk management availability. A possible explanation for this might be that Saudi Arabia was not aware of the urgent need for local expertise and, more importantly, the sudden increase of the cyberattacks against the major infrastructure in Saudi Arabia.

Prior studies indicated that managing IT assets can be a challenge in Saudi organisations. The findings further support the idea that assets management in particular can be challenging which confirmed the findings that were also reported AbuSaad et al. (2011). The data revealed that some of the IT and data assets are not registered in the organisations' assets registry, and therefore it is difficult to identify the assets and their associated risks. Another reason is the lack of understanding of the assets value by some of the asset owners that lead to unrealistic risk ratings; this could negatively influence the entire risk management process. Poor communication can be another reason. The data revealed that when a risk is identified in another department, it takes some time to identify the asset owner and even more time to mitigate the risk due to poor communication.

One of the challenges indicated in the literature is the generic ISRM standards instructions and guidelines. This finding was also reported by Al-Ahmad and Mohammad (2012 2013) and Flores, Antonsen, and Ekstedt (2014). The data indicated that these standards are generic and therefore there is a need to study the organisation process and customise the ISRM standards prior to implementing any of these standards. This challenge is considered a global one and not simply limited to Saudi Arabia.

The data indicated that the "understandability of policy language" is a challenge for some of the Saudi organisations. The understandability issue can possibly be related to the language barrier because Saudi Arabia's mother tongue is the Arabic language. This finding may be explained by the fact that the official communication language in all of public sector organisations such as government agencies is Arabic, and therefore standards and policies

that are originally in other language such as English are being translated. When translating from English to Arabic, for example, there may not be an exact word-for-word translation but only a general idea of what is being said, which could lead to misinterpretations as some technical terms cannot be translated directly.

Finally, the data provided evidence that the existence of several ISRM approaches may lead to the selection of an inappropriate ISRM standard. It was indicated that Saudi organisations have no clear methodology to select applicable ISRM standards. Some organisations prefer standards that are well documented, other organisation choose standards with available resources such as the availability of certified professionals or service providers. A possible explanation for this might be the lack of governmental policy for selecting ISRM approaches that guide classify organisations according to their size, sector, industry, and so on. However, the Saudi government's latest cybersecurity initiatives, discussed in Section 2.7.2, have already issued new policies and standards related to information security management that could help resolving this challenge in future.

According to these findings, it can be inferred that Saudi Arabian organisations face many ISRM challenges. Some of these challenges are discussed in detail in the next sections. The other challenges are the shortage of information security expertise, managing IT assets, generic ISRM standards instructions and guidelines, understandability of standards, and the selection of an ISRM approach.

5.4 Factors Influencing the Effectiveness of ISRM Standards

This section addresses the third research question:

RQ 3. *What are the factors that must be considered when developing an effective ISRM model for large Saudi Arabian organisations?*

This section highlights the factors emerged from phase one data collection and the semistructured interviews in order to develop an enhanced ISRM for large Saudi Arabian organisations.

5.4.1 People

5.4.1.1 National Culture

As discussed in the literature review Section 2.8.1.1, national culture has a direct influence on organisations' information security. Prior studies have noted the importance of national culture on the employees' behaviour, including their behaviour towards information security. It has been shown that the way of thinking, assumptions, and decision-making is directly influenced by culture. In addition, it affects the adoption of information security standards, protecting assets, and the compliance of information security policies and procedures in organisations (AlHogail and Mirza 2014; Alkahtani, Dawson, and Lock 2013; Fomin, Vries, and Barlette 2008; Übelacker 2013). Therefore, national culture influences the level of information security awareness as well as ethics and accountability in organisations. Moreover, it has been indicated that management theories that have been applied in other cultures which are not applicable for the Saudi culture due to cultural differences.

Consistent with studies by AbuSaad et al. (2011), Aldraehim et al. (2012), and Alnatheer and Nelson (2009), the results of this research indicate that there is a significant gap between Western countries' culture and Saudi culture. The data revealed that the maturity level of understanding of risk management, privacy, and compliance among staff members represent the main cultural gap in Saudi organisations. Top or upper management, for example, are not aware of the importance and the value of the risk management of their information assets, which influences their ISRM investment decisions. Staff members, on the other hand, do not understand the importance of information security compliance and its implications in workplace, and that greatly influences their decision regarding information assets. Moreover, the data suggest that due to the cultural differences, the international information security management standards cannot provide a comprehensive solution for all security risk-related issues. Therefore, Saudi culture played a significant role in organisations' ISRM compliance and effectiveness.

One interesting finding is that the view of privacy in Saudi Arabia is different from Western and most other countries. For example, female photos cannot be viewed or assessed by any male other than close relatives, such as husband or father, for any reason except for

an emergency. Thus, female data must be assessed and handled by other females only. This finding is likely to be related to the national culture that is influenced by Islamic law. Therefore, expatriates who work in Saudi organisations could mistakenly access these data because they are unaware of the Islamic law and national culture. Another example is the confidential data exposure (e.g., customer bank account details) by employees as discussed in Section 5.4.1.3.

Another important finding is that the non-compliance behaviour in Saudi organisations has been linked to Saudi culture. This confirms previous studies by Alzamil (2018) and Alkahtani, Dawson, and Lock (2013), which revealed that national culture is crucial for an accurate prediction of employee behaviour in an organisation. A possible explanation for the negative effect of Saudi culture on employee behaviour is that the development of security culture plans is isolated from national culture. The reason behind that could be the utilisation of international information security management standards that do not consider national culture. These findings suggest that Saudi culture has a direct effect in ISRM, thus cultural-related controls should be re-evaluated to ensure that they do not conflict with Saudi national culture and also fulfil their special needs.

5.4.1.2 Management Commitment and Support

Previous research has shown that one of the key factors to the unsuccessful existence of information security management in Saudi Arabia is the conflicts of management style of the Western and Arab leaders and managers. Further, culture plays an important role in management commitment and support behaviour towards information security.

The current research confirmed the discussion by Veiga and Martins (2017), Soomro, Shah, and Ahmed (2016) and Glaspie and Karwowski (2018) that top management support is vital for promoting the information security culture and thus the success of ISRM implementation. Another important finding was that the top management do not consider information security as a priority function when it comes to planning and investment. A possible explanation for this might be a low awareness of the importance of information security. This point is discussed in Section 5.4.3.1.

Further, the data revealed that both Groups A and B concurred that a top management proactive mindset and behaviour is vital for an effective ISRM and improved information security posture for Saudi organisations. This indicates that top management in Saudi Arabia are more reactive towards information security planning and practices, which may lead to catastrophic consequences. This is likely to be related to national culture and the low awareness of the importance of information security.

Finally, the results of this study, which were supported by both Groups A and B, suggested that in order to have an effective and successful information security management system, a top-down approach is required. The success of information security management programs is dependent upon how much time, money, and effort top managers dedicate to them. Additionally, organisational culture, which is promoted by the top management, could have an impact on the ability to successfully manage information security risk profiles over time by providing a general sense of empathy for employees who are impacted as well as offering concrete solutions that help prevent future breaches from occurring.

5.4.1.3 Ethical Culture

One unanticipated finding from the research data was the role ethical culture in the ISRM effectiveness in Saudi organisations. Ethics can be defined as the values and rules that influence someone's behaviour and the decision to distinguish right from wrong (Bishop et al. 2018; Singer 1998). Ethical conduct policies are an important factor that establishes employees' moral codes and controls their behaviour (Hinde, 2003). They facilitate security awareness programs in which employees are held responsible for ensuring adequate security practices are implemented, thus reducing security risks. Surfing the Internet for non-business related purposes during working hours or sharing the organisation's confidential information with others are examples of unethical conduct (Schwartz 2015). Organisational ethical culture is critical because it enables ways of thinking about the organisation's norms and standards that employees use to make moral decisions and judgments. However, little is known about the organisational ethical culture in the context of IS behaviour (Chen, Chau, and Li 2019).

The data from this research showed that some Saudi organisations face ethical conduct behavioural issues. It has been highlighted that some employees seem to be careless

about following policies because they are not fully aware of how their behaviour can negatively affect their organisation's information security. For example, some employees tend to misuse customers' personal data by screenshotting customer's details—including full name and bank account details such as available credit—and sharing it with friends. It is clear that some employees proceed with these violations without a sense of guilt, even if they know that such behaviour is illegal. This behaviour continues to occur even though the organisation has already warned all employees about such actions. Accordingly, one participant's organisation deactivated their screenshot option in all computer devices to prevent this action from happening. This can be considered to be a noncompliance behaviour and, moreover, an ethical conduct issue. This might suggest that the low level of IS awareness discussed in Section 5.4.1.2 and the ethical culture could contribute to such behaviour. Further, it indicates that ethical culture is associated with the organisation's awareness program. The data contributes a clearer understanding of the reasons of the non-compliant behaviour in Saudi organisations. The low level of ethical culture strategy is a good predictor variable for explaining employees' information security non-compliance behaviour.

Saudi organisations must promote an ethical organisational culture in order to improve information security risk management. It must be a top-down approach in which the top management is involved by developing and communicating codes of conduct and lead by example. A code of ethics for information security must be documented according to Saudi culture. This will prevent any conflict and inappropriateness of the code with the local culture that will potentially improve its effectiveness. The code should offer the values, principles, and standards to guide employees to making the correct decisions and conduct. This includes how they should comport themselves with respect to authorisation, organisational equipment and assets, colleagues, working hours, and confidential information. A code of ethics should outline the organisation's values and ethical rules that they expect their employees to follow. Also, it must clearly express ethical and non-ethical actions to help the employees understand what is expected.

An ethics training program could help reinforce the organisation's code of conduct and send a clear message about the organisation's ethical stance. Moreover, reinforcing ethical behaviour by appreciating those who have a record clear of ethical violations is a significant way to promote ethical culture in Saudi organisations. Another way to promote

ethical culture is by utilising IT to manage ethical conduct starting from code documentation, updates, auditing reporting code violation, and archiving. Finally, information security awareness programs and ethical culture programs should be integrated to ensure an effective ISRM.

5.4.1.4 Education and Training

As mentioned in the literature review, the shortage in information security and risk management professionals is a challenge for many organisations. They lack staff with the necessary skills to manage security risks.

Information security and risk management disciplines were not adopted on a large scale by Saudi Arabian universities as discussed in Section 3.8.2.1.

The data confirmed the findings of the previous work discussed by Al-Saud (2012), Hathaway, Spidalieri, and Alsowailm (2017), and Kshetri (2016) that Saudi Arabia faces a serious shortage of information security specialists; this shortage requires time and effort from governing bodies to address the causes and find proper solutions. It also confirmed the findings of the previous work of Alharbi, Atkins, and Stanier (2017), Alkahtani, Dawson, and Lock (2013), Alshitri and Abanumy (2014), and Alsmadi and Zarour (2018) that there is a need to develop information security educational programs such as higher education and specialised training centres in order to meet the local market demand, resulting in improving the information security level in Saudi Arabia. It is clear from the data that the educational system in Saudi Arabia does not provide adequate information security and risk management programs to fill the existing gap, although there is a plan in place that already has been implemented to educate locals with better information security and risk management qualifications. This result may be explained by the fact that although the Saudi government's recent initiatives have taken steps forward building information security educational programs and training, the fruitful results of these initiatives need time and, more importantly, the demand is still higher than the expected outcome. Further, the lack of an integrated industry effort such as large technology vendors who should utilise their expertise to develop strategies and programs for information security training.

Another important finding was that there is a gap in risk evaluation knowledge between assets owners and the IT risk management team. It has been noted that once the risks have been identified, business owners cannot provide a realistic evaluation of the risks because they do not understand the risk evaluation criteria. It seems possible that these results are due to the lack of risk management training for the asset owners and others who might be involved in the risk management activities. It can thus be suggested that all employees who are involved in any of the risk management activities must enrol in a risk management training program. The program should focus on risk management fundamentals, risk assessment, and, more importantly, the evaluation of risk. In addition, a risk evaluation sheet with clear samples of identified risks and their evaluation should be provided to employees to work as a reference guide showing different types of risks and impact scale illustration. This should be dependent of each business unit to determine their pre-agreed current risks and their impact scale. ISO/IEC 27005:2018 Annex B provides a guideline that may assist risk management professionals to prepare this sheet in a systematic manner (ISO/IEC27005 2018). This sheet should be updated regularly by the information security risk management team. A sample of an illustrative impact scale is shown in Table 5-1 below.

Table 5-1 Illustrative Impact Scale Sample

Rating	Level	Criteria
5	**Very High**	Financial loss of $X or more Sever loss of market share Long-term negative media coverage Severe injuries or fatalities Multiple senior managers leave and high turnover of staff Severe prosecution and fines
4	**High**	Financial loss of $X up to $X Significant loss of market share Short-term negative media coverage Serious injuries A few senior managers leave and other staff Significant fines
3	**Medium**	Financial loss of $X up to $X Minimal loss of market share Reputational damage Minor injuries Increase in staff turnover
2	**Low**	Financial loss of $X up to $X moderate customers loss Reputational No injuries Staff morale problems
1	**Very Low**	Financial loss of $X up to $X Minimal customer loss No injuries

5.4.2 Process

5.4.2.1 Information Technology Audit

Previous studies have shown that one of the key elements to successfully managing an organisation's information technology risk is its audit. It has been shown that national culture may also play an important role in the acceptance and the effectiveness of information technology audits.

The current research found that the majority of Saudi organisations regularly conduct audits on their IT infrastructure. This finding is contrary to previous studies, which have

indicated that internal audits are not given sufficient credence and importance. A possible explanation for this might be that the Saudi government's recent information security initiatives have developed new mandatory compliance requirements according to SAMA's and NCA's frameworks, which includes auditing practices.

However, this finding from Group A is contrary to the finding of Group B. The data from Group B indicates that auditing activities are not conducted properly by some organisations in Saudi Arabia. These poor quality audit activities could lead to audit failure that eventually exposes an organisation to risk. Disqualification is one reported reason behind audit failure. It was indicated that due to the shortage in qualified information security and risk management professionals, some organisations tend to assign non-qualified employees to conduct auditing activities. This finding suggests that although audit activities are carried out in most of the Saudi organisations, the level and quality of the audit do not meet the minimum requirements, resulting in inappropriate auditing activities and reports. In general, therefore, it seems that the shortage of qualified risk management professionals discussed earlier in Section 5.4.1.4 is the main cause of the inappropriate auditing, which can be resolved by proper education and training.

5.4.2.2 Clear Roles and Responsibilities

Well-established roles and responsibilities are viewed as determinants of an organisation's success. It was suggested that the clarity of roles and responsibilities lead to better employee performance (Florah 2017). Employees with better clarity on roles and responsibilities perform better than those with unclear roles and responsibilities. Moreover, unclear roles and responsibilities affect communication within organisational team members in which it will be difficult to clearly identify who is responsible for what, what to expect from them, and who should be informed when a certain action was taken (Gur 2019).

The results of this research indicated that unclear roles and responsibilities are another factor that negatively contributes to unsuccessful ISRM in Saudi organisations. This finding was unexpected and suggests that by establishing clearer roles and responsibilities, effective communication among employees to address risk-related information systems and technology could be accomplished. Moreover, employees who clearly understand their

responsibilities would perform better and be more accountable. These results were also supported by Group B, who emphasised that the ambiguity of responsibilities in Saudi organisations may result in information security projects delays and, ultimately, in information security risk exposure.

A possible explanation for these results may be the lack of adequate management support discussed in Section 5.4.1.2 because it is part of the management responsibilities to make sure that roles and responsibilities documentation is clear, readily available, and understood by all organisational staff. Another reason could be the national culture and organisational culture effect because many organisations—especially government agencies—do not have established roles and responsibilities, or they could have old and outdated ones.

It is possible, therefore, that Saudi organisations could improve their information security posture by establishing clear and well-documented roles and responsibilities. They should provide detailed description of each role and assure that the employee has understand it.

5.4.2.3 Sharing of information Security Knowledge

Several studies have shown that information security knowledge sharing is considerably important due to the dramatic changes in this field. It was indicated that, due to the rapid change in cybersecurity attacks, information security-related knowledge sharing such as new threats and information security best practices could potentially increase awareness, mitigate risks, and improve decision-making that may assist in protecting organisations from cybersecurity threats.

The current research revealed that most organisations in Saudi Arabia do not practice sharing of information security knowledge. This coincides with the previous work by Almuqrin et al. (2020) and Chandran and Alammari (2020), which showed that Saudi organisations lack knowledge sharing due to many factors such as cultural backgrounds and organisational and relational identifications.

In contrast to the previous findings, however, these findings also revealed that oil and

gas and financial institutes are an exception as they tend to practice knowledge sharing. Yet, there are no regulations or policies to guide through the knowledge sharing process by the local regulator. For example, financial institutes are requested to report information security incidents to SAMA who then share it with other financial institutes. This is just a part of the knowledge-sharing process which includes other steps for proper knowledge sharing, such as the explicit knowledge sharing which includes awareness, access, guidance, and completeness of the data.

While sharing of information security knowledge is considered an investment in terms of resources time and efforts, national culture might influence knowledge sharing behaviour in Saudi Arabia. The findings discussed in Section 5.4.1.1 showed that national culture was considered to be a main contributor for top management behaviour. The research data indicated that management in Saudi organisations consider investment in technology rather than people and process improvement investment. It was revealed that some organisations have more advanced technologies than most other organisations in the rest of the world; yet, they are more prone to information security threats and data breaches due to a lower investment in people and process improvement resulting in less effective information security management plan.

A possible explanation for this might be the lack of regulations that enforce knowledge-sharing process among organisations. Governing bodies need to understand the importance and influence of the knowledge sharing on organisations information security, address causes of low adoption, and find proper solutions. Moreover, knowledge sharing must be a part of the organisational culture using deferent techniques including training, meeting, benchmarking, and more. Finally, periodic information security conferences organised by the government is suggested to bring together information security and risk management professionals, from public and private sector organisations as well as academia. The purpose is to share information security knowledge and address new and advanced threats.

