UNIVERSITY OF KWAZULU-NATAL

Managing IT Outsourcing Risks: The case of large organisations in South Africa

By

Abdulbaqi Eyitayo Badru

215065196

A dissertation submitted in fulfilment of the requirements for the degree of Master of Commerce (Information Systems and Technology)

School of Management, IT and Governance

College of Law and Management Studies

Supervisor: Mr. Nurudeen Ajayi

2017

DECLARATION

I, Abdulbaqi Eyitayo Badru, declare that

(i) The research reported in this dissertation, except where otherwise indicated, is my original research.

(ii) This dissertation has not been submitted for any degree or examination at any other university.

(iii) This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other Researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;
b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.

(vi) This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation and in the References sections.

Signature:

Date: 23/12/2017

ACKNOWLEDGEMENTS

I give all thanks and adoration to Almighty Allah for sparing my life the duration of my study. My utmost gratitude goes to my parents, Mr Yunus Olasunkanmi Badru and Alhaja Mrs Lutifat Abiodun Badru, and my uncle, Dr Oyerinde Ashamu for believing in me and granting me the opportunities to reach this height.

I extend my sincere gratitude to my supervisor, Mr Nurudeen Abimbola Ajayi, for his brotherly guidance and support he bestowed on me. I am honoured and privileged to have worked under your guidance. Thank you to everyone who has contributed to the success of this study in one way or another. To Mr Michael Ferendinos, for his support during the data collection phase of this study. To the staff of the UKZN Teaching and Learning Office (UTLO): Dr Rubby Dhunpath, Ms Corlia Ogle, Mrs Silindile Mchunu, Mrs Christinah Mulaudzi, Professor Michael Samuel, and in especially, Dr. Reshma Subbaye for her constructive critique and knowledge she showered on me. To ISACA, for the tuition fee scholarship awarded to me to cover the second year of this study. To my supportive friends Ms. Nsofwa Kangwa, Ms Lukhele Mammie, Ms Nondumiso Cele, Mr. Marco Bozza, Ms Zainab Sanusi and Mr Victor Faniran, thank you.

Lastly, I would like to acknowledge the support and encouragement from my siblings, Dr Zulaykha Badru, Ms Rihanat Badru and Ms Mastura Badru; my nieces, Aishat and Asiyah and my nephew, Abdullah; and, my dearest, Barrister Nafisat Lasisi for staying strong for me. To all my friends and colleagues, you are all amazing fellows, thank you for always being positive towards me.

ABSTRACT

Information technology (IT) is significant to achieving business objectives. Despite the significance of IT to the business, organisations are outsourcing the whole, or part thereof, of their IT department to reduce cost and focus on the core of their business. The outsourcing of IT, however, comes together with risks such as vendor lock-in, loss of control and information breaches that could lead to IT outsourcing (ITO) failure. If these risks are not properly identified and managed, organisations will remain vulnerable. While studies have been conducted on ITO and risk management, very few have conducted exploratory research to address how to manage the risks of ITO.

Hence, using a qualitative approach, this study explored how large organisations manage the common risks of ITO. These risks are the operational risk, business continuity risk, data privacy risk and compliance risk of the IT Service Provider (ITSP). The study further explored the impact of these risks on large organisations and the mitigating controls organisations can have in place to reduce their impact and likelihood of occurrence. Interviews, which were recorded, was conducted with 12 experts from two large organisations in South Africa. The recorded interviews were transcribed, coded using NVivo software and analysed using thematic analysis. The main themes of this study were governance, develop ITO risk profile, ITSP audit, risk treatment, and assurance. Findings show that organisations need to constitute a Risk Management Committee with a substantial level of experience in the management of risks and ITO. This is to ensure the effective identification, assessment and treatment of ITO risks. Furthermore, the constituted Risk Committee must conduct verification exercises to identify the inherent risks of ITO. They must also conduct maturity assessment and business impact analysis (BIA) in assessing the probability of occurrence and impact of ITO risks. The Committee must establish technical and administrative controls in mitigating the risks of ITO. The findings further show that organisations must integrate risk governance and assurance polices in their ITO risk management strategy to continuously monitor residual risks and identify potentially new risks. A governance Framework for IT Service Provider Risk Management (ITSPRM) that may serve as a guide in the effective management of ITO risks was also developed and presented.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BA	British Airways
BGFRS	Board of Governance of the Federal Reserve System
BIA	Business Impact Analysis
CGEIT	Certified in the Governance of Enterprise IT
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
COBIT	Control Objectives for Information and Related Technology
CRISC	Certified in Risk and Information Systems Control
CRM	Customer Relations Management
CV	Curriculum Vitae
DBMS	Database Management Systems
DEC	Digital Equipment Corporation
E2EE	End-to-End Encryption
ERP	Enterprise Resource Planning
HIPAA	Health Insurance Portability and Accountability Act
IBM	International Business Machine
IOSCO	International Organization of Securities Commissions
IRM	Institute of Risk Management
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITO	IT Outsourcing
ITSP	IT service provider
ITSPRM	IT Service Provider Risk Management
NTFS	New Technology File System
OS	Operating System
PCI DSS	Payment Card Industry Data Security Standard
RACM	Risk and Control Matrix
RFP	Request for Proposal
SIM	Security Inventory Management
SLA	Service Level Agreement
SOC	Service Organisation Control
SWOT	Strength weakness opportunity and threat
TCE	Transactional Cost Economics
UKZN	University of KwaZulu-Natal
USA	United States America