5.4.2.4 Established Information Security Policies ISP

As mentioned in the literature review, it is the ISP that assists organisations to have

the risk management take place. ISP is crucial during the first phase of ISRM planning in order to have risk management activities carried out. Previous studies examining non-compliance behaviour observed that poor ISP management is one of the main reasons for the non-compliance behaviour in Saudi organisations. It has been concluded that poor ISP management includes outdated, scattered, inaccessible, and overly broad ISP documentation as well as employees' low awareness of their organisations' ISP and its importance. Other studies have suggested that national culture could result in employees' low perception of the importance of threats and vulnerabilities which potentially impact ISP compliance in Saudi organisations.

The current research found that most of the Saudi organisations have a published ISP in place. It has been indicated that the ISP is regularly reviewed and updated accordingly. Consistent with the literature, however, this research found that ineffective ISP management is an issue for number of organisations. It showed that ISP non-compliance behaviour has been linked to ineffective ISP enforcement, low awareness, and national culture. It was also argued that although the majority of Saudi organisations have the latest information security technologies acquired and implemented, the effectiveness of information security management systems are low due to ineffective ISP enforcement. Moreover, Group B's findings emphasised that despite having an ISP in the majority of organisations in Saudi Arabia, they fail to enforce them successfully. This ineffective ISP enforcement is the main reason of the ISP non-compliance behaviour in Saudi organisations. Top management was found to be a role model in raising employee ISP awareness. This result may be explained by the fact that top management are not aware of the importance of ISP and, therefore, ISP is overlooked. This could be linked to the management low awareness discussed in Section5.4.1.2.

Another explanation for ISP non-compliance behaviour could be the negative experience the employees encounter when trying to comply with ISP. The data indicated some employees would not adhere to ISP practices because they think it would hinder their daily job progress. Therefore, it is suggested that employee's awareness regarding the importance of ISP practices plays a vital role in improving the compliance behaviour. Further, simplifying the ISP processes may also improve the compliance behaviour, resulting in fewer mistakes made, less time spent learning new rules and regulations because it allows for easier

understanding from all parties involved, improved employee satisfaction due to increased clarity in expectations, as well as reduced stress levels associated with constantly being updated about changes within the organisation's IT department. Moreover, maintaining a well-documented ISP is another factor that offers several benefits to ISP compliance behaviour. It could improve the ISP accessibility, awareness of its importance, and, more importantly, simplify its processes, making it easy to understand and implement. Accordingly, employees would have a better experience with ISP in which the compliance behaviour would improve. Finally, it was emphasised that organisations should not rely on awareness because non-compliance may occur regardless of the emphasis on it. ISP enforcement by deterrence sanctions is the last strategy to influence the behaviour of employees to comply with ISP. Therefore, the enforcement should be viewed from the perspective of awareness and sanctions.

5.4.2.5 Cross-Departmental Collaboration

One unanticipated finding from the research data was the influence of cross-departmental collaboration within an organisation on ISRM. Cross-departmental collaboration can be defined as "any joint action across diverse departments that is intended to increase public value and address difficult public challenges through coordination, partnering, conflict resolution, and cooperation" (Wipulanusat, Sunkpho and Stewart 2021, p. 2). Each organisation is considered an ecosystem in which it is not possible to implement a solution or make a change in one part of an organisation without affecting other parts of the organisation. Studies have shown that a lack of communication between employees from different department leads to ineffective work progress. It has been indicated that cooperation between departments is vital to reach the desired organisational goals. Cross-departmental collaboration within an organisation is a reflection of a healthy organisational culture (Ali 2007).

The data indicated that insufficient cross-departmental collaboration could negatively affect the information security process in the whole organisation. Information security and risk management teams encounter many communication and collaboration issues with other departments within their organisation. For example, risk identification and analysis tasks are

not given a priority by some employees in other departments, which causes a major delay in the risk assessment cycle resulting in incomplete risk reports. Therefore, risk management teams need to spend time and effort to push those who are not cooperating to finish the required tasks. This problem arises consistently throughout the risk management cycle.

A possible explanation for the ineffective collaboration among departments might be the lack of top management support. Effective cross-departmental collaboration requires that effective strategies and measures to be taken that are initiated and supported by the top management as well as department heads. Moreover, prompt and authentic information exchanges throughout the organisational hierarchy have to be ensured. Finally, obstacles which prevent effective collaboration among departments must be pointed out and resolved.

Another possible explanation for this is the lack of business comprehension among departments. The lack of understanding of organisations' business strategies and the role of each department could lead to ineffective communication and response. Leaders must allow teams to learn about each other and understand the importance of each team. This could improve trust among department teams, which could potentially improve collaboration.

5.4.3 Technology

5.4.3.1 Ongoing Information Security Awareness Program

The information security literature has, in general terms, emphasised the importance of employees' attitudes and behavioural intentions as predictors of actual information security compliance. Prior studies have noted the importance of information security awareness program as it is considered a precautionary measure to prevent information security threats. In addition, it has been noted that information security awareness is considered to be one of the strongest lines of defence in organisations against IT threats because most of the employees are not aware of the information security measures and consider IT as a tool to perform their job responsibilities quickly and efficiently; additionally, most of the time, information security is viewed as an unnecessary hindrance (Alzahrani and Alomar 2016; Veiga and Martins 2017; Tsohou et al. 2006). Therefore, there is a need to establish an information security awareness program to ensure an appropriate degree of

security awareness within an organisation (Alnatheer 2015).

These results from both Groups A and B confirmed the findings of much of the previous work by Kshetri (2016), Aldosari (2019), Omar (2017), and Alzahrani and Alomar (2016), who argued that one of the main reasons Saudi organisations are subjected to frequent and destructive cyberattacks and data breaches is the low level of awareness. Moreover, the data indicated that the low level of awareness is influenced by the culture as well as education and training, which has been confirmed by Aldossary and Zeki (2013) and AlKaabi (2014).

It is therefore suggested that Saudi organisations should provide mandatory information security awareness training programs for all employees, including senior managers. Further, each training must conclude with an assessment to assure the employees' understanding. It is also advisable to include the training attendance and assessment results as part of an employee's annual performance appraisal process.

To address cultural differences, information security awareness programs should be provided in the employees' native language. It is advisable to focus on certain aspects in certain languages while the same aspects may not receive the same attention in other languages. That means the concepts and associated risks should be presented and explained in the appropriate languages (Kruger et al. 2011). In addition, Arabic language translated material should be available for Saudi and Arab employees and should be presented and explained in clear language.

The traditional approach to information security awareness training programs has not kept up with the advancement in cyberattacks. The use of technology in information security awareness training such as online webinars and on-demand training could save time and effort and eventually reduce training costs. Moreover, such programs have steadily increased in the past several years and can be easily up-to-date with the current security advancement. It is a way to provide an interactive teaching experience and reinforce the concepts learned. Therefore, information security awareness training programs should take advantage of the technology to develop more specific and relevant training programs designed specifically for the skills required and fit the work environment in Saudi organisations.

5.4.3.2 Measurement of Information Security Awareness

Prior studies have noted the importance of information security awareness training program in the employees' behaviour toward information assets. Yet, the measurement of the effectiveness of the ISA is as important. It has been indicated that organisations must measure employees' understanding for policies, procedures, threats, and much more. Measuring information security awareness helps to identify an employee's current understanding of the company's cybersecurity policies and procedures are, as well as their ability to act on them in order to prevent data breach from cyberattacks from happening or mitigate the damage. Measuring employees' awareness can be achieved by developing assessments that test their basic knowledge regarding cybersecurity, policies, risks of identity theft, data breaches, phishing scams, malware attacks, and more. This must be completed by all employees within the organisations, including top management. The results of these assessments can identify employees' ISA weakness so that the awareness program training is corrected accordingly.

The current study found that some Saudi organisations developed awareness measurement programs which that may assist in measuring the effectiveness of the information security awareness training. Employees are required to complete assessments after conducting the information security training. It has been shown that some employees are not interested in taking these assessments and because they are not mandatory. This result may be explained by the fact that there is lack of enforcement over employees to take or complete the test.

The research data also show that the majority of the organisations do not have any information security awareness measurement programs in place. This could lead to less effective outcomes from information security awareness training programs because the role of information security awareness measurement is to determine how effective the information security awareness training program is in establishing a strong information security awareness program. Information security awareness tests proves that the information security awareness training program is effective in employees to protect the company against threats.

It is therefore suggested that the awareness program should clearly define the objectives, identify strategies, and success measures. The next step is developing and implementing the evaluation tools to measure the effectiveness of the awareness program. Prior to the training, a baseline should be established by testing the employees' awareness level. After training, another test must be completed by the same employees. Finally, the results and behaviour should be compared of the employees before and after the training.

The implementation of measurement methods should include simulations and questionnaires to determine employees' information security awareness levels and draw feedback in order to redesign and improve the information security awareness program interventions. For example, a passing information security awareness test proves the employee understands the difference between identity fraud and a phishing attack. If an employee fails the information security awareness test, then they are not well aware of the concepts of information security. A maximum passing score means that the candidate is well aware of the information security concepts and has good knowledge about them.

Information security awareness measurement could utilise technology such as interactive multimedia and simulation to ensure that employees have the necessary knowledge and skills to identify, prevent, report, and respond appropriately when they are exposed.

5.4.3.3 Third-Party Management

As mentioned in the literature review, information security incidents from ICT outsourcing have dramatically increased. Third parties are considered one of the critical information security risks. It was indicated that proper third-party management is vital to minimise its risk and protect organisations data assets. Third parties can be employees, contractors, service providers, or partners who have access to sensitive data and systems. It was also emphasised that due to the shortages of skilled people in the Saudi Arabian working population, more migrant labour and workforce are needed from different countries resulting in an increase of the ICT outsourcing services demand. Therefore, proper management of third parties is vital in Saudi organisations.

The data from Group A indicated that many organisations in Saudi Arabia outsource their ICT and information security services to third parties in which the level of outsourcing varies from very limited services testing to full ICT services outsourcing. The data revealed that all organisations perform an adequate level of information security checks to ensure third-party eligibility and may perform information security assessment as well as signing non-disclosure agreements with third parties. Furthermore, they monitor the third parties by doing a regular security assessment to ensure their adherence to the provided rules and also enforce their policies.

In contrast to the Group A findings, the Group B findings reveal that most organisations in Saudi Arabia have very poor third-party management. It was indicated that third parties involved in small-sized projects are not given the same attention in terms of the enforcement of policy and procedure. Further, in larger projects, the enforcement and proper assessment only takes place at the beginning of the project most of the time. This result may be explained by the fact that the awareness of the importance of third-party management is very low. Another reason could be the increased level of trust towards third parties, which could be influenced by the national culture.

It is therefore suggested that organisations in Saudi Arabia must enforce a third-party management program that includes the following:

- Managing third-party risks: A comprehensive and well-written contract, which outlines the rights and responsibilities of all parties such as policies, controls, and risk monitoring.

- Top management support: It is the top/upper management's responsibility to establish a culture of collaboration with the third-party, while also controlling the risks that may emerge.

- Evaluate the third-party management program effectiveness: The third-party management must be evaluated by the program regularly to identify potential risks and to ensure that compliance requirements are met.

- Utilising technology: Technology could assist in facilitating and managing third parties

by automating processes, risk management, audits, compliance, and performance.

5.4.3.4 Risk Management Process Automation

One interesting finding of this research was the risk management process automation influence on the ISRM effectiveness. The risk management automation eliminates error, assists with decision-making, facilitating tasks, and improving performance. Moreover, it collects, organises, and categorises risk management data accurately and enables constant monitoring.

The results of this research revealed that a complicated risk management process influences ISRM effectiveness in Saudi organisations. It was indicated that spreadsheets are still in use during the risk assessment phase, which makes it harder to collect and assess the data. Moreover, it makes it more difficult to make decisions and implement effective planes. This can lead to less effective choices or even worse outcomes than if they were made with minimal complexity. A possible explanation for not utilising automated risk management tools is the cost and return of investment (ROI). Risk management automation tools are quite expensive and some organisations do not have dedicated budget for that. It is possible that they do not see the value of it or do not have proper ROI.

Therefore, it is suggested that organisations in Saudi Arabia leverage automated risk management tools and technology. It could help in resolving many ISRM issues discussed in the previous sections, such as the ineffective collaboration between different risk assessment teams, improper risk assessment, and unclear roles and responsibilities. Risk management automation assists organisations receiving accurate and accessible data that improves the risk analysis and reporting. Moreover, it helps organisations to act proactively with regards to risk acceptance and mitigation. Automation of risk management may improve risk scoring activities, indicated in Section 4.6.1.3, based on the likelihood and the impact because organisations can determine which risks pose the biggest threat in a more accurate and efficient manner.

5.5 The Enhanced ISRM Model

The enhanced ISRM model is an incorporation of the factors derived from literature and the data collection phase one analysis and discussion. The review of literature revealed eleven factors that were discussed in Section 2.8 and presented in the initial ISRM model Figure 2.7. In the same manner, the phase one data collection supported some of the factors presented in the initial ISRM model and, more importantly, revealed new factors that may influence ISRM effectiveness in Saudi Arabia. Accordingly, the enhanced ISRM model was developed and presented in Figure 5.1.

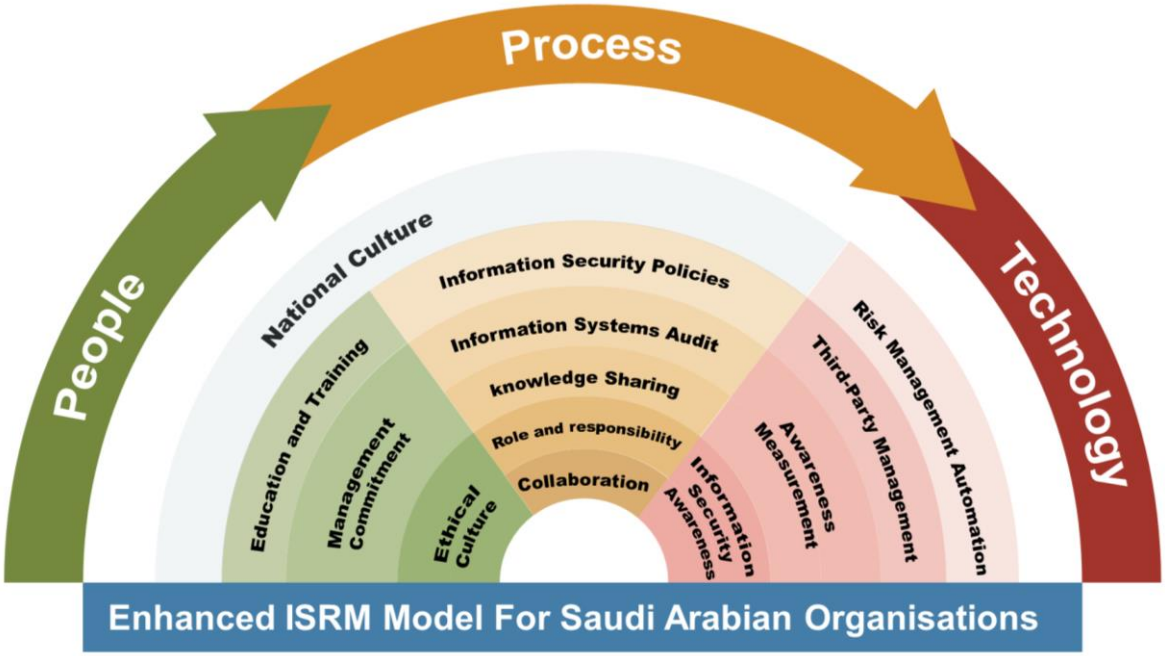

Figure 5.1 Enhanced ISRM for Saudi Arabian Organisations

Source: Researcher's Compilation (2021)

5.6 Summary

This chapter discussed the results from the phase one data collection. In this chapter, the researcher was able to answer the research questions and provide interpretation for data in the previous chapter. Accordingly, the researcher was able to develop the enhanced ISRM model for Saudi organisations. The enhanced ISRM model was developed based on the initial ISRM model presented in CHAPTER 2 and the factors extracted and analysed from the

interviews.

The next chapter discusses an evaluation of the enhanced ISRM model developed by presenting the ISRM model to focus group participants. The result is the proposed ISRM model.

CHAPTER 6. EVALUATION OF THE ISRM MODEL

6.1 Introduction

The previous chapter presented the enhanced ISRM model, which provides the groundwork of this research. As discussed in Section 3.5.3, this research data collection was conducted in two phases. The first phase, the qualitative semistructured interviews, provided a broad view and evaluation of research problem as well as the enhancement of the initial ISRM model. The second phase, the focus groups, provided a final overview and feedback of the developed ISRM model.

This chapter discusses and evaluates the enhanced ISRM model developed throughout this research. In order to obtain the desired results, the enhanced ISRM model which emerged from the literature review and the phase one data analysis was presented to participants. They were then asked to discuss current ISRM issues, experiences, and improvements related to the ISRM model for Saudi organisations. Also, they were asked specific prompt questions which encouraged them to identify factors that could aid or should be avoided the proposed ISRM model for Saudi organisations.

Focus group methodology, sampling, and participant characteristics are discussed in Section 3.5.3.2 and Section 3.5.3.3, respectively. Data interpretation and discussion from focus groups are presented in this chapter focusing on PPT dimensions factors. Finally, the research question is addressed and proposed ISRM model for Saudi Arabian organisations is presented.

6.2 Data Interpretation

All focus groups participants were asked the same questions and were encouraged to discuss their experiences, views, and opinions through open-ended questions. The questions covered a number of aspects, including participants' view of the need for enhanced ISRM model for Saudi organisations, their perspective and feedback on an enhanced ISRM model, and the likelihood of compliance improvement. The following subsections interpret the data

collected from the focus group participants.

6.2.1 The Need for Enhanced ISRM Standard

The researcher asked the participants questions regarding the need for an enhanced ISRM standard to best fit Saudi organisations. Table 6-1 shows that more than 80 percent of the participants agreed that there is a need for an enhanced ISRM to best fit Saudi Arabia. The data indicated that Saudi organisations face challenges with implementing the international ISRM standards in which they are less effective and should be enhanced accordingly.

"Yes, I think we need to have local security standards initiatives organised by the government" FP2

"I think available the security management standards in the market is good but they need so much work to make it better working in our company environment…. We use 2 standards the iso 27000 and NIST and we still think that they need some changes in the controls for example" FP7

It is apparent from this table that only two participants did not see the need for a localised ISRM standard. One of the participants stated:

"The ISO is ok for us… we didn't need to look for alternatives… I think every company has to work with standards according to their needs… you cannot find a standard that is applicable for all" FP3

The other participant outsourced ISRM activities to a third-party and felt confident that they do great job with the international ISRM standard:

"I don't think it's necessary to have ISRM standard specific for us… I mean Saudi Arabia… Our contractor is doing well with risk management and we are satisfied with the outcome" FP11

Table 6-1 Participant Reply about the Need for Enhanced ISRM in Saudi Arabia

Focus Group	Participant	The need for Enhanced ISRM Standard	Organisation's Industry/Classification
G1	FP1	Yes	Health/Private Sector
	FP2	Yes	Education/Public Sector
	FP3	No	Government Agency/Public Sector
	FP4	Yes	Retail/Private Sector
G2	FP5	Yes	Retail/Private sector
	FP6	Yes	Financial Institute/Private Sector
	FP7	Yes	Government Agency/Public Sector
	FP8	Yes	Government Agency/Public Sector
G3	FP9	Yes	Government Agency/Public Sector
	FP10	Yes	Financial Institute/Private Sector
	FP11	No	Retail/Private sector

The next subsections present the data from the participants' perspectives and feedback after they were introduced to the enhanced ISRM model for Saudi organisations.

6.2.2 People

Participants were presented with the enhanced ISRM model and were asked if it encompassed the factors that they consider important. Factors related to the People dimension were reviewed by the participants, starting with national culture. National culture was the key topic discussed by the focus group. The data revealed that there is a lack of security culture in many organisations that could potentially pose a great security risk to the organisations. It was indicated that for an effective ISRM, culture should be considered prior to commencing any IT security-related activities.

"Yes yes… I can see security culture is the main reason… we need security culture across entire our company" FP3

"Our culture is different… so much.. we face problems with culture all the time… but during the recent years we see some improvement specially with the new regulations" FP8

"People must understand the culture before starting any security activities in any organisation… culture make huge difference… culture is different for each company" FP

The majority of participants agreed that supportive management is the key for an effective ISRM in Saudi organisations. Proactive managers behaviour is highlighted again, which ties with the research findings in data collection phase one.

"Without the management support… we cannot achieve any our company security goals… that's why when we face issues with other department for example, we reach them to gain support and help resolving these issues…" FP3

"The mindset of reactive management is a major concern I think… we need supportive proactive thinking… security is still not their major concern" FP7

"I totally agree with others… management initiatives in this manager is necessary… what I notice with most enterprises in Saudi Arabia is that things come from bottom-up… it's not working like this" FP8

The data from focus groups indicated that ethical culture and risk management skills are not as important as other factors under People's dimension. Only participants provided their thoughts about these two factors, such as:

"We do have strong ethics and morality in our environment but it could be better… I'm not sure if we should give it a priority because we have other activities that are more important… I think" FP7

"I'm not sure if ethics are directly related to our subject" FP11

"In general, there is a problem with risk management understanding… it's not well understood by many of the staff even some senior managers… that's why in some cases we need to fight to get the risk activities done properly, even sometimes we know that the reports provided are not actually correct but we can do nothing… Its lack of understanding mainly" FP7

In summary, most of the participants concurred that national culture, management commitment and support, ethical culture, and risk management skills are vital factors which Saudi organisations must consider for an effective ISRM. Participants could not determine additional factors to be considered under the People's dimension. Their feedback indicated that these factors presented in the enhanced ISRM model are sufficient for the purpose of

developing the proposed ISRM model for Saudi organisations; therefore, the researcher will not modify People's dimension factors in the proposed ISRM model.

6.2.3 Process

The participants were asked to provide their feedback about Process dimension factors presented in the enhanced ISRM model. The data showed that participants had more interest discussing these factors and it was clear that Process dimension factors captured their attention more than the People's dimension did as new factors emerged from the discussion. Some of these factors are valuable and have been incorporated in the proposed ISRM model.

From the focus group data, more than 90 percent of the participants agreed that a proper information systems audit is crucial for an effective ISRM in Saudi Arabia. There were several opinions regarding the information systems audit influence on risk management. It has been confirmed that Saudi organisations face issues with carrying out a proper information systems audit due to disqualification and lack of expertise. Participant FP8 stated:

"Sometimes audit tasks are being assigned to nonexperience employees due lack of expertise or even tight schedules" FP8

Also, another participant stated that audit reports related to information security might be overlooked by the management because information security is not their priority.

"The only issue with audit is the management response with regards the provided report by the audit team, usually external, financial audit are very critical in their view" FP

In the same manner, more than 90 percent of the participants confirmed that roles and responsibilities are a major concern in Saudi organisations that could reflect the effectiveness of the ISRM. The data indicated that the majority of the organisations—especially government agencies—need clearer and updated roles and responsibility in order to perform better and improve ISRM effectiveness.

"With no clear roles and responsibility… no one would do tasks that they think it's not their responsibility… we face that so often during the risk assessment phase" FP

"I cannot emphasise it more… roles and responsibilities are not well

prepared which make work with other employees quite complicated… if we have established and well documented responsibilities and can avoid conflicts and save too much time at work… this issue can be seen in most government entities" PF

The data showed that sharing of knowledge was controversial with just over 35 percent of participants agreeing that it is an important factor in the ISRM model, while the rest could not perceive its importance. However, it was indicated that information security knowledge sharing is not well practiced in Saudi organisations due to lack of regulation, which support the results in the literature review and the data collected in phase one.

"We have no official channels to share security with others… sometimes during conferences or meetings but not in a regular basis… I think it's a good idea to have a hub to share knowledge with other entities in the region… it will be a win-win for all" FP

"Knowledge sharing has nothing to do with risk management I think… could be in direct" FP

The data indicated that ISP was the main Process dimension factor in which all participants agreed was vital for an effective ISRM. Some participants argued that ISRM cannot be successfully implemented with poor ISP due to its role in the risk management activities. Moreover, it was indicated by other participants that enforcement of the ISP is necessary because they believe that it potentially reduces risk exposure.

"I believe that policy is the key for healthy and security environment… considering enforcement and sanction because some staff do not follow the rules without enforcement" FP7

"No policy means no security… that's why we fight to enforce it" FP

Another factor that was discussed was the cross-departmental collaboration factor. More than half of the participants agreed that it is an issue that needs to be considered in the ISRM model. The data demonstrated that the collaboration among different units within an organisation is vital during the risk management activities. Collaboration was considered important for effective risk treatment plan implementation because it needs a timely commitment from all units of the organisation and therefore the collaboration is vital.

"Collaboration is very important not only between departments but in the whole company" FP

"It is very necessary to have collaboration all the time during risk management cycle… especially during the risk treatment plan implementation phase… sometime we face resistance with other departments during this phase… they do not give it a priority regardless of the severity of the risk" FP

The last factor under the Process dimension in the enhanced ISRM model was the ICT outsourcing factor. Surprisingly, the data showed that ICT outsourcing was not of significant important for most of the participants and therefore does not have a significant influence in ISRM effectiveness.

Unlike the People's dimension, new factors emerged from the data in this discussion. Risk transparency was suggested by some participants as a potential factor that may influence ISRM in Saudi organisations. It was indicated that the lack of transparency, especially during the risk assessment phase, could negatively impact the risk management activities as a result, as commented by this participant:

"One of the elements that you might consider is the transparency… risk transparency… it plays a role in the risk management progress… for example sometime we realise that there is something not right during the assessment phase that we could relate to the transparency" FP

Another participant confirmed that risk transparency could be considered a factor that influences ISRM and therefore could be added to the proposed ISRM model. It is clear that from the participants' feedback that there is a concern regarding the transparency level that could negatively influence ISRM in some organisations in Saudi Arabia.

"It's a valid point that transparency could be added as in your design model because transparency is very important in risk management… we face issues with the transparency" FP

In the same manner, the handover process was highlighted by the participants as another factor that could be considered in the proposed ISRM model. It has been indicated that in some cases, risk management activities could not be carried out due to a poor handover process among team members within an organisation. For example, some employees could not provide data about their information or IT assets because they do not know that these assets exist due to poor handover as highlighted by FP:

"Handover can be a problem… we face it all the time when someone

leave the company and someone else takes his place… sometimes we need to contact those who left the company recently to verify some information about the existence of some assets" FP

Enforcement was the last Process dimension factor highlighted by the participants. The data revealed that policy enforcement is an essential factor that influences ISRM in Saudi organisations. It was indicated that the non-compliance behaviour within some organisations in Saudi Arabia is a result of inconsistent policy enforcement. Moreover, the data showed that third parties could pose an information security risk for Saudi organisations due to the inconsistent policy enforcement as commented by participants:

"To be honest… there is no proper enforcement due to many reasons… I think culture that you mentioned earlier and management as well…. sometimes when we have a project with a tight schedule, we tend not consider enforcement and the same thing with vendors" FP

"External policy enforcement… I mean by external is our service providers or third parties… they do not follow our procedure sometimes however the management do not take series actions" FP

Overall, these results confirmed that information systems audit, roles and responsibilities, ISP, and cross-departmental collaboration are vital Process dimension factors that Saudi organisations must consider for an effective ISRM. It has been indicated that the knowledge sharing factor did not show much interest. However, other factors such as risk transparency and the handover process have been initiated during the discussion as Process dimension factors. It has been revealed that these new factors could influence the effectiveness of ISRM in Saudi organisations. Therefore, process dimension factors are reconsidered in the discussion section later in this chapter.

6.2.4 Technology

Issues related to the Technology dimension that influence the effectiveness of ISRM were discussed with the focus groups participants. The participants were asked to provide their feedback about factors presented in the enhanced ISRM model. The data showed that technology factors were critical for most of the focus group participants.

Ongoing IS awareness and training were considered crucial by all focus group participants. It was indicated that using technology would significantly assist in delivering

timely, efficient, and cost-effective IS awareness and training program. It includes online webinars, on-demand training, and self-assessment as commented below:

"I do not think that any company can survive from cyberattacks without intensive awareness program" FP

"Awareness is the key to stay ahead… we utilise some available services such as online as well as on-demand training depending on the level of employee in our company" FP

"The on-demand awareness program is cost effective with some drawback… I mean it needs to be enforced by setting up deadlines and required self-assessment" FP

Awareness measurement was considered vital by more than 70 percent of the participants. The data revealed that employees' awareness level is considered very low although training and awareness programs were provided. It has been indicated that the measurement of the awareness level is one way to determine the effectiveness of the awareness programs and also to determine the weakness. This would help in developing of more effective training and awareness programs which could improve information security awareness among the employees. This data links with the existence literature discussed earlier.

"As I said… enforcement for self-assessment is required to measure their awareness" FP

Moreover, the data showed that most of the Saudi organisations do not practice information security awareness measurement properly. It has been indicated that some organisations require their employees to take an assessment at the end of their training and awareness session as a mandatory requirement for their yearly appraisal. There is no actual measurement of the awareness level in this process because the employees who do not pass the awareness test are required to repeat the training and retake the test until they pass the it.

"We don't have something like that… actually there is a test at the end of the training and most of them do not take it because it's not required" FP

"Measurement of awareness… no… they are required to perform something like a quiz at the end of the training and they have to pass it… if

not they need to repeat until they pass" FP

The last technology dimension factor discussed was the risk management automation, which showed interest by more than 60 percent of the focus group participants. The data revealed that using technology such as risk assessment activities automation is a better approach for effective ISRM. It was indicated that risk management activities automation tools are efficient and could save time and money. However, some organisations in Saudi Arabia do not utilise such tools to automate their risk management activities, which supports the results in the data collected in phase one.

"Risk management tools is worth investment… I mean it's expensive but the return is very high… it save a lot of time and effort even communication efforts… assigning tasks and setting reminders follow-ups… many many benefits" FP

"I'm sure it useful tool… let's say fancy tool… because it's very expensive to acquire" FP

From the discussion, third-party management emerged as a new factor that could be included in the proposed ISRM model. It was indicated that third parties could pose risk for Saudi organisations; therefore, an effective management automation tool is needed to reduce their potential risk. Automation could help in categorising, tracking third-parties according to their risk level and assign the depth of necessary assessment individually as expressed by the following participant:

"We managed to automate third-party risk management that seems to be useful… previously we had many problems with managing vendors risk especially with the increase number of the vendors everyday… automation made it easier for us to track third-party… identify the depth of the assessments for each vendor" FP

In summary, these results show that IS awareness, awareness measurement, IT assets management, and risk management automation are crucial Technology dimension factors that Saudi organisations must consider for an effective ISRM. It has been indicated that the knowledge sharing factor did not show much of interest. Moreover, third-party management was suggested during the discussion as a technology dimension factor that could enhance the effectiveness of ISRM in Saudi organisations.

6.3 Discussion

The previous sections discussed the data collection phase two, the focus groups, and analysed the data obtained from the interviews. From the data, it was confirmed that there is a need for an enhanced ISRM to best fit Saudi Arabia due to many factors. These factors were discussed thoroughly with all focus group participants.

This section discusses the focus group participants' overview and feedback regarding the initial ISRM model factors in order to develop the proposed ISRM model for Saudi Arabian organisations.

6.3.1 People

Consistent with the literature and the results of the phase one data, it was confirmed that national culture is a key factor that influences the effectiveness of ISRM in Saudi organisations. The data indicated that the consideration of national culture may assist in understanding the organisational culture resulting in a proper IT security-related activities plan could be developed and implemented. This result may be explained by the fact that national culture consideration is vital for developing any organisational program such as ISRM because not doing so could result in conflicting and immature programs.

One interesting finding emerged from focus group data, one that has not been indicated earlier in this research, was the risk transparency factor and its possible influence in ISRM effectiveness. Transparency can be defined as the quality of organisations or individuals of being open to explicitly disclose information, plans, processes, and actions (Meijer 2009). It can contribute to organisations' corporate sustainability and proactive management (Vaccaro and Echeverri 2010). Risk transparency is the idea of being transparent about what could happen as indicated by the participants because there is a tendency to hide information about potential risks for unknown reasons. It was clear that participants were pointing to the transparency during risk management activities, which demonstrates how transparency could influence the risk management process. This result may be explained by the fact that transparency could be influenced by the national and organisational culture as well. Therefore, awareness of the importance of transparency, especially during risk

management activities, could possibly help in improving risk transparency. Moreover, the transparency must be a top-down approach, meaning that transparency culture must be promoted by the top management.

Although the remaining factors such as management commitment, ethical culture, and education and training were discussed with no significant input from the participants, who indicated that those factors are important and may influence ISRM effectiveness. A possible explanation for this might be that those factors are not as significant as the national culture factor. These findings suggest that all Peoples' dimension factors are significant and therefore will be considered in the proposed ISRM model.

6.3.2 Process

Process dimension discussion was more of an interest for most of all focus groups and new significant factors emerged from this discussion. The results confirmed the findings from phase one that information systems audits are consistently carried out by Saudi organisations. However, assigning non-qualified employees and the disregarded audit reports by the management have been indicated as concerns that may negatively influence ISRM. A possible explanation for these results may be related to the lack of necessary risk management skills discussed in the previous chapters and the management's low awareness of the importance of information security.

The data also confirmed the findings from the phase one data that some Saudi organisations, especially government agencies, have poor or outdated roles and responsibilities documentation. This could create a gap among employees involved in risk assessment activities because they are not aware their responsibilities in these activities and, as a result, all risk management activities would be affected.

These data were unable to demonstrate that knowledge sharing can be considered an important factor. It has been indicated that it would not influence ISRM effectiveness because there is little or an indirect relation between ISRM and knowledge sharing. This rather contradictory result with the findings from the literature has been discussed in the previous chapter.

The data confirmed the findings from the literature and the phase one data that ISP is a critical factor influencing the effectiveness of ISRM. It has been indicated that a well-established ISP plays a major role in successful risk management activities; however; enforcement could be the key to accomplish that. There is an indirect relation between policy enforcement and ISRM; for example, enforcing a policy could limit the exposure of confidential information and minimise the number of vulnerabilities in the organisations systems which results in a lower level of risk exposure.

In a similar manner, the data confirmed the findings from the phase one data that cross-department collaboration is an important factor for an effective ISRM. The reason was that collaboration could improve risk assessment activities because it may improve communication quality and therefore improve productivity among risk team members.

6.3.3 Technology

The results of this research show that technology-related factors are significant for an effective ISRM in Saudi organisations. Consistent with the results of the phase one data, it has been confirmed that utilising technology in information security awareness training programs could improve the effectiveness of ISRM in Saudi organisations. A possible explanation is that online webinars and on-demand training could save time and effort, and eventually reduce training costs. Moreover, such programs can be easily updated with the current security advancement.

In accordance with the present results, the literature and the data from phase one have demonstrated that measuring information security awareness is vital. Although most Saudi organisations do not practice it, the data validated that the awareness measurement could assist in identifying weaknesses that help in redesigning more effective awareness programs. Therefore, an awareness measurement should be part of a comprehensive information security awareness program.

In a similar manner, the data confirmed the findings from the phase one data that third-party management is an important factor that may influence ISRM effectiveness. It was indicated that third-party management tools could reduce possible risks posed by third

parties.

Finally, the results from the focus group confirmed the importance of the risk management automation factor for an effective ISRM. It has been indicated that risk management automation tools are not popular among Saudi organisations due to their high cost. Although the return of investment is high, it is possible that the management are not aware of its real value. The data and literature have indicated that Saudi Arabia is one of the top countries in technology investment. Therefore, an awareness program of the importance of technology for top management may assist in a better understanding of the role of technology in improving ISRM in Saudi Arabian organisations.