CHAPTER 1: INTRODUCTION

1.1 Introduction

Today, information technology (IT) serves as the backbone to most organisation's sustenance. This is because it serves as an enabler of corporate strategies and a catalyst for change to the business models of various organisations (Kumar, 2016). IT is a combination of hardware and software used to facilitate the collection, storage, and dissemination of data, information and knowledge (Bourgeois, 2014). Different IT solutions such as Database Management systems (DBMS), Customer Relations Management (CRM) Systems, and Enterprise Resource Planning (ERP) systems (Rana, 2013) are being developed to enable or support business processes. These solutions are also supporting globalisation as well as access to real-time information that allows for real-time decision-making (Globalization101, 2012).

The integration of IT into different sectors and organisational units has led to the creation of integrated solutions that facilitate the restructuring of business processes. For example, the integration of IT into the manufacturing sector has helped to restructure manufacturing processes into becoming lean and efficient (Rana, 2013). The integration of IT into supply chains has changed the operational dynamics of how supply chains (Eamonn *et al.*, 2015). Supply chains are now more efficient because of the use of the internet to facilitate supply chain processes. Consequently, supply chains have evolved from the physical exchange of information between artisans and consumers to a virtual chain of suppliers, manufacturers, and consumers now referred to as the value web (as shown in Figure 1-1) (Eamonn *et al.*, 2015).

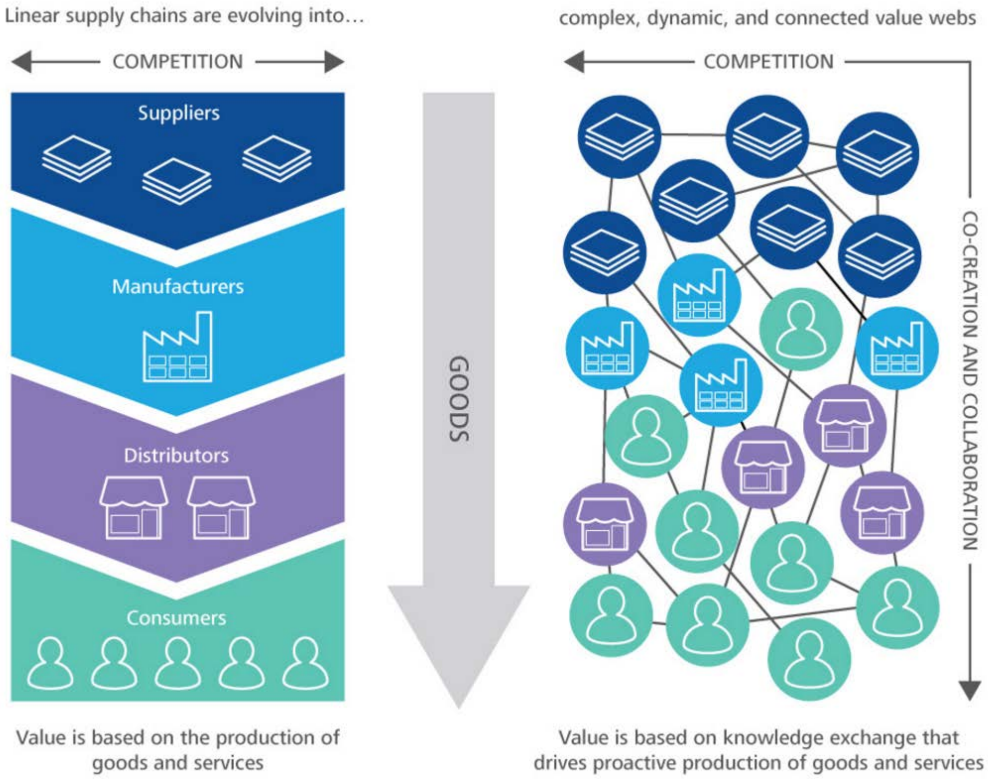

Linear supply chains are evolving into…
COMPETITION
Suppliers
Manufacturers
Distributors
Consumers
Value is based on the production of goods and services
GOODS
complex, dynamic, and connected value webs
COMPETITION
CO-CREATION AND COLLABORATION
Value is based on knowledge exchange that drives proactive production of goods and services