6.4 Proposed ISRM Model for Saudi Organisations

To answer the main question for this research which is: *What are the factors that must be considered when developing an effective ISRM model for Saudi Arabian organisations?*

In order to answer this question, a comprehensive review of the literature was conducted. This helped in constructing the initial ISRM model from factors that might influence ISRM effectiveness in large Saudi Arabian organisations. The next step involved collecting the phase one data, the semistructured interviews, which were analysed utilising the NVivo application to uncover significant factors which resulted in the enhanced ISRM model. Finally, phase two data, the focus group, was analysed the same way to confirm and support previous results that were used to reveal the proposed ISRM model which could be used to improve ISRM standards effectiveness in large Saudi Arabian organisations as shown in Figure 6.1. These factors were discussed in a great detail in the previous chapters.

An Arabic translation version of the proposed ISRM model is included in Appendix 6.

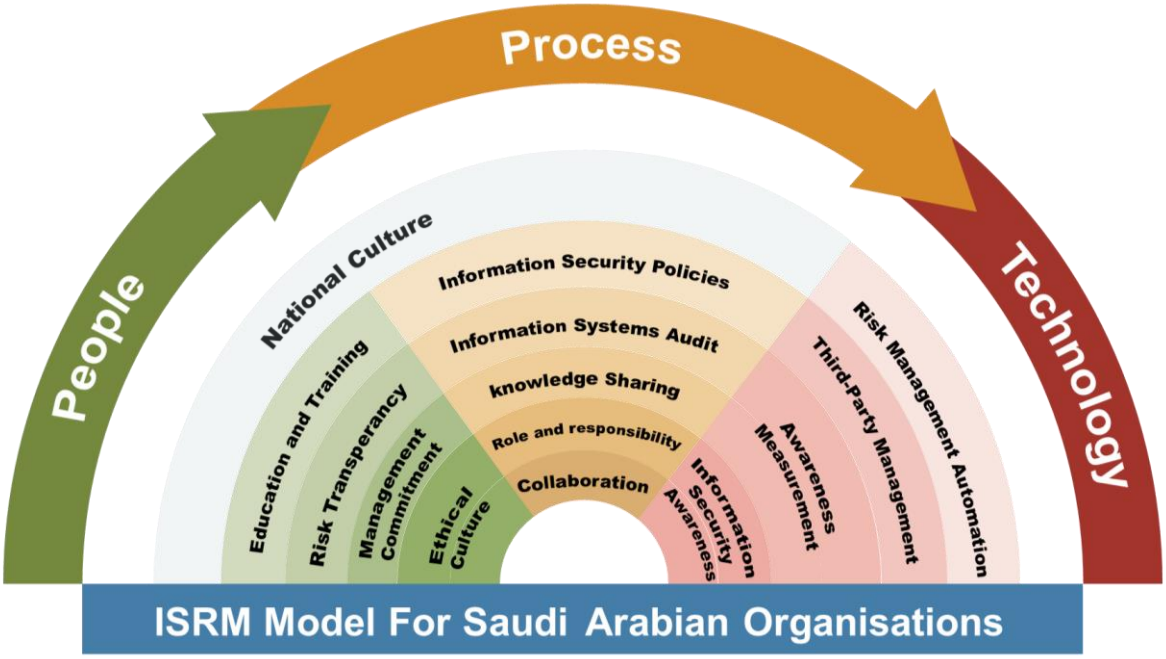

Figure 6.1 The Proposed ISRM for Saudi Arabian Organisations

Source: Researcher's Compilation (2021)

6.5 Summary

This chapter examined and confirmed the potential ISRM factors that emerged from this research. The focus group data were carefully coded and qualitatively analysed, which revealed a number of interesting factors that were discussed and considered in the proposed ISRM model.

Similar to phase one, phase two data themes were grouped into PPT dimensions. The data showed that national culture under the People's dimension was one of the main factors that influence ISRM effectiveness. Moreover, risk transparency was revealed as a new factor that may influence ISRM in Saudi organisations. Risk transparency was then considered in the proposed ISRM model. It was clear from the data that an information system audit is the key factor under the process dimensions. Finally, utilising technology for training programs in information security awareness is a key factor that may influence the effectiveness of ISRM in large Saudi Arabian organisations.

CHAPTER 7. CONCLUSION

This chapter summarises the major findings of this research based on the objectives and research questions defined in Chapter 1. A summary of the research highlights the results that contributed to information and security risk management theory and practice. The research significance, limitations encountered in conducting this research, and future research opportunities within this field are suggested. Finally, a summary of the chapter is presented.

7.1 Summary of the Research

The researcher studied the ISRM implementation challenges and the factors that influence ISRM in large Saudi Arabian organisations based on academic research. All of the factors that emerged from the literature review were combined to develop an integrative model. To this end, three research questions were considered that followed an inductive reasoning approach as they attempted to extend the existing literature through theoretical contributions in the field of information security risk management.

Given the nature of this study, an exploratory research method was used. It is a form of research carried out when there is a need for a greater understanding of a topic, especially if the area of research has not been done before. The choice of this research method is further justified by the lack of systematic research about the ISRM phenomenon in the Saudi Arabian context. This research design is a top-down approach that demonstrates the research progress stages. A cross-sectional time horizon was employed for data collection, which provided advantages because data can be collected within a shorter time frame. The participants can be observed simultaneously at a specific time. In this sense, the data collection process requires less effort.

Sampling phase one used semistructured interviews. The participants were divided into Groups A and B to achieve data triangulation. Group A had 10 prequalified participants from information security specialists from the top 100 Saudi Arabian companies in 2018, public universities, government agencies, and IT vendors within Saudi Arabia. The data

obtained from the interviews were analysed, and the data yielded were encoded using NVivo software package. Group B involved eight participants from IT security solution vendors, IT security consultation service providers, and information system integrators who provide their services to Saudi organisations. Thematic coding was used on the transcripts of the phase one data that unveiled the ISRM factors, resulting in producing the enhanced ISRM model.

In sampling phase two, the researcher approached and recruited the focus group participants through LinkedIn. The participants were drawn from CIOs, IT managers, security engineers, and security analysts, with four participants in each of the three focus groups. The data obtained during the focus group phase were analysed using the NVivo Software package.

From the first sub-objective of this research, the researcher posed the first research question: "What is the level of Saudi Arabian large organisations' compliance with ISRM standards?"

The prior research conducted on government agencies, healthcare, defence, financial institutions, and private enterprises have noted that only a few Saudi Arabian organisations comply with ISRM standards. However, the research results discussed in Section 5.3.3.1 indicated that 90 percent of the organisations comply with one or more ISRM standards such as ISO, NIST, COBIT, PCI, and the ISF Standard of Good Practice. This research findings contradict previous studies that noted that ISRM is poorly implemented in Saudi Arabia. The observed increase in ISRM compliance could be attributed to the Saudi Arabian government's introduction of new information security initiatives discussed in Section 3.7.2.2 that emphasises the need to comply with information security standards. Moreover, the increased number of cyberattacks on critical and major economic organisations could be another reason that has encouraged Saudi organisations to reassess their information security approach, leading to strict compliance with international information security standards such as ISRM standards.

In fact, the Saudi government has begun to recognise the importance of information security through initiatives that promote the adoption of information security standards. This way, a regulatory environment favours initiatives that comply with international information security standards such as ISRM standards. These initiatives have introduced mandatory

requirements to enhance compliance with information security standards, including ISRM standards such as ISO 27005, which are considered key to improving information security.

From the second sub-objective of this research, the researcher posed the second research question: “What are the ISRM standards implementation challenges in Saudi Arabian organisations?”

Based on the literature review, one of Saudi Arabian organisations' main challenges is the shortage of information security expertise. The education system outcome is poor in quality information security and risk management education and training programs. Now the need arises as cyberattacks target Saudi Arabia's most significant infrastructure. Likewise, previous studies highlighting how managing IT assets can be daunting because the IT and data assets are not included in the organisation's assets registry, making it difficult to identify the assets and their associated risks. Another identified reason could be the faulty evaluation of some assets, which invariably leads to an unrealistic risk rating that could negatively impact the risk management process. In addition, the data revealed that when a risk is identified in a particular department, it takes a considerable amount of time to identify the asset owner and takes even more time to mitigate the risk due to poor communication. The generic nature of ISRM standards instructions and guidelines from previous literature has also been identified as a pressing challenge.

Another challenge identified was the language barrier as when translating standards and policies from English to Arabic, misinterpretations can be generated. Finally, the study revealed that due to the increasing number of ISRM approaches available, choosing the appropriate ISRM standard becomes difficult. In this sense, the proposed model can help organisations implement ISRM and effectively protect their information assets. These revelations make it safe to infer that many ISRM challenges confound organisations in Saudi Arabia.

From the third sub-objective of the study, the third research question was formulated: “What are the factors that must be considered when developing an effective ISRM model for large Saudi Arabian organisations?”

This research considered the People Process Technology dimensions for improving

information security risk management in large Saudi Arabian organisations. Based on the literature review, the semistructured interviews and focus groups (with participants from organisations, public universities, government agencies, and IT vendors within Saudi Arabia) were defined and validated 14 factors that influence ISRM effectiveness in large Saudi Arabian organisations. The factors are grouped in the people, process, and technology dimensions as follows:

- People. Crucial for successful implementation and maintenance of risk management in an organisation is considering employees' behaviour towards information security. For this reason, an organisation needs a trained team that understands the risk culture, focuses on improving security awareness, provides security-specific training regularly, and improves the organization's security culture to comply with information security policies and procedures in organisations. The people dimension includes the following factors: national culture, ethical culture, education and training, management commitment, and risk transparency.

- Process. The enabling of an operation or task in an organisation that produces a specific goal. To successfully manage an organisation’s IT risk is the audit for an IT infrastructure that needs to meet quality minimum requirements according to policies and standards, with the cooperation between departments to address challenges. Likewise, employees with clarity on roles and responsibilities perform better and contribute to successful ISRM in Saudi organisations. In addition, it is important to share information security knowledge because the field changes rapidly, and new threats and information security best practices could potentially improve organisations’ security posture. The process dimension includes the following factors: information systems audit, information security knowledge sharing, information security policies, roles and responsibilities, and cross-departmental collaboration.

- Technology. This corresponds to tools and techniques people use to work and communicate efficiently, including information systems and digital technologies that are changing the way business is being executed. The literature emphasised the importance of employees' attitudes and behavioural intentions as predictors of actual information security compliance, where information security awareness is one of the

strongest lines of defence in organisations against IT threats. Culture and education play a major role in the entire organizations' awareness level, hence the importance of IS awareness programs in organisations as a precautionary measure to prevent information security risks, third-party to technological support, or using management automation tools that require a dedicated budget. The dimension includes the following factors: ongoing information security awareness program, information security awareness measurement, third-party management, and risk management process automation.

7.2 Research Significance

This project is a valuable resource for academics, researchers, and practitioners in information security risk management in large Saudi Arabian organisations. The main contribution of this study is the ISRM implementation challenges, ISRM standards level of compliance and the regional-specific ISRM model for large Saudi Arabia organisations based on newly identified factors considering national culture reflecting the context situation. The literature review provided the essential theoretical background to determine the research gap. The semistructured interviews and focus groups were essential to define and validate the factors influencing ISRM effectiveness in large Saudi Arabian organisations. In this way, the significance of this model lies in understanding the ISRM effectiveness considering cultural and social implications in Saudi Arabia. Likewise, the proposed ISRM model can serve as a reference for similar economies considering that organisations face digital transformation processes, and also adopting and using digital technologies that require best practices to protect information assets. There are several implications for further research which may expand on the insights yielded by this research.

This research also has practical implications. Based on the model that improves ISRM implementation effectiveness in large Saudi Arabia organisations, the project contributes to the awareness of ISRM in Saudi Arabia to assist organisations in adopting ISRM and implementing it more effectively. The outcomes of this research will be relevant to both public and private organisations belonging to different economic sectors to implement ISRM and effectively protect their information assets. The ISRM model can make organisational

business processes more efficient and resilient to cybercrimes in response to rapid technological change. Moreover, it is also relevant to other Gulf Cooperation Council (GCC) countries due to its cultural, commercial, and economic similarities serving as a base for further studies, assisting organisations in adopting ISRM in developing economies.

7.3 Research Limitations

All research projects suffer from limitations that generate complications in fulfilling the research objectives, providing directions for future research. The model development had not considered the following control variables, which may produce different statistic results such as industry type, education level, and organisation maturity level.

Due to the sensitivity of the research topic and the confidentiality of the data, it was not unproblematic to convince potential participants to contribute to this research. The study participants were reluctant to disclose information that might be considered confidential. Considering that the study addressed security issues in the organisation, the participants refrained from answering the questions openly, fearing that their answers would go against the organization's policies, or, worse, could affect their organisation's reputation. In this sense, to avoid low participation, the researcher designed general research questions about security that would not cause a breach of the confidentiality clause or the divulgence of sensitive organisational data.

The search for candidates to participate in the study took several months, and LinkedIn allowed to approach and recruit the participants. After that, they were contacted via email. The researcher conducted semistructured interviews and focus groups with the obtained sample size via WebEx and Zoom online meeting platforms. Despite these efforts, the response rate was low, approximately 10 percent.

Additionally, there can be a biased response in interview and focus group data. Cultural factors such as saving face, inability to accept criticism, and believing “everything is fine” affected the responses, especially when interviewing management participants.

Another limitation was the limited budget available for research. Saudi Arabia is

geographically large and the population is dispersed widely. The researcher could not afford travel costs, such as flights and accommodation, especially since there were three phases of data collection. This financial limitation was compounded because the researcher is based in Australia. In addition to distance, the time zone difference between Australia and Saudi Arabia was also a limitation because it made contacting participants more challenging. These variables also influenced the communication with universities and the smooth scheduling of participants for data collection.

Although it was difficult to avoid all limitations during project execution, the research presents a useful perspective regarding the factors required to introduce the ISRM model in Saudi Arabia organisations successfully.

7.4 Future Research

Based on the findings, contributions, and limitations of the research, future research may include the following:

- Apply the ISRM model to Saudi Arabia and other countries in the region, such as Gulf Cooperation Council (GCC) countries, and other Middle Eastern countries that share a similar culture. To this end, the countries should be explored, initially identifying legal and cultural aspects. Depending on the results, adjustments to the initial model can be proposed.

- Benchmark the proposed ISRM model from this research on security controls of any available ISRM standards such as ISO 27005 or NIST. This way, the applicability of the model can be deepened.

- Conduct a comparative study between Saudi organisations and other developed countries such as Australia, deepening in public policies existing in the country related to the massification of information and communication technologies in organisations.

- Conduct case studies or focus groups to gather rich contextual data on different means of creating a security culture in developing countries such as Saudi Arabia.

- Replicate the research in different environments and cultures to determine the role of culture in ISRM effectiveness.

- Conduct the research with small- and medium-sized enterprises as a unit of analysis, comparing the results with this research outcome.

7.5 Summary

The present research aimed to develop an effective ISRM model for large Saudi Arabian organisations. This research identified 14 factors grouped in PPT dimensions that influence organizations' information security risk management. These findings of this study suggest that most Saudi Arabian organisations have no set guidelines that aid the selection of appropriate ISRM standards. The findings will be of interest to understand why Saudi organisations have low information security levels and are exposed to related risks, contributing to an understanding of how ISRM practices must be aligned with organisational goals and objectives. The most important limitation lies in the fact that the model development had not considered the following control variables: industry type, organization size, education level, and organisation maturity level. In addition the study participants were reluctant to disclose information that might be considered confidential. Despite its limitations, the study certainly adds to the understanding of the factors required to successfully introduce the ISRM model in Saudi Arabian organisations. Further research might explore the applicability of the research model in different environments and cultures to determine the role of culture in ISRM effectiveness. Another important practical implication is that this research will be relevant to both public and private organisations in different economic sectors to implement ISRM and effectively protect their information assets.

REFERENCES

2017 Cost of Data Breach Study. 2017.

2018 Cost of a Data Breach Study: Global Overview. 2018.

2019 Cyberthreat Defense Report. 2019. Annapolis: Cyber Edge Group.

Abdur, Syed. 2015. "Leveraging Standards for Risk Assessment." https://www.bringa.com/standards-for-risk-assessment/.

AboulEnein, Sameh. 2017. "Cybersecurity Challenges in the Middle East." https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/GCSP-Cybersecurity%20Challenges%20in%20the%20Middle%20East.pdf

"About Citc." 2019. Communications and Information Technology Commission CITC. https://www.citc.gov.sa/en/aboutus/Pages/default.aspx.

"About Nca." 2020. National Cybersecurity Authority. https://nca.gov.sa/en/pages/about.html.

"About Us." 2019. ISO. https://www.iso.org/home.html.

Abu-Musa, Ahmad. 2009. "Exploring Cobit Processes for Itg in Saudi Organizations: An Empirical Study." *International Journal of Digital Accounting Research* 9: 99-126.

Abu-Musa, Ahmad. 2010. "Information Security Governance in Saudi Organizations: An Empirical Study." *Information Management & Computer Security* 18 (4): 226-276. doi:10.1108/09685221011079180.

AbuSaad, Belal, Fahad Saeed, Khaled Alghathbar, and Bilal Khan. 2011. "Implementation of Iso 27001 in Saudi Arabia – Obstacles, Motivations, Outcomes, and Lessons Learned" *Australian Information Security Management Conference*: Secau Security Research Centre, Edith Cowan University, Perth, Western Australia.

Adams, Jean, Belinda Bateman, Frauke Becker, Tricia Cresswell, Darren Flynn, Rebekah McNaughton, Yemi Oluboyede, Shannon Robalino, Laura Ternent, and Benjamin Sood. 2015. "Triangulation and Integration of Results." NIHR Journals Library.

Agrawal, Vivek. 2017. "A Framework for the Information Classification in Iso 27005 Standard" *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, doi:10.1109/CSCloud.2017.13.

Ajmi, Lama, Aldhubaiban Hadeel, Najla Alqahtani, Atta UrRahman, and Maqsood Mahmud. 2019. "A Novel Cybersecurity Framework for Countermeasure of SMEs in Saudi

Arabia" *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, doi:10.1109/CAIS.2019.8769470.

Akhyari, Nasir, AA Ruzaini, and AH Rashid. 2018. "Information Security Culture Guidelines to Improve Employee's Security Behavior: A Review of Empirical Studies." *Journal of Fundamental and Applied Sciences* 10 (2S): 258-283.

Akinyode, Babatunde, and Tareef Khan. 2018. "Step-by-Step Approach for Qualitative Data Analysis." *International Journal of Built Environment and Sustainability* 5 (3).

Al-Ahmad, W., and B. Mohammed. 2015. "A Code of Practice for Effective Information Security Risk Management Using Cobit 5" *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, doi:10.1109/InfoSec.2015.7435520.

Al-Ahmad, Walid , and Bassil Mohammad. 2013. "Addressing Information Security Risks by Adopting Standards." *International Journal of Information Security S*cience (2): 28-43.

Al-Ahmad, Walid, and Bassil Mohammad. 2012. "Can a Single Security Framework Address Information Security Risks Adequately." *International Journal of Digital Information and Wireless Communications* 2 (3): 222-230.

Al-Gahtani, Said S., Geoffrey S. Hubona, and Jijie Wang. 2007. "Information Technology (It) in Saudi Arabia: Culture and the Acceptance and Use of It." *Information & Management* 44 (8): 681-691. http://dx.doi.org/10.1016/j.im.2007.09.002.

Al-Saud, Naef. 2012. "A Saudi Outlook for Cybersecurity Strategies Extrapolated from Western Experience." *Joint Force Quarterly* (64): 75.

Al-Adaileh, Raid, and Muawad Al-Atawi. 2011. "Organizational Culture Impact on Knowledge Exchange: Saudi Telecom Context." *Journal of Knowledge Management* 15 (2).

Al Amro, Sulaiman. 2017. "Cybercrime in Saudi Arabia: Fact or Fiction?" *International Journal of Computer Science Issues (IJCSI)* 14 (2): 36.

Al Asmri, Mushabab. 2014. "Organisational Culture, Leadership Behaviour and Job Satisfaction among Primary Health Care Professionals in Saudi Arabia: A Mixed-Methods Study." School of Public Health and Social Work Queensland University of Technology.

Al Omoush, Khaled Saleh, Saad Ghaleb Yaseen, and Mohammad Atwah Alma'aitah. 2012. "The Impact of Arab Cultural Values on Online Social Networking: The Case of Facebook." *Computers in Human Behavior* 28 (6): 2387-2399. doi:https://doi.org/10.1016/j.chb.2012.07.010.

Alabdulatif, Afnan. 2018. "Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia." PhD Dissertation, University of Houston. https://uh-ir.tdl.org/handle/10657/3107

Alarifi, Abdulaziz, Holly Tootell, and Peter Hyland. 2012. "A Study of Information Security Awareness and Practices in Saudi Arabia" *Communications and Information Technology (ICCIT), 2012 International Conference on Communications and Information Technology.* IEEE. doi:10.1109/ICCITechnol.2012.6285845.

Alassafi, Madini O, Abdulrahman Alharthi, Robert J Walters, and Gary B Wills. 2016. "Security Risk Factors That Influence Cloud Computing Adoption in Saudi Arabia Government Agencies" *Information Society (i-Society), 2016 International Conference on Communications and Information Technology.* IEEE.

Alassafi, Madini O., Abdulrahman Alharthi, Robert J. Walters, and Gary B. Wills. 2017. "A Framework for Critical Security Factors That Influence the Decision of Cloud Adoption by Saudi Government Agencies." *Telematics and Informatics*. doi:http://dx.doi.org/10.1016/j.tele.2017.04.010.

Alcántara, Manuel, and Andrés Melgar. 2016. "Risk Management in Information Security: A Systematic Review." *Journal of Advances in Information Technology* 7 (1).

Aldosari, Sultan 2019. "A Review of Cybersecurity in the Saudi Arabian Context." *Journal of Contemporary Scientific Research* 2 (8).

Aldossary, A., and A. Zeki. 2013. "The Influence of Students' Knowledge on Security Towards Their Behavior with Security Risks within the Context of Saudi Arabia" *2013 International Conference on Advanced Computer Science Applications and Technologies*, doi:10.1109/ACSAT.2013.9.

Aldossary, A., and A. Zeki. 2015. "Web User' Knowledge and Their Behavior Towards Security Threats and Vulnerabilities" *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, doi:10.1109/ACSAT.2015.51.

Aldraehim, Majid Saad, Sylvia L Edwards, Jason A Watson, and Taizan Chan. 2012. "Cultural Impact on E-Service Use in Saudi Arabia: The Role of Nepotism." *International Journal for Infonomics (IJI)* 5 (3/4): 655-662.

Alelyani, Salem, and Harish Kumar. 2018. "Overview of Cyberattack on Saudi Organizations." *Journal of Information Security and Cybercrimes Research* 1 (1).

Alfawaz, Salahuddin M. 2011. "Information Security Management: A Case Study of an Information Security Culture." Queensland University of Technology.

Alharbi, Fawaz, Anthony Atkins, and Clare Stanier. 2017. "Cloud Computing Adoption in Healthcare Organisations: A Qualitative Study in Saudi Arabia." In *Transactions on Large-Scale Data- and Knowledge-Centered Systems Xxxv*, edited by Abdelkader Hameurlain, Josef Küng, Roland Wagner, Sherif Sakr, Imran Razzak and Alshammari Riyad, 96-131. Berlin, Heidelberg: Springer Berlin Heidelberg.

AlHogail, A., and A. Mirza. 2014. "Information Security Culture: A Definition and a Literature Review." *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, doi:10.1109/WCCAIS.2014.6916579.

AlHogail, Areej. 2015. "Design and Validation of Information Security Culture Framework." *Computers in Human Behavior* 49: 567-575. http://dx.doi.org/10.1016/j.chb.2015.03.054.

Ali, Inass. 2007. "Customer Relationship Management: A Qualitative Cross-Case Analysis in the Uk and Saudi Arabia." PhD Thesis, Stirling Management School.

AlKaabi, Ahmed. 2014. "Strategic Framework to Minimise Information Security Risks in the Uae." University of Bedfordshire.

Alkahtani, Hend, Ray Dawson, and Russell Lock. 2013. "The Impact of Culture on Saudi Arabian Information Systems Security." Loughborough University.

Alkahtani, Hend K. 2018. "Raising the Information Security Awareness Level in Saudi Arabian Organizations through an Effective, Culturally Aware Information Security Framework." PhD Thesis, Loughborough University.

Almarhabi, Khalid. 2016. "Adherence to Ict Security and Privacy Policies in Saudi Arabia." *International Journal of Computer Applications* 147 (4).

Almubayedh, Dhoha, Ghadeer Alazman, Manal Alabdali, Rouqaiah Al-Refai, and Naya Nagy. 2018. "Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study" *2018 21st Saudi Computer Society National Computer Conference (NCC)*: IEEE.

Almuqrin, Abdullah, Zuopeng Justin Zhang, Aljawharah Alzamil, Ibrahim Mutambik, and Abdullah Alhabeeb. 2020. "The Explanatory Power of Social Capital in Determining Knowledge Sharing in Higher Education: A Case from Saudi Arabia." *Malaysian Journal of Library & Information Science* 25 (3): 71-90.

Alnatheer, Mohammed. 2012. "Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia." Queensland University of Technology, Brisbane.

Alnatheer, Mohammed. 2015. "Information Security Culture Critical Success Factors" *Information Technology - New Generations (ITNG), 2015 12th International Conference on*, doi:10.1109/ITNG.2015.124.

Alnatheer, Mohammed, and Karen Nelson. 2009. "Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context." Australian Information Security Management Conference. https://ro.ecu.edu.au/ism/2/

Alotaibi, Faisal, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. "A Survey of Cyber-Security Awareness in Saudi Arabia" *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*: IEEE.

Alqahtani, Abdullah, Robert Goodwin, and Denise de Vries. 2018. "Cultural Factors Influencing E-Commerce Usability in Saudi Arabia." International Journal of Advanced and Applied Sciences 6 (6): 1-10.

Alqahtani, Sulaiman. 2018. "Developing and Assessing a Social Networking Framework for Universities in Saudi Arabia." School of Information Systems, Curtin University.

Alsaif, Maryam, Nura Aljaafari, and Abdul Raouf Khan. 2015. "Information Security Management in Saudi Arabian Organizations." *Procedia Computer Science* 56: 213-216. http://dx.doi.org/10.1016/j.procs.2015.07.201.

Alshammari, Tareq, and Harman Singh. 2018. "Preparedness of Saudi Arabia to Defend against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and Gci Index." *Archives of Business Research* 6 (12).

Alshitri, Khalid, and Abdulmosen Abanumy. 2014. "Exploring the Reasons Behind the Low Iso 27001 Adoption in Public Organizations in Saudi Arabia" *2014 International Conference on Information Science & Applications (ICISA)*, doi:10.1109/ICISA.2014.6847396.

Alsmadi, Izzat, and Mohammad Zarour. 2018. "Cybersecurity Programs in Saudi Arabia: Issues and Recommendations" *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*: IEEE.

Altinay, Levent, Alexandros Paraskevas, and SooCheong Shawn Jang. 2015. *Planning Research in Hospitality and Tourism*. Oxfordshire, England: Routledge.

Alumaran, Saleh, Giampaolo Bella, and Feng Chen. 2015. "The Role and Impact of Cultural Dimensions on Information Systems Security in Saudi Arabia National Health Service." *International Journal of Computer Applications* 112 (2). http://dx.doi.org/10.5120/19639-1217.

Alwazir, Albara, and Jacob Dichter. 2020. *Ussabc Economic Brief: Saudi Arabia's Emergence in Cyber Technology.* http://www.us-sabc.org.

Alzahrani, Ahmed, and Khalid Alomar. 2016. "Information Security Issues and Threats in Saudi Arabia: A Research Survey." *International Journal of Computer Science Issues (IJCSI)* 13 (6): 129.

Alzamil, Zakarya. 2012. "Information Security Awareness at Saudi Arabians' Organizations: An Information Technology Employee's Perspective." *International Journal of Information Security and Privacy* 6 (3): 38-55. http://dx.doi.org/10.4018/jisp.2012070102.

Alzamil, Zakarya 2018. "Information Security Practice in Saudi Arabia: Case Study on Saudi Organizations." *Information & Computer Security* 26 (5): 568-583.

Alzeban, Abdulaziz. 2015. "The Impact of Culture on the Quality of Internal Audit: An Empirical Study." *Journal of Accounting, Auditing & Finance* 30 (1): 57-77. doi:10.1177/0148558x14549460.

Amancei, Cristian. 2011. "Practical Methods for Information Security Risk Management." *Informatica Economica* 15 (1): 151-159.

Andress, Jason. 2011. "Chapter 1 - What Is Information Security?" In *The Basics of Information Security*, 1-16. Boston: Syngress.

Antunes, Mário, Marisa Maximiano, Ricardo Gomes, and Daniel Pinto. "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal." *Journal of Cybersecurity and Privacy 1*, no. 2 (2021): 219-238.

Armstrong, Helen. 2013. "Two Approaches to Information Security Doctoral Research" Berlin, Germany: Springer Berlin Heidelberg.

Arsene, Liviu, and Bogdan Rusu. 2020. *Iranian Chafer Apt Targeted Air Transportation and Government in Kuwait and Saudi Arabia*. https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf.

Ashenden, Debi. 2008. "Information Security Management: A Human Challenge?" *Information Security Technical Report* 13 (4): 195-201.

Atul, Vashistha. 2020. The Future of Risk Management Is Automated. *Forbes*.

Balter, Ariel, Ian Blazina, Nicolas Beard, Ilya Ivlev, and Joanne Valerius. 2006. "How Many Interviews Are Enough?" *Field Methods* 18 (1): 59-82.

Barafort, Béatrix, Antoni-Lluís Mesquida, and Antonia Mas. 2017. "Integrating Risk Management in It Settings from Iso Standards and Management Systems Perspectives." *Computer Standards & Interfaces* 54: 176-185.

Barbour, Rosaline, and David Morgan. 2017. *A New Era in Focus Group Research: Challenges, Innovation and Practice*. Berlin, Germany: Springer.

Bartol, Nadya. 2014. "Cyber Supply Chain Security Practices DNA – Filling in the Puzzle Using a Diverse Set of Disciplines." *Technovation* 34 (7): 354-361.

Beckers, Kristian, Maritta Heisel, Bjørnar Solhaug, and Ketil Stølen. 2014. "Isms-Coras: A Structured Method for Establishing an Iso 27001 Compliant Information Security Management System." In *Engineering Secure Future Internet Services and Systems*, 315-344. Berlin, Germany: Springer.

Bell, Jennifer 2018. Ksa Must Become More Resilient against Cyberattacks. Arab News. http://www.arabnews.pk/node/1343151/saudi-arabia.

Beňová, Vladimír Bolek–František Korček–Martina. 2015. "Information Security Risk Management in Slovak Enterprises." *CER Comparative European Research 2015*: 13.

Billings, Adam 2018. People, Process, Technology: Optimizing Risk Management Initiatives. *Corporate Compliance Insights*.

Biscoe, Chloe 2018. "Cyber Attacks Could Cost Saudi Arabia up to Sar30 Billion. IT Governance." https://www.itgovernancegulf.com/blog/cyber-attacks-could-cost-saudi-arabia-up-to-sar30-billion.

Bishop, David L., David S. Lee, O. C. Ferrell, John Fraedrich, and Linda Ferrell. 2018. *Business Ethics: Ethical Decision Making and Cases*. Boston: Cengage.

Bisman, Jayne. 2010. "Postpositivism and Accounting Research: A (Personal) Primer on Critical Realism." *Australasian Accounting, Business and Finance Journal* 4 (4): 3-25.

Bitzer, Michael, Nicolas Brinz, and Philipp Ollig. "Disentangling the Concept of Information Security Properties-Enabling Effective Information Security Governance." *ECIS*. 2021.

Bjerke, Bjorn, and Abdulrahim Al-Meer. 1993. "Culture' S Consequences: Management in Saudi Arabia." *Leadership & Organization Development Journal* 14 (2): 30-35.

Blake, Eben 2015. Iran and Saudi Arabia Heading toward a Cyber War. http://www.ibtimes.com/iran-saudi-arabia-heading-toward-cyber-war-1989789.

Borek, Alexander, Ajith Kumar Parlikad, and Philip Woodall. 2011. "Towards a Process for Total Information Risk Management" *Proceedings of the 16th International Conference on Information Quality, University of South Australia, Adelaide*,

Brain, Christine. 2001. *Advanced Psychology: Applications, Issues and Perspectives*. Cheltemham, UK: Nelson Thornes.

Breier, Jakub, and Frank Schindler. 2014. "Assets Dependencies Model in Information Security Risk Management." In *Information and Communication Technology*, edited by Linawati, MadeSudiana Mahendra, ErichJ Neuhold, AMin Tjoa and Ilsun You, 405-412. Berlin Heidelberg: Springer.

Broderick, J. Stuart. 2001. "Information Security Risk Management — When Should It Be Managed?" *Information Security Technical Report* 6 (3): 12-18.

Bronk, Chris, and Eneken Tikk-Ringas. 2013. "Hack or Attack? Shamoon and the Evolution of Cyber Conflict." *Global Politics and Strategy*.

Bundy, Jim 2021. Introducing an Automated Approach to Risk Management. OPTIV. https://www.optiv.com/insights/discover/blog/introducing-automated-approach-risk-management.

Calder, Alan. 2006. *International It Governance: An Executive Guide to Iso 17799/Iso 27001*. London, UK: Kogan Page Publishers.

Calder, Alan, and Steve Watkins. 2008. *It Governance: A Manager's Guide to Data Security and Iso 27001/Iso 27002.* London, UK: Kogan Page Ltd.

Calder, Alan, and Steve Watkins. 2010. *Information Security Risk Management for Iso27001/Iso27002*. Ely, UK: It Governance Ltd.

Carey-Smith, Mark. 2011. "Improving Information Security Management in Nonprofit Organisations." PhD Thesis, Queensland University of Technology. https://eprints.qut.edu.au/45717/.

Carter, Nancy, Denise Bryant-Lukosius, Alba DiCenso, Jennifer Blythe, and Alan J Neville. 2014. "The Use of Triangulation in Qualitative Research." *Oncology Nursing Forum*, 41 (5): 545-547.

Chandran, Daniel, and Abdullah Alammari. 2020. "Influence of Culture on Knowledge Sharing Attitude among Academic Staff in Elearning Virtual Communities in Saudi Arabia." *Information Systems Frontiers*: 1-10.

Chaula, Job, Louise Yngstrom, and Stewart Kowalski. 2006. "Technology as a Tool for Fighting Poverty: How Culture in the Developing World Affect the Security of Information Systems" *Fourth IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06)*: IEEE.

Chen, Hao, Patrick Chau, and Wenli Li. 2019. "The Effects of Moral Disengagement and Organizational Ethical Climate on Insiders' Information Security Policy Violation Behavior." *Information Technology & People*.

Chu, Xinmin, Xin Luo, and Yan Chen. 2018. "A Systematic Review on Cross-Cultural Information Systems Research: Evidence from the Last Decade." *Information & Management*. https://doi.org/10.1016/j.im.2018.08.001.

Chua, Hui, Siew Wong, Yeh Low, and Younghoon Chang. 2018. "Impact of Employees' Demographic Characteristics on the Awareness and Compliance of Information Security Policy in Organizations." *Telematics and Informatics* 35 (6): 1770-1780.

Cole, Ben. 2014. "Information Technology Audit." TechTarget. https://searchcompliance.techtarget.com/definition/IT-audit-information-technology-audit.

Cost of a Data Breach Report 2019. 2019. Michigan, USA: Ponemon Institute. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/.

Cost of a Data Breach Report 2020. 2020. Michigan, USA. https://www.ibm.com/account/reg/sa-en/signup?formid=urx-46542.

Creswell, John. 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 3rd ed. Thousand Oaks, CA: Sage Publications.

Creswell, John. 2014. *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research* 5th ed. Frenchs Forest, Sydney: Pearson Australia.