Figure 1-1: Supply Chain evolution (Eamonn *et al.*, 2015)

The use of IT has brought significant benefits to organisations. However, the maintenance of IT requires substantial cost, expertise, time, and resources. The challenge of acquiring these requirements has led to some organisations outsourcing the whole or part of their IT functions (Davis *et al.*, 2004). The outsourcing of IT promises opportunities such as reduction in cost, focus on core competence, and use of external expertise (Ravi, 2010). However, IT outsourcing (ITO) comes with potential risks such as information privacy risks, political risks, operational risks and environmental risks (Deloitte, 2014b). These risks could lead to vendor lock-in, unsatisfactory service quality, loss of intellectual properties and extra cost (Samantra *et al.*, 2014; Thanapol *et al.*, 2013).

Risks are causing futile and unsatisfactory ITO engagements, which is depriving organisations of attaining the benefits or objectives of outsourcing IT (Vasant *et al.*, 2017). Vasant *et al.* (2017) and Deloitte (2012) reported that the operational risk, business continuity risk, information privacy risk and regulatory compliance risk of IT service provider (ITSP) are the common risks faced by the outsourcing organisation. The possible impact of these risks on organisations is necessitating the development of ITSP risk management framework to help manage these risks effectively (Deloitte, 2014b).

1.2 Background of the study

In the past, the structure of organisations was such that organisational units and their respective processes are managed and controlled in-house (Ritchie, 2015). However, the management of organisations soon got to observe that the bloated strategy of managing all business activities in-house was hindering their respective organisations from competing globally (Handfield, 2008; Ritchie, 2015). This observation led to the search for a more flexible and cost-effective way of managing organisational processes and resources (Handfield, 2008). The outcome of the search resulted in the business concept known as "outsourcing" (Davis *et al.*, 2004; Handfield, 2008). Outsourcing is the contracting out of an organisation's processes and resources to a third-party organisation, who is capable of delivering the function more efficiently and perhaps at a cheaper rate (Gilley *et al.*, 2000). Over the years, outsourcing has evolved from the contracting out of ancillary functions, to support functions and now, core business functions (Handfield, 2008).

The outsourcing of IT started in the 20th Century (Gonzales *et al.*, 2004). Eastman Kodak's arrangement with International Business Machine (IBM), Digital Equipment Corporation (DEC) and Businessland in 1989 is considered as the first ITO arrangement (Dibbern *et al.*, 2004; Loh *et al.*, 1992; Ritchie, 2015). This arrangement is marked as a significant event referred to as "the Kodak effect" because of the influence Kodak's move to outsource IT had on other large and small organisations such as J.P. Morgan, Xerox Corporation, DuPont who also entered into ITO contracts worth billions of dollars (DiRomualdo *et al.*, 1998; Loh *et al.*, 1992).

According to Statista (2015), the ITO market has been fluctuating in recent times as a result of discouraging outcomes of unsuccessful engagements, which is mostly caused by the lack of risk and project management approaches. However, industry analysts have projected an exponential increase in the rate at which organisations would outsource IT. Gartner (2014) forecasted that the ITO global market would reach $288 billion in 2013 with expected growth of 5.2% in 2014. Deloitte (2016), through a global outsourcing survey report, projected a growth of 5% from 2014 to 2016 and indicated that participants showed the willingness to continue outsourcing IT. These projections were based on the rapid and continuous adoption of technology.

1.3 Research problem

ITO is becoming a common practice in most organisations (Ritchie, 2015). Whilst some organisations are benefiting from ITO, other organisations are struggling with achieving their ITO objectives (Deloitte, 2016). In a survey (on global outsourcing and insourcing) administered by Deloitte Consulting LLP in 2012, 48% of ITO contracts were reported as unsuccessful (failed half-way) and 24% were unsatisfactory due to concerns over service quality (Deloitte, 2014a). ITO risks such as the risks of the ITSP have been identified as major causes of unsuccessful ITO contracts (Deloitte, 2012; Vasant *et al.*, 2017). The negative impact of these risks has resulted in the failure of top organisations such as Kodak (Mitchell, 2014).