Creswell, John, and Cheryl Poth. 2018. *Qualitative Inquiry & Research Design: Choosing among Five Approaches* 4th ed. Thousand Oaks, CA: SAGE.

Da Veiga, Adéle, and Nico Martins. 2015. "Information Security Culture and Information Protection Culture: A Validated Assessment Instrument." *Computer Law & Security Review* 31 (2): 243-256. http://dx.doi.org/10.1016/j.clsr.2015.01.005.

Dhillon, Gurpreet, and James Backhouse. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives." *Information Systems Journal* 11 (2): 127-153.

Diab, Charbel. 2019. "Sama Cyber Security Framework Compliance: Deliver a Seamless and Secure Digital Banking Experience." https://www.onespan.com/blog/sama-cyber-security-framework-compliance.

Dinglasa, Ramil A. 2020. "Cultural and Emotional Intelligence: Its Role in the Cross-Cultural Adjustment of Filipino Expatriates in the Kingdom of Saudi Arabia." *International Journal of Human Resource Studies* 10 (1): 276303-276303.

Dols, Taco, and AJ Silvius. 2010. "Exploring the Influence of National Cultures on Non-Compliance Behavior." *Communications of the IIMA* 10 (3): 2.

Dubois, Éric, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. 2010. "A Systematic Approach to Define the Domain of Information System Security Risk Management." In *Intentional Perspectives on Information Systems Engineering*, edited by Selmin Nurcan, Camille Salinesi, Carine Souveyet and Jolita Ralyté, 289-306. Berlin Heidelberg: Springer.

Edmunds, Holly. 1999. "The Focus Group Research Handbook." *The Bottom Line*.

Elnaim, Bushra. 2013. "Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future" *Information and Knowledge Management*,

Elsayed, Amany M. 2014. "Outsourcing Digitization Projects in Saudi Arabia: An Overview of Current Practices." *Library Collections, Acquisitions & Technical Services* 38 (1-2): 37-46.

Envisioning an Ict Led Approach to the National Transformation Program for the Kingdom of Saudi Arabia. 2016. http://www.idcntpreport.com/.

Fareed, Aisha. 2017. "Saudi Facilities Sustained Nearly 1,000 Cyber Attacks in 2016." *ArabNews*. http://www.arabnews.com/node/1061151/saudi-arabia.

Fenz, Stefan, Johannes Heurix, Thomas Neubauer, and Fabian Pechstein. 2014. "Current Challenges in Information Security Risk Management." *Information Management & Computer Security* 22 (5): 410.

Flick, Uwe. 2004. "Triangulation in Qualitative Research." *A Companion to Qualitative Research* 3: 178-183.

Florah, Oluoch. 2017. "The Effect of Clarity of Roles and Responsibilities of the Board on the Performance of Public Technical Vocational and Entreprenuership Training (Tvet) Institutions in Nyanza Region, Kenya."

Florea, Radu, and Ramona Florea. 2016. "Internal Audit and Risk Management. Iso 31000 and Erm Approaches." *Economy Transdisciplinarity Cognition* 19 (1): 72.

Flores, Waldo, Egil Antonsen, and Mathias Ekstedt. 2014. "Information Security Knowledge Sharing In organizations: Investigating the Effect of Behavioral Information Security Governance And National Culture." *Computers & Security* 43: 90-110. doi:10.1016/j.cose.2014.03.004.

Fomin, Vladislav, H. Vries, and Yves Barlette. 2008. "Iso/Iec 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption." *EUROMOT 2008 Conference, Nice, France*.

Fonseca-Herrera, Omar A., Alix E. Rojas, and Hector Florez. "A model of an information security management system based on NTC-ISO/IEC 27001 standard." *IAENG Int. J. Comput. Sci 48*, no. 2 (2021): 213-222.

Fredrik, Karlsson , Åström Joachim, and Karlsson Martin. 2015. "Information Security Culture State-of-the-Art Review between 2000 and 2013." *Information and Computer Security* 23 (3): 246-285. doi:10.1108/ICS-05-2014-0033.

Gal-Or, Esther, and Anindya Ghose. 2005. "The Economic Incentives for Sharing Security Information." *Information Systems Research* 16 (2): 186-208.

Galletta, Anne. 2013. *Mastering the Semistructured Interview and Beyond: From Research Design to Analysis and Publication* 18. New York, NY: NYU Press.

García-Porras, C., S. Huamani-Pastor, and J. Armas-Aguirre. 2018. "Information Security Risk Management Model for Peruvian Smes." *2018 IEEE Sciences and Humanities International Research Conference (SHIRCON)*, doi:10.1109/SHIRCON.2018.8592994.

Geronimo, Adelle. 2019. "Saudi Arabia Cybersecurity Market to Reach $5.5 Billion in Four Years." Tahawul Tech. https://www.tahawultech.com/industry/technology/saudi-arabia-cybersecurity-market-to-reach-5-5-billion-in-four-years/.

Gibbon, Gavin. 2019. "Middle East Data Breaches Cost $6m Each: New Report." Arabian Business. https://www.arabianbusiness.com/technology/431560-middle-east-data-breaches-cost-6m-each-says-new-report.

Glaspie, Henry, and Waldemar Karwowski. 2018. "Human Factors in Information Security Culture: A Literature Review." In *Advances in Human Factors in Cybersecurity*, 269-280.

The Global Competitiveness Report 2019. 2019. Geneva. https://www.weforum.org/reports/the-global-competitiveness-report-2017-2018.

Goel, Rajni, Anupam Kumar, and James Haddow. "PRISM: a strategic decision framework for cybersecurity risk assessment." *Information & Computer Security* 28, no. 4 (2020): 591-625.

Golafshani, Nahid. 2003. "Understanding Reliability and Validity in Qualitative Research." *The Qualitative Report* 8 (4): 597-606.

Govender, Sunthoshan, Elmarie Kritzinger, and Marianne Lock. 2016. "The Influence of National Culture on Information Security Culture." *2016 IST-Africa Week Conference*: IEEE. doi:10.1109/ISTAFRICA.2016.7530607.

Groll, Elias. 2017. "Cyberattack Targets Safety System at Saudi Aramco." Foreign Policy. https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/.

Guest, Greg, Emily Namey, and Kevin McKenna. 2017. "How Many Focus Groups Are Enough? Building an Evidence Base for Nonprobability Sample Sizes." *Field Methods* 29 (1): 3-22. doi:10.1177/1525822x16639015.

Gur, Natty. 2019. "The Impact of Unclear Responsibilities and Expectations on People and Work." Galaxiez. https://galaxiez.com/2019/07/15/the-impact-of-unclear-responsibilities-and-expectations-on-people-and-work/.

Haber, Morey, and Brad Hibbert. 2018. "Risk Management Frameworks." In *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations*, 241-247. Berkeley, CA: Apress.

Hain, Sebastian. 2011. "Risk Perception and Risk Management in the Middle East Market: Theory and Practice of Multinational Enterprises in Saudi Arabia." *Journal of Risk Research* 14 (7): 819-835.

Hakmeh, Joyce. 2017. *Cybercrime and the Digital Economy in the Gcc Countries*. London, UK: Chatham House.

Hallstensen, Christoffer, Einar Snekkenes, and Gaute Wangen. 2017. "A Framework for Estimating Information Security Risk Assessment Method Completeness." *International Journal of Information Security*. doi:10.1007/s10207-017-0382-0.

Hamilton, Sarah. 2020. How Automated Risk Assessment Is Changing Risk Management. https://www.360factors.com/blog/automated-risk-assessment/.

Harvey-Jordan, Stephanie, and Sarah Long. 2001. "The Process and the Pitfalls of Semistructured Interviews." *Community Practitioner* 74 (6): 219.

Hassan, Rashid. 2021. "Middle East Faced Wave of Cybersecurity Threats since Start of Pandemic." Arab News. https://www.arabnews.com/node/1953826/middle-east.

Hathaway, Melissa, Francesca Spidalieri, and Fahad Alsowailm. 2017. *Kingdom of Saudi Arabia Cyber Readiness at a Glance*. http://www.potomacinstitute.org/150-cyber-

readiness-index/cyber-readiness-translations/2430-kingdom-of-saudi-arabia-cyber-readiness-at-a-glance?jus1=3.

Hennink, Monique, Bonnie Kaiser, and Mary Weber. 2019. "What Influences Saturation? Estimating Sample Sizes in Focus Group Research." *Qualitative Health Research* 29 (10): 1483-1496. doi:10.1177/1049732318821692.

Henshel, Diane, Char Sample, Mariana Cains, and Blaine Hoffman. 2016. "Integrating Cultural Factors into Human Factors Framework and Ontology for Cyber Attackers." In *Advances in Human Factors in Cybersecurity*, 123-137. Berlin, Germany: Springer.

Hofstede, Geert. 1980. "Culture and Organizations." *International Studies of Management & Organization* 10 (4): 15-41.

Hofstede, Geert. 2011. "Dimensionalizing Cultures: The Hofstede Model in Context." *Online Readings in Psychology and Culture* 2 (1): 8.

What About Saudi Arabia? 2019. Hofstede Insights. https://www.hofstede-insights.com/country/saudi-arabia/

Hofstede, Geert, Gert Hofstede, and Michael Minkov. 2005. *Cultures and Organizations: Software of the Mind* 2. Princeton, NJ: Citeseer.

Höne, Karin, and Jan Eloff. 2002. "What Makes an Effective Information Security Policy?" *Network Security* 2002 (6): 14-16. https://doi.org/10.1016/S1353-4858(02)06011-7.

Hossain, Dewan. 2011. "Qualitative Research Process." *Postmodern Openings* (07): 143-156.

ICS2. 2019. *Strategies for Building and Growing Strong Cybersecurity Teams, Cybersecurity Workforce Study*.

Idris, Abdallah. 2007. "Cultural Barriers to Improved Organizational Performance in Saudi Arabia." *SAM Advanced Management Journal* 72 (2): 36.

Internet User Penetration in Saudi Arabia. 2021. https://www.statista.com/statistics/484930/internet-user-reach-saudi-arabia/.

Internet World Stats. 2019. https://www.internetworldstats.com/middle.htm#sa.

Iqbal, Zaheema , and Muhmmad Khan. 2019. "Saudi Women in Cybersecurity Narrowing the Gap of Human Capital Crisis." *Global Foundation for Cyber Studies and Research*.

ISO31000:2018. 2018. *Risk Management - Guidelines*. International Standards Organization

The Iso Survey 2019. 2020. Geneva. https://www.iso.org/the-iso-survey.html.

ISO/IEC27000. 2018. *Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*. International Standards Organization. http://www.saiglobal.com.dbgw.lis.curtin.edu.au/PDFTemp/osu-2015-07-29/9485459998/ISO-IEC_27000-2014_3.PDF.

ISO/IEC27005. 2018. *Information Technology — Security Techniques — Information Security Risk Management*. International Standards Organization

ISO/TR31004. 2013. *Risk Management — Guidance for the Implementation of ISO 31000*. International Standards Organization

Jacob, Stacy, and Paige Furgerson. 2012. "Writing Interview Protocols and Conducting Interviews: Tips for Students New to the Field of Qualitative Research." *The Qualitative Report* 17 (42): 1-10.

Jakábová, Martina, Jana Urdziková, and Emília Mironovová. 2013. "Standardization of Information Security Management System: Iso/Iec 27001: 2005, Itil®, Cobit®." *International Journal of Recent Contributions from Engineering, Science & IT (iJES)* 1 (2): 11-18.

Javaid, Muhammad, and Mian Iqbal. 2017. "A Comprehensive People, Process and Technology (Ppt) Application Model for Information Systems (Is) Risk Management in Small/Medium Enterprises (Sme)." *2017 International Conference on Communication Technologies (ComTech)*, doi:10.1109/COMTECH.2017.8065754.

Johnson, Dave. 2019. "What Is Linkedin? A Beginner's Guide to the Popular Professional Networking and Career Development Site." Business Insider. https://www.businessinsider.com/what-is-linkedin/?r=AU&IR=T.

Jones, Seth, Newlee, Newlee, Harrington, Nicholas. 2019. *Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.-Iranian Escalation*. Washington. https://www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation.

Jung, Gregory 2013. "How the Malicious Insider Affects Cybersecurity within Companies." PhD Disseration, M.S. Utica College, Ann Arbor. http://search.proquest.com/docview/1475266008?accountid=10382

Kannan, Ganapathy, and V. Sivasubramanian. 2016. "Transforming Risk Culture through Organizational Culture Leveraging Cobit 5 for Risk." *COBIT Focus*: 1-7.

Kaplan, Bonnie, and Joseph A Maxwell. 2005. "Qualitative Research Methods for Evaluating Computer Information Systems." In *Evaluating the Organizational Impact of Healthcare Information Systems*, 30-55. Berlin, Germany: Springer.

Kaptein, Muel. 2011. "Understanding Unethical Behavior by Unraveling Ethical Culture." *Human Relations* 64 (6): 843-869.

Karyda, Maria, Evangelos Kiountouzis, and Spyros Kokolakis. 2005. "Information Systems Security Policies: A Contextual Perspective." *Computers & Security* 24 (3): 246-260.

Khanduri, Aditya. 2020. "People, Process, Technology: The Ppt Framework, Explained." https://www.plutora.com/blog/people-process-technology-ppt-framework-explained.

Khidzir, N., A. Mohamed, and N. Arshad. 2010a. "Information Security Risk Management: An Empirical Study on the Difficulties and Practices in Ict Outsourcing" *2010 Second International Conference on Network Applications, Protocols and Services*, doi:10.1109/NETAPPS.2010.49.

Khidzir, N. Z., A. Mohamed, and N. H. Arshad. 2010b. "Information Security Risk Factors: Critical Threats Vulnerabilities in Ict Outsourcing" *2010 International Conference on Information Retrieval & Knowledge Management (CAMP)*, doi:10.1109/INFRKM.2010.5466918.

Kincheloe, Joe, and Peter McLaren. 2011. "Rethinking Critical Theory and Qualitative Research." In *Key Works in Critical Pedagogy*, 285-326. Leiden, The Netherlands: Brill Sense.

Knowles, William, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, and Kevin Jones. 2015. "A Survey of Cyber Security Management in Industrial Control Systems." *International Journal of Critical Infrastructure Protection* 9: 52-80. https://doi.org/10.1016/j.ijcip.2015.02.002.

Krauss, Clifford, and Nicole Perlroth. 2018. "A Cyber Attack in Saudi Arabia Failed to Cause Carnage, but the Next Attempt Could Be Deadly." *Independent*. https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html.

Krippendorff, Klaus. 2018. *Content Analysis: An Introduction to Its Methodology*. Thousand Oaks, CA: Sage Publications.

Krueger, Richard, and Mary Casey. 2015. *Focus Groups: A Practical Guide for Applied Research* 5th ed. Thousand Oaks: Sage Publications.

Krueger, Thomas. 2018. Finding Better Research Participants and Avoiding Fraud: A Framework for Recruiting Qualified Participants for Qualitative and Quantitative Research. https://uxplanet.org/finding-better-research-participants-and-avoiding-fraud-eef18bb82f98.

Kruger, H. A., L. Drevin, S. Flowerday, and T. Steyn. 2011. "An Assessment of the Role of Cultural Factors in Information Security Awareness" *2011 Information Security for South Africa*, doi:10.1109/ISSA.2011.6027505.

Kshetri, Nir. 2016. "Cybersecurity in Gulf Cooperation Council Economies." In *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, 183-194. Berlin, Germany: Springer International Publishing.

Kuzminykh, Ievgeniia, Bogdan Ghita, Volodymyr Sokolov, and Taimur Bakhshi. 2021 "Information Security Risk Assessment." MDPI, no. 3 (2021): 602-617.

Kwon, Juhee, and Eric Johnson. 2011. "An Organizational Learning Perspective on Proactive Vs. Reactive Investment in Information Security." *WEIS*: Citeseer.

Labuschagne, WG Bornman L. 2004. "A Comparative Framework for Evaluating Information Security Risk Management Methods." *Standard Bank Academy for Information Technology, Rand Afrikaans University*.

Lakshmanan, Ravie. 2020. "Iranian Apt Group Targets Governments in Kuwait and Saudi Arabia." The Hacker News. https://thehackernews.com/2020/05/iran-hackers-kuwait.html?m=1.

Leavy, Patricia. 2017. *Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches*. New York, NY: Guilford Publications.

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. 2019. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior." *International Journal of Information Management* 45: 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Lim, Joo S, Shanton Chang, Sean Maynard, and Atif Ahmad. 2009. "Exploring the Relationship between Organizational Culture and Information Security Culture" *Australian Information Security Management Conference*.

Limited, Information Security Forum. 2011. *The Standard of Good Practice for Information Security 2011*.

Lin, Hsien-Cheng. 2014. "An Investigation of the Effects of Cultural Differences on Physicians' Perceptions of Information Technology Acceptance as They Relate to Knowledge Management Systems." *Computers in Human Behavior* 38: 368-380. https://doi.org/10.1016/j.chb.2014.05.001.

Liu, Xinping, and Lei Zheng. 2018. "Cross-Departmental Collaboration in One-Stop Service Center for Smart Governance in China: Factors, Strategies and Effectiveness." *Government Information Quarterly* 35 (4): S54-S60.

Looso, S., M. Goeken, and W Johannsen. 2011. "Comparison and Integration of It Governance Frameworks to Support It Management." In *Quality Management for It Services: Perspectives on Business and Process Performance*, 90-107. Hershey, PA: IGI Global.

Ma, Qingxiong, Allen C. Johnston, and J. Michael Pearson. 2008. "Information Security Management Objectives and Practices: A Parsimonious Framework." *Information Management & Computer Security* 16 (3): 251-270. doi:10.1108/09685220810893207.

Maghrabi, Rozan Omar, and Prashant C Palvia. 2012. "The Impact of Information Technology (It) on National Culture: The Case of Saudi Arabia." https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1198&context=icis2012

Mahfuth, A., S. Yussof, A. A. Baker, and N. Ali. 2017. "A Systematic Literature Review: Information Security Culture" *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. doi:10.1109/ICRIIS.2017.8002442.

Malaika, Abdulaziz. 1993. "Management Characteristics and Organisation Context in Saudi Arabia." PhD Thesis, Loughborough University.

Maneerattanasak, Urairat, and Nitaya Wongpinunwatana. 2017. "A Proposed Framework: An Appropriation for Principle and Practice in Information Technology Risk Management" *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, doi:10.1109/ICRIIS.2017.8002513.

Manek, Sheila. 2019. "Saudi Arabia's Top Ict Industry Leaders Gather in Riyadh." IDC Corporate. https://www.idc.com/getdoc.jsp?containerId=prCEMA44854019.

Marathamuthu, M. 2015. "An Enhanced Information Security Framework for Effective Management of Enterprise Information Assets." ProQuest Dissertations Publishing.

Mason, Jennifer. 2017. *Qualitative Researching*. Thousand Oaks, CA: Sage.

Masue, Orest, Idda Swai, and Mackfallen Anasel. 2013. "The Qualitative-Quantitative'disparities' in Social Science Research: What Does Qualitative Comparative Analysis (Qca) Brings in to Bridge the Gap?" *Asian Social Science* 9 (10): 211.

McCumber, John 2004. *Assessing and Managing Security Risk in It Systems*. Boca Raton, FL: Auerbach Publications.

Meijer, Albert. 2009. "Understanding Modern Transparency." *International Review of Administrative Sciences* 75 (2): 255-269.

Menachery, Martin. 2018. In the Middle East, 43.5% of Ics Computers Were Attacked by Malware. The 6th International Industrial Cybersecurity Conference. https://www.refiningandpetrochemicalsme.com/events/23926-in-the-middle-east-435-of-ics-computers-were-attacked-by-malware-in-h1-2018-says-kaspersky-lab-cybersecurity-expert.

Miles, Matthew , Michael Huberman, and Johnny Saldaña. 2014. *Qualitative Data Analysis: A Methods Sourcebook*, 3rd ed. Thousand Oaks, CA: Sage.

Mohammed, Derek , and Shereeza Mohammed. 2017. "Survey of Information Security Risk Management Models." *International Journal of Business, Humanities and Technology* 7 (4). http://www.ijbhtnet.com/journals/Vol_7_No_4_December_2017/3.pdf.

Moon, Jewook, Chanwoo Lee, Sangho Park, Yanghoon Kim, and Hangbae Chang. 2018. "Mathematical Model-Based Security Management Framework for Future Ict Outsourcing Project." *Discrete Applied Mathematics* 241: 67-77. https://doi.org/10.1016/j.dam.2016.03.013.

Moore, Susan. 2021. *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021* STAMFORD. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem.

Moreno, Valter. 2002. "Validity Issues in Phenomenological Research: Bridging Theory and Practice in a Study of It-Driven Radical Organizational Change." *AMCIS 2002 Proceedings*: 241.

Morgan, Steve. 2020. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-will-cost-the-world-16-4-billion-a-day-in-2021/.

Moshashai, Daniel, Andrew Leber, and James Savage. 2020. "Saudi Arabia Plans for Its Economic Future: Vision 2030, the National Transformation Plan and Saudi Fiscal Reform." *British Journal of Middle Eastern Studies* 47 (3): 381-401. doi:10.1080/13530194.2018.1500269.

Myers, Michael. 2009. *Qualitative Research in Business & Management Qualitative Research in Business and Management*. Los Angeles

Myers, Michael, and D. Avison. 2002. *Qualitative Research in Information Systems : A Reader*. London: SAGE.

Myers, Michael , and Michael Newman. 2007. "The Qualitative Interview in Is Research: Examining the Craft." *Information and Organization* 17 (1): 2-26. https://doi.org/10.1016/j.infoandorg.2006.11.001.

Nabi, SyedIrfan, Abdulrahman Mirza, and Khaled Alghathbar. 2010. "Information Assurance in Saudi Organizations – an Empirical Study." In *Security Technology, Disaster Recovery and Business Continuity*, edited by Tai-hoon Kim, Wai-chi Fang, MuhammadKhurram Khan, KirkP Arnett, Heau-jo Kang and Dominik Ślęzak, 18-28. Berlin Heidelberg: Springer.

Naden, Clare 2018. Reducing the Risks of Information Security Breaches with Iso/Iec 27005. International Standards Organization (ISO). https://www.iso.org/news/ref2309.html.

Nasir, Akhyari , Ruzaini Arshah, and Mohd Ab Hamid. 2017. "Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework." In *Proceedings of the 2017 International Conference on Information System and Data Mining*, *Charleston, SC, USA*, 56-60. 3077593: ACM. doi:10.1145/3077584.3077593.

National Information Assurance (IA) Glossary. 2010. https://www.hsdl.org/?abstract&did=7447.

Neale, Bren. 2012. "Qualitative Longitudinal Research: An Introduction to the Timescapes Methods Guides Series." *Economic and Social Research Council*.

Nemati, Hamid. 2010. *Security and Privacy Assurance in Advancing Technologies: New Developments.* Hershey, PA: IGI Global.

Nicastro, Felicia. 2006. "People, Processes, and Technology: A Winning Combination." In *Information Security Management Handbook* 3: 241.

NIST, National Institute of Standards and Technology. 2011. *Nist 800-39 Managing Information Security Risk*.

NIST, National Institute of Standards and Technology. 2018. *Nist 800-37 Risk Management Framework for Information Systems and Organizations*.

O'Connor, H, and Nancy Gibson. 2003. "A Step-by-Step Guide to Qualitative Data Analysis." *Pimatisiwin: A Journal of Aboriginal and Indigenous Community Health* 1: 63-90.

O'Gorman, Brigid; Wueest, Wueest; O'Brien, Dick; Cleary, Gillian. 2019. *Internet Security Threat Report 2019*. Mountain View: Symantec Corporation. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

Okonofua, Henry, Shawon Rahman, and Reni Ivanova. 2019. "An Empirical Examination of the Effects of It Leadership on Information Security Risk Management in USA Organizations." *Proceedings of 34th International Confer* 58: 464-474.

Omar, Samer. 2017. "Cyber Criminals Continue Their Attacks on Saudi Sectors." Riyadh Daily. http://alriyadhdaily.com/article/86f4dc5824044704ae0794b8e0d490ae.

Opec Share of World Crude Oil Reserves. 2019. Organization of the Petroleum Exporting Countries OPEC. https://www.opec.org/opec_web/en/data_graphs/330.htm.

Pa, Noraini , Bokolo Jnr, Rozi Nor, and Masrah Murad. 2015. "Risk Assessment of It Governance: A Systematic Literature Review." *Journal of Theoretical & Applied Information Technology* 71 (2).

Pape, Sebastian, Ludger Goeke, Alejandro Quintanar, and Kristian Beckers. 2020. "Conceptualization of a Cybersecurity Awareness Quiz" *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity*. Berlin, Germany: Springer.

Parsons, Kathryn, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. 2017. "The Human Aspects of Information Security Questionnaire (Hais-Q): Two Further Validation Studies." *Computers & Security* 66: 40-51.

Perlroth, Nicole, and Clifford Krauss. 2018. *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*. New York Times. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html#:~:text=Experts%20Fear%20Another%20Try.,-Read%20in%20app&text=In%20August,%20a%20petrochemical%20company,down%20the%20plant,%20investigators%20believe.

Perthes, Volker. 2018. "Conflict and Realignment in the Middle East." *Survival* 60 (3): 95-104.

Petrescu, Anca, and Nicoleta Sîrbu. 2019. "Information Security Risk Management in the European Union." In *Throughput Accounting in a Hyperconnected World*, 275-292. Hershey, PA: IGI Global.

Philips, Zoe, Karl Claxton, and Stephen Palmer. 2008. "The Half-Life of Truth: What Are Appropriate Time Horizons for Research Decisions?" *Medical Decision Making* 28 (3): 287-299.

Proactive Vs Reactive Task Management. 2020. Improve. http://improveconsulting.biz/proactive-vs-reactive-task-management/.

Prodan, Mircea, Adriana Prodan, and Anca Alecandra Purcarea. 2015. "Three New Dimensions to People, Process, Technology Improvement Model." In *New Contributions in Information Systems and Technologies*, 481-490. Berlin, Germany: Springer.

Quadri, Aman, and Muhammad Khan. 2019. *Cybersecurity Challenges of the Kingdom of Saudi Arabia*. https://www.gfcyber.org/cybersecurity-challenges-of-the-ksa-past-present-and-future/

Raggad, Bel G. 2010. *Information Security Management: Concepts and Practice*. Boca Raton, FL: CRC Press.

Razi, Muhammad , and Haider Madani. 2013. "An Analysis of Attributes That Impact Adoption of Audit Software: An Empirical Study in Saudi Arabia." *International Journal of Accounting & Information Management* 21 (2): 170-188.

Recker, Jan Christof. 2008. "Understanding Process Modelling Grammar Continuance: A Study of the Consequences of Representational Capabilities." PhD Dissertation, Queensland University of Technology. https://eprints.qut.edu.au/16656/.

Renukappa, Suresh, Subashini Suresh, Saeed Al Nabt, Redouane Sarrakh, and Khaled Algahtani. 2020. "An Ism Approach to Evaluate Critical Success Factors for Knowledge Management Strategies in the Kingdom of Saudi Arabia." In *Harnessing Knowledge, Innovation and Competence in Engineering of Mission Critical Systems*. London: IntechOpen.

Reza, Alavi, Islam Shareeful, Jahankhani Hamid, and Al-Nemrat Ameer. 2013. "Analyzing Human Factors for an Effective Information Security Management System." *International Journal of Secure Software Engineering (IJSSE)* 1 (4): 50-74. doi:10.4018/jsse.2013010104.

Riivari, Elina, Anna-Maija Lämsä, Johanna Kujala, and Erika Heiskanen. 2012. "The Ethical Culture of Organisations and Organisational Innovativeness." *European Journal of Innovation Management*. https://jyx.jyu.fi/handle/123456789/40633

The Risk It Framework. 2009.

Rizvi, Raza , Nick Roudev, and Benjamin Lyons. 2019. *Cybersecurity in the Kingdom of Saudi Arabia – an Overview and Update.* http://www.elexica.com/en/legal-topics/information-communication-and-technology/120219-cybersecurity-in-the-kingdom-of-saudi-arabia.

Rouse, Margaret. 2016. What Is Linkedin? https://whatis.techtarget.com/definition/LinkedIn.

Runeson, Per, Martin Höst, Austen Rainer, and Björn Regnell. 2012. "Case Study Research in Software Engineering." In *Guidelines and Examples*. Wiley Online Library.

Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. "Information Security Conscious Care Behaviour Formation in Organizations." *Computers & Security* 53: 65-78. https://doi.org/10.1016/j.cose.2015.05.012.

Safa, Nader Sohrabi, and Rossouw Von Solms. 2016. "An Information Security Knowledge Sharing Model in Organizations." *Computers in Human Behavior* 57: 442-451. http://dx.doi.org/10.1016/j.chb.2015.12.037.

Sahibudin, S., M. Sharifi, and M. Ayat. 2008. "Combining Itil, Cobit and Iso/Iec 27002 in Order to Design a Comprehensive It Framework in Organizations" *2008 Second Asia International Conference on Modelling & Simulation (AMS)*. doi:10.1109/AMS.2008.145.

Saira, Muzafar, and Nz Jhanjhi. 2020. "Success Stories of Ict Implementation in Saudi Arabia." In *Employing Recent Technologies for Improved Digital Governance*, edited by Ponnusamy Vasaki, Rafique Khalid and Zaman Noor, 151-163. Hershey, PA: IGI Global.

Saldaña, Johnny. 2015. *The Coding Manual for Qualitative Researchers*. London: Sage.

Saleh, Mohamed S., and Abdulkader Alfantookh. 2011. "A New Comprehensive Framework for Enterprise Information Security Risk Management." *Applied Computing and Informatics* 9 (2): 107-118. http://dx.doi.org/10.1016/j.aci.2011.05.002.

Sanusi, Fasilat and Satirenjit Johl 2021. "Assessment of Top Management Commitment and Support on IS Risk Management Implementation in the Business Organization." *Risk Management*, 275.

Saudi Arabia - Information and Communications Technology. 2018. https://www.export.gov/article?id=Saudi-Arabia-information-communications-technology.

Saudi Arabia Gdp - Gross Domestic Product. 2021. https://countryeconomy.com/gdp/saudi-arabia.

Saudi Arabia Information Technology Report - Q1 2015. 2015. 1643768942. London. ProQuest Central; ProQuest SciTech Collection. http://search.proquest.com/docview/1643768942?accountid=10382

"Saudi Arabia Oil Facilities Ablaze after Drone Strikes." 2019. BBC World Service. https://www.bbc.com/news/world-middle-east-49699429.

Saudi Arabia: Gross Domestic Product. 2021. https://www.statista.com/statistics/268059/gross-domestic-product-of-saudi-arabia/.

Sawada. 2018. *Global Threat Intelligence Report 2018*. http://go.nttict.com/2018-Global-Threat-Intelligence-Report.html

Saxena, Stuti. 2018. "National Open Data Frames across Japan, the Netherlands and Saudi Arabia: Role of Culture." *Foresight* 20 (1): 123-134. doi:10.1108/FS-07-2017-0038.

Schmidt, Mark B., Allen C. Johnston, Kirk P. Arnett, Jim Q. Chen, and Suichen Li. 2008. "A Cross-Cultural Comparison of Us and Chinese Computer Security Awareness." *Journal of Global Information Management (JGIM)* 16 (2): 91-103.

Schwartz, Arthur. 2015. "The 5 Most Common Unethical Behaviors in the Workplace." Philadelphia Business Journal. https://www.bizjournals.com/philadelphia/blog/guest-comment/2015/01/most-common-unethical-behaviors-in-the.html.

Setiawan, H., F. A. Putra, and A. R. Pradana. 2017. "Design of Information Security Risk Management Using Iso/Iec 27005 and Nist Sp 800-30 Revision 1: A Case Study at Communication Data Applications of Xyz Institute" *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, doi:10.1109/ICITSI.2017.8267952.

Shamseddine, Reem. 2017. "Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces." *Reuters*. https://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

Shanthamurthy, Dharshan. 2011. "Leveraging Iso 27005 Standard's Risk Assessment Capabilities." Computer Weekly. https://www.computerweekly.com/tip/Leveraging-ISO-27005-standards-risk-assessment-capabilities.

Shojaie, Bahareh. 2018. "Implementation of Information Security Management Systems Based on the Isoiec 27001 Standard in Different Cultures." https://www.semanticscholar.org/paper/Implementation-of-information-security-management-Shojaie/61516f95dd81512b37d8d7410222cec3727bde1c

Singer, Peter. 1998. "Ethics." In *Encyclopedia Britannica*. https://www.britannica.com/topic/Encyclopaedia-Britannica-English-language-reference-work/Fifteenth-edition

Singh, Umesh Kumar, and Chanchala Joshi. 2017. "Information Security Risk Management Framework for University Computing Environment." *IJ Network Security* 19 (5): 742-751.

Smithson, Janet. 2000. "Using and Analysing Focus Groups: Limitations and Possibilities." *International journal of social research methodology* 3 (2): 103-119.

Soomro, Zahoor Ahmed, Mahmood Hussain Shah, and Javed Ahmed. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36 (2): 215-225. http://dx.doi.org/10.1016/j.ijinfomgt.2015.11.009.

Spong, Rebecca. 2018. "Cyber Attacks a 'Real Threat' to Gulf Business." Arab News. https://www.arabnews.com/node/1274021/business-economy.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. 2002. "Risk Management Guide for Information Technology Systems." National Institute of Standards and Technology. Accessed 29 April 2015, csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Straub, D. W., K. D. Loch, and C. E. Hill. 2001. "Transfer of Information Technology to the Arab World: A Test of Cultural Influence Modeling." *Journal of Global Information Management* 9 (4): 6-28. http://search.proquest.com/docview/57512332?accountid=10382

Strauss, Anselm. 1987. *Qualitative Analysis for Social Scientists*. Cambridge, UK: Cambridge University Press.

"Study: 60% of Saudi Institutions Hit by Virus Attacks, Malware." 2018. *Arab News*. https://www.arabnews.com/node/1169846/saudi-arabia.

Susanto, Heru, and Mohammad Almunawar. 2018. *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard*. Cambridge, MA: Apple Academic Press.

Szmit, Maciej. 2015. "Security Management and Risk Management Approach in Cybersecurity and Information Security Management." https://www.researchgate.net/profile/Maciej-Szmit/publication/277008998_Szmit_2015_Zylina/links/555dd67408ae6f4dcc8cf7d2/Szmit-2015-Zylina.pdf?origin=publication_list

Talib, Amir , Fahad Alomary, Hanan Alwadi, and Rawan Albusayli. 2018. "Ontology-Based Cyber Security Policy Implementation in Saudi Arabia." *Journal of Information Security* 9 (4): 315-333.

Tang, Mincong, Meng'gang Li, and Tao Zhang. 2016. "The Impacts of Organizational Culture on Information Security Culture: A Case Study." *Information Technology and Management* 17 (2): 179-186. doi:10.1007/s10799-015-0252-2.

Taylor, Richard. 2015. "Potential Problems with Information Security Risk Assessments." *Information Security Journal: A Global Perspective* 24 (4-6): 177-184.

Telecommunication Indicators in the Kingdom of Saudi Arabia by the End of Q3-2017. 2018. Ministry of Communications and Information Technology. http://www.mcit.gov.sa/en/standard-indicators/99050.

Telekomunikasi, Jl. 2014. "Analysis of Iso27001 Implementation for Enterprises and Smes in Indonesia" *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security*, *Kuala Lumpur*.

Theoharidou, Marianthi, Spyros Kokolakis, Maria Karyda, and Evangelos Kiountouzis. 2015. "The Insider Threat to Information Systems and the Effectiveness of Iso17799." *Computers & Security* 24 (6): 472-484. https://doi.org/10.1016/j.cose.2005.05.002.

Thurmond, Veronica. 2001. "The Point of Triangulation." *Journal of Nursing Scholarship* 33 (3): 253-8. http://dx.doi.org/10.1111/j.1547-5069.2001.00253.x.

Top 100 Listed Companies in the Arab World 2018. 2018. https://www.forbesmiddleeast.com/list/top-100-listed-companies-in-the-arab-world-2018.

The Total Population in 2019. 2019. https://www.stats.gov.sa/en/indicators/1.

Trajkovski, Jasmina, and Ljupcho Antovski. 2013. "Risk Management Framework That Meets the Implementation Challenges in It-Centric Micro and Small Companies." *International Journal of Human Capital and Information Technology Professionals* 4 (2): 16-26.

Trajkovski, Jasmina, and Ljupcho Antovski. 2017a. "Risk Management Framework for It-Centric Micro and Small Companies with Model for Risk Assessment." In *University-Industry Links: Coproducing Knowledge, Innovation & Growth*.

Trajkovski, Jasmina, and Ljupčo Antovski. 2017b. "Perception of Risk Management and Its Impact on Proposed Risk Management Framework for It-Centric Micro, Small and Medium Enterprices." *Mechanical Engineering Scientific Journal*: 53.

Tsohou, Aggeliki , Maria Karyda, Spyros Kokolakis, and Evangelos Kiountouzis. 2006. "Formulating Information Systems Risk Management Strategies through Cultural Theory." *Information Management & Computer Security* 14 (3): 198-217. doi:10.1108/09685220610670378.

Tsohou, Aggeliki, Maria Karyda, and Spyros Kokolakis. 2015. "Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs." *Computers & Security* 52: 128-141. https://doi.org/10.1016/j.cose.2015.04.006.

Tsohou, Aggeliki, Spyros Kokolakis, Costas Lambrinoudakis, and Stefanos Gritzalis. 2009. "Information Systems Security Management: A Review and a Classification of the Iso Standards" *International Conference on e-Democracy*. Berlin, Germany: Springer.

Übelacker, Sven. 2013. "Security-Aware Organisational Cultures as a Starting Point for Mitigating Socio-Technical Risks." https://www.researchgate.net/profile/Sven-Uebelacker/publication/271135142_Security-Aware_Organisational_Cultures_as_a_Starting_Point_for_Mitigating_Socio-Technical_Risks/links/54be81890cf218d4a16a7a84/Security-Aware-Organisational-Cultures-as-a-Starting-Point-for-Mitigating-Socio-Technical-Risks.pdf

Upadhyay, Shailendra , Mark Driver, Christian Canales, Ruggero Contu, and Lawrence Pingree. 2021. *Forecast Analysis: Information Security and Risk Management, Worldwide*. Stamford. https://www.gartner.com/en/documents/4004647/forecast-analysis-information-security-and-risk-management-worldwide.

Vaccaro, Antonino, and Dalia Patiño Echeverri. 2010. "Corporate Transparency and Green Management." *Journal of business ethics* 95 (3): 487-506.

Van Niekerk, JF, and Rossouw Von Solms. 2010. "Information Security Culture: A Management Perspective." *Computers & Security* 29 (4): 476-486.

Veiga, Adéle, and Nico Martins. 2017. "Defining and Identifying Dominant Information Security Cultures and Subcultures." *Computers & Security* 70 (Supplement C): 72-94. doi: https://doi.org/10.1016/j.cose.2017.05.002.

Veltsos, Christophe. 2018. Lessons from the Iso/Iec 27005:2018 Security Risk Management Guidelines. Security Intelligence. https://securityintelligence.com/lessons-from-the-iso-iec-270052018-security-risk-management-guidelines/.

Von Solms, Basie, and Rossouw Von Solms. 2004. "The 10 Deadly Sins of Information Security Management." *Computers & Security* 23 (5): 371-376. doi: http://dx.doi.org/10.1016/j.cose.2004.05.002.

Wahlgren, Gunnar, and Stewart Kowalski. 2018. "It Security Risk Management Model for Handling It-Related Security Incidents: The Need for a New Escalation Approach." In *Security and Privacy Management, Techniques, and Protocols*, 129-151. Hershey, PA: IGI Global.

Walsham, Geoff. 1995. "The Emergence of Interpretivism in Is Research." *Information Systems Research* 6 (4): 376-394.

Wangen, G. 2017. "Information Security Risk Assessment: A Method Comparison." *Computer* 50 (4): 52-61. doi:10.1109/MC.2017.107.

Wangen, Gaute, and Einar Snekkenes. 2013. "A Taxonomy of Challenges in Information Security Risk Management" *Proceeding of Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013*. Oslo: Akademika Forlag.

Watkins, Steve G. 2010. *Information Security Risk Management for Iso27001/Iso27002*, 2nd ed. Ely, UK: IT Governance Ltd.

Webb, Jeb. 2013. "Towards an Intelligence-Driven Information Security Risk Management Process for Organisations" *24th Australasian Conference on Information Systems (ACIS)*: RMIT University.

Webb, Jeb, Atif Ahmad, Sean B. Maynard, and Graeme Shanks. 2014. "A Situation Awareness Model for Information Security Risk Management." *Computers & Security* 44 (0): 1-15. http://dx.doi.org/10.1016/j.cose.2014.04.005.

Weller, Susan , Ben Vickers, H Russell Bernard, Alyssa Blackburn, Stephen Borgatti, Clarence Gravlee, and Jeffrey Johnson. 2018. "Open-Ended Interview Questions and Saturation." *PloS one* 13 (6): e0198606.

What Is 'Iso'? 2019. https://www.bsigroup.com/en-AU/About-BSI/FAQs/What-is-ISO/.

Wheeler, Evan. 2011. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Amsterdam, The Netherlands: Elsevier.

Wild, Jason. 2018. "Six Most Common Security Frameworks Explained." https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/.

Wipulanusat, Warit, Jirapon Sunkpho, and Rodney Stewart. 2021. "Effect of Cross-Departmental Collaboration on Performance: Evidence from the Federal Highway Administration." *Sustainability* 13 (11): 6024.

World Economic Situation and Prospects 2017. 2017. New York, NY. https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/2017wesp_full_en.pdf.

"The World Factbook: Saudi Arabia." 2021. The Central Intelligence Agency. https://www.cia.gov/the-world-factbook/countries/saudi-arabia/.

Wright, Bianca 2019. "Saudi Arabia's Cybersecurity Concerns Increase as Threats Evolve." IDG Communications. https://www.cio.com/article/3445225/saudi-arabias-cybersecurity-concerns-increase-as-threats-evolve.html.

Wright, Craig. 2008. *The It Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments*. Amsterdam, The Netherlands: Elsevier.

Xie, F., Y. Peng, W. Zhao, D. Chen, X. Wang, and X. Huo. 2012. "A Risk Management Framework for Cloud Computing" *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, doi:10.1109/CCIS.2012.6664451.

Yaokumah, Winfred. 2013. "Evaluating the Effectiveness of Information Security Governance Practices in Developing Nations: A Case of Ghana." Ph.D. Capella University. Ann Arbor, MI. http://search.proquest.com/docview/1346677782?accountid=10382

Yin, Robert. 2003. *Case Study Research : Design and Methods*. 3rd ed. Thousand Oaks, Calif.: Thousand Oaks, CA: Sage Publications.

Zahrani, Yousef. 2018. "Culture of Patient Safety in Public Hospitals in the Asir Region of Saudi Arabia as Perceived by Healthcare Providers and Managers : A Mixed Method Study." PhD Thesis: School of Population and Global Health The University of Western Australia. Perth

APPENDIX 1 Participants Information

Human Research Ethics Office

Curtin University

Participant Information and Consent Forms

PARTICIPANT INFORMATION STATEMENT

HREC Project Number:	***RDBS-19-16***
Project Title:	**Information Security Risk Management *(ISRM) Model for Saudi Arabian Organisations***
Principal Investigator:	***Dr Paul Alexander*** ***Associate Professor***
Student researcher:	*Naser Alshareef*
Version Number:	*2.1*
Version Date:	*29 March 2016*

What is the Project About?

Existing Information Security Risk Management (ISRM) frameworks provide a common approach. ISRM has much in common with other security approaches however, it is very general and doesn't consider regional and cultural factors. For example, difficulties in identifying an organization's assets as well as team members' lack of experience are considered major factors of information security risk management, but these lack effectiveness in the Saudi Arabian context.

The overall research objectives are to develop an ISRM framework, based on existing ISRM frameworks, to operate in the context of Saudi Arabian organisations, as well as to revealing critical factors of an adopted and developed ISRM framework for Saudi Arabian context.
The main research objectives are:
1. To determine the key success and failure factors of effective ISRM implementation.
2. To determine the critical factors necessary for developing ISRM framework applicable for Saudi Arabian enterprise organisations.
3. To develop ISRM framework based on existing ISRM frameworks that works in the Saudi Arabian context.

This research will propose a new conceptual Information Security Risk Management (ISRM) framework more appropriate for Saudi Arabian organisations. This new framework will be based on current ISRM frameworks and will develop an applicable and effective Information Security Risk Management design theory for Saudi Arabia.

The significance of this framework lies in its understanding of the Information Security Risk Management issues considering cultural and social complications in Saudi Arabia because there is evidence of compromise of ISRM as it is practiced in Western Countries. There is little evidence of ISRM research in a Saudi Arabian context and development of this framework will add to the knowledge base for further research and practice, and in an extension of knowledge

in ISRM in Saudi Arabia, and due its cultural, commercial and economic similarities to other countries in the Gulf, serve as a base for comparative studies between western countries and Middle Eastern countries.

All Participants are adults with IT security experience. Participants will be 15-20 interviewees from different organisation from Saudi Arabia. Also, 2-3 focus groups with a total of 6 participants for each.

Who is doing the Research?

The project is being conducted by Naser Alshareef and supervised by Dr. Paul Alexander.

Why am I being asked to take part and what will I have to do?

Participants will be IT security specialists who could provide valuable information.
The study will take place at a mutually convenient location.
We will ask you questions about information security risk management ISRM such as whether or not your organization implements ISRM and why.
Interview should take 30-45 minutes with each participant. It's open ended questions and might take a bit longer if participants welling to give more details.
Face to face or conference call semi structure interviews. Conference calls could be via Skype, Facetime or regular phone call. Interviews will be voice recorded where the researcher will provide the interviews transcripts after completing all interviews.
There will be no cost to you for taking part in this research and you will not be paid for taking part.
We will make a digital audio recording so we can concentrate on what you have to say and not distract ourselves with taking notes. After the interview/focus group we will make a full written copy of the recording.

Are there any benefits' to being in the research project?

There may be no direct benefit to you form participating in this research.
We hope the results of this research will allow us to:
Develop ISRM Framework for Saudi Organisations to Improve IT Security Management

Are there any risks, side-effects, discomforts or inconveniences from being in the research project?

There are no foreseeable risks from this research project.
Apart from giving up our time, we do not expect that there will be any risks or inconveniences associated with taking part in this study.

Who will have access to my information?

The information collected in this research will be non-identifiable (anonymous). This means that we do not need to collect individual names or information is anonymous and will not include a code number or name. No one, not even the research team will be able to identify your information. Any information we collect and use during this research will be treated as confidential. The following people will have access to the information we collect in this research: the research team and the Curtin University Ethics Committee
Electronic data will be password-protected and hard copy data (including audio tapes) will be in locked storage at Curtin University.

The information we collect in this study will be kept under secure conditions at Curtin University for 7 years after the research has ended and then it will be destroyed.
You have the right to access, and request correction of, your information in accordance with relevant privacy laws.
The results of this research may be presented at conferences or published in professional journals. You will not be identified in any results that are published or presented.
Whilst all care will be taken to maintain privacy and confidentiality of any information shared at a focus group or group discussion, you should be aware that you may feel embarrassed or upset if one of the group members repeats things said in a confidential group meeting.

Will you tell me the results of the research?

We are not able to send you any results from this research as we do not collect any personal information to be able to contact you.

Do I have to take part in the research project?

Taking part in a research project is voluntary. It is your choice to take part or not. You do not have to agree if you do not want to. If you decide to take part and then change your mind, that is okay, you can withdraw from the project. You do not have to give us a reason; just tell us that you want to stop. Please let us know you want to stop so we can make sure you are aware of any thing that needs to be done so you can withdraw safely. If you chose not to take part or start and then stop the study, it will not affect your relationship with the University, staff or colleagues. If you chose to leave the study we will use any information collected unless you tell us not to.

What happens next and who can I contact about the research?

- Researcher: Naser Alshareef — Supervisor: Dr Paul Alexander
- n.alshareef@student.curtin.edu.au — @cbs.curtin.edu.au

Phone# +96600000000 — Phone# +61 8 9266

If you decide to take part in this research we will ask you to sign the consent form. By signing it is telling us that you understand what you have read and what has been discussed. Signing the consent indicates that you agree to be in the research project. Please take your time and ask any questions you have before you decide what to do. You will be given a copy of this information and the consent form to keep.

Curtin University Human Research Ethics Committee (HREC) has approved this study. Should you wish to discuss the study with someone not directly involved, in particular, any matters concerning the conduct of the study or your rights as a participant, or you wish to make a confidential complaint, you may contact the Ethics Officer on +61 (08) 9266 9223 or the Manager, Research Integrity on +61 (08) 9266 7093 or email hrec@curtin.edu.au.

APPENDIX 2 Consent Form

Curtin University

CONSENT FORM

HREC Project Number:	***RDBS-19-16***
Project Title:	***Information Security Risk Management (ISRM) Model for Saudi Arabian Organisations***
Principal Investigator:	***Dr Paul Alexander*** ***Associate Professor***
Student researcher:	*Naser Alshareef*
Version Number:	*2.1*
Version Date:	*29 March 2016*

- I have read, the information statement version listed above and I understand its contents.
- I believe I understand the purpose, extent and possible risks of my involvement in this project.
- I voluntarily consent to take part in this research project.
- I consent to being audio recorded.
- I have had an opportunity to ask questions and I am satisfied with the answers I have received.
- I understand that this project has been approved by Curtin University Human Research Ethics Committee and will be carried out in line with the National Statement on Ethical Conduct in Human Research (2007) – updated March 2014.
- I understand I will receive a copy of this Information Statement and Consent Form.

Participant Name	
Participant Signature	
Date	

Declaration by researcher: I have supplied an Information Letter and Consent Form to the participant who has signed above, and believe that they understand the purpose, extent and possible risks of their involvement in this project.

Researcher Name	
Researcher Signature	
Date	

Note: All parties signing the Consent Form must date their own signature.

APPENDIX 3 Invitation Letter

Curtin University

School of Information Systems

Information security risk management model (ISRM) for Saudi Organisations

This is Naser Alshareef, Saudi PhD candidate in the school of information systems at Curtin University in Western Australia. I am conducting research in information security risk management in Saudi organisations. My research aims to identify factors that influence ISRM in Saudi organisations.

This email is to request your permission to participate an online interview. The interview duration is expected to be from 30-50 minutes. If you would like to participate, you will provided with a link via email to access the WebEx online meeting room. Your participation is anonymous and your identity will not be published or disclosed.

I will keep you updated on my results of this study and at the end of my degree I will share with you the ISRM model.

If you would like to participate, please contact me at the email or number listed below to discuss your participation and email you the "participant information sheet" to understand more about my study, and later we can start off the interview.

Your help and cooperation is highly appreciated

Regards,

Naser Alshareef

Perth, Western Australia

APPENDIX 4 Semistructured Interview

Introducing the researcher to participants:

I'm Naser Alshareef, a PhD student at Curtin University. My PhD research is to improve information security risk management framework in Saudi organizations. This interview is to gather data from you to facilitate my research findings. Data collected will follow confidential and your personal information including your name and organization will be anonymous. You are free to skip questions and withdraw the interview at any time at your convenience. The interview will be voice recorded for transcription matters only. If you wish not to, please let me know.

The interview Questions

1. I would like to start with your experience, how long have you been working for this organization and what is your job title?
2. Please describe your organization working field?
3. What is your organization size?
4. Who is responsible for IT security in your company "Job Title"?
5. To whom does your information security organisation's head report to?
6. In your opinion, what is Information Security Risk Management ISRM?
7. Does your organisation comply with any international ISRM framework or best practices? If yes, what is it?
8. Is your organisation ISRM certified?
9. Why did you comply with this standard or framework among others?
10. Do you have a corporate level information security policy? If yes, how often do you review and update?
11. How effective is the ISRM framework or methodology you adopt for your organization security?
12. What are the factors that could hinder the compliance of an ISRM framework or methodology in your organization?
13. Do you evaluate your Information Security risk using audit reviews?
14. Which security measures has your organisation implemented?
15. What do you consider to be your greatest security risk for your organization?

16. Does Saudi Arabia's culture had any effect on the implementation of ISRM? In terms of policy compliance or privacy perspectives?
17. Do you measure employees information security awareness level? How?
18. Does your organisation provide employee training to raise information security awareness? How often?
19. Do you share ISRM knowledge with other Saudi organizations?
20. Does your organization outsource any of information security areas? If yes, what are they?
21. How does your organisation ensure an adequate and appropriate level of information security over third parties?
22. What are factors that could improve the effectiveness of the ISRM standard to best fit your organization?

APPENDIX 5 Focus Group

Introducing the researcher to participants:

I'm Naser Alshareef, a PhD student at Curtin University. My PhD research is to improve information security risk management framework in Saudi organizations. This focus group interview is to gather data from you to facilitate my research findings. Data collected will follow confidential and your personal information including your name and organization will be anonymous. You are free to skip questions and withdraw the interview at any time at your convenience. The interview will be voice recorded for transcription matters only. If you wish not to, please let me know.

The focus group questions

1. Are you involved in any information security risk management activities in your organisation?
2. Do you believe that it would be more effective to enhance international ISRM standards to best fit Saudi organisations? How?
3. If you could add or remove any factors from the new ISRM model provided, what would it be? Why these specific factors are essential?
4. Of all the things we've talked about, what is the most important factor that you may reconsider in your organisation's ISRM activities in the future?
5. How likely do you think will the new ISRM model assist the ISRM compliance of Saudi organisations?

APPENDIX 6 Arabic Version of the Proposed ISRM Model