More recently, the chaos (stranded passengers) at the British Airways (BA) terminal (Heathrow and Gatwick) was reported to have been caused by a glitch in their global IT system that is outsourced (Jonathan, 2017). Jonathan (2017) confirmed that BA had suffered six major IT failures within twelve months of outsourcing IT, which has affected their productivity and reputation. Most daunting cases such as that of BA have been associated with the incompetence of the outsourcing organisation to effectively manage the risks of the ITSP (MacInnis, 2003; Paul, 2004). The need to manage these risks effectively is growing urgently because of their negative impact on organisations.

Reports from the "South African sourcing pulse survey" (KPMG, 2012), the IT sourcing strategy indicated in organisations' annual reports such as Nampak (2012) Integrated Annual Report 2012, and studies by Johnston *et al.* (2009) and Pengilly (2007) showed the substantial involvement of South African organisations in ITO. The significant involvement of South Africa organisations in ITO, the risks involved in ITO and the potential negative impacts of these risks on organisations is necessitating the continuous research on risks, and risk management practices of ITO to propose effective ways of managing risks involved in outsourcing IT. This study explores how large organisations in South Africa manage ITSP's risk, and proposes an IT Service Provider Risk Management (ITSPRM) Framework to assist organisations to manage some of the risks of ITO effectively.

1.4 Research questions

The four common risks of ITO mentioned in this section are operational risk, business continuity risk, information privacy risk and compliance risk of ITSP.

The research questions are as follows:

1. How do large organisations identify IT Service Provider's risks?
2. How are large organisations assessing IT Service Provider's risks?
    a. What are the impacts of the four common risks of ITO on large organisations?
3. How are large organisations treating IT Service Provider's risks?
    a. What are the mitigating controls large organisations in South Africa have in place to manage IT Service Provider's risks?

1.5 Research objectives

The main objective of this study is:

- To propose an IT service provider risk management framework to help organisations effectively manage IT Service Provider's risks.

To achieve the main objective of this study, the below were the primary objectives of this study:

1. To explore how large organisations identify IT Service Provider's risks.
2. To understand how large organisations assess IT Service Provider's risks.
    a. To highlight the impacts of the four common IT Service Providers' risks on large organisations.
3. To understand how large organisations treat IT Service Provider's risks.
    a. To explore the mitigating controls large organisations, have in place to manage IT Service Provider's risks and highlight the controls to manage the four common risks of ITO.

1.6 Justification

ITO brings substantial benefits to organisations; however, some organisations are failing to benefit from ITO due to the risks involved. The willingness of organisations to continue engaging in ITO, the high rate of unsatisfactory ITO engagement and the potential negative impact of risks on organisations is necessitating the continuous research on ITO risks. The increased chances of organisations being engulfed by the consequences of

ITSP’s risks is requiring the development of an ITSPRM framework to help effectively manage ITSP’s risk. (Deloitte, 2014b; Tompkins *et al.*, 2005).

1.7 Scope of the study

This study focused on the operational risk, business continuity risk, information privacy risk and compliance risk of ITSP in investigating how large organisations within South Africa identify, assess and treat ITSP’s risks. This is because these risks are the common and severe risks of ITO (Deloitte, 2012; Vasant *et al.*, 2017). The context of the study is on two large organisations (telecommunication and retail) in South Africa that have been engaging in ITO for more than four years.

1.8 Significance of the study

Many studies were found to have explored the risk management practices of ITO contract management, vendor management and project management. However, limited studies were found to have explored the risk management of ITSP, which has been identified as the common and main risks of ITO (Deloitte, 2012; Vasant *et al.*, 2017). This study contributes to the literature on the risk management methods, tools and strategies organisations could adopt in identifying, assessing and treating ITSP’s risks. The study proposes an ITSPRM framework that could be adopted by organisations to effectively manage ITSP’s risks.

1.9 Research methodology

Research methodology is a systematic approach towards solving a specific research problem or achieving specific research objectives (Rajasekar *et al.*, 2013). It comprises of the science of examining how research is conducted, which involves the procedures and techniques a researcher has adopted in investigating a research problem or achieving specific research objectives.

The qualitative research approach was adopted in this study because it allowed for an in-depth investigation of the risk management practices large organisations have in place to manage ITSP’s risks (Patton, 1990). The exploratory case study design was used to acquire applicable data to answer the research questions. Two large organisations (Telecommunication and Retail) within South Africa that have been outsourcing part of their IT functions for over four years were used as the study site. The purposive and snowball sampling technique were used to choose the sample from the study site. The samples were staff from the study site who are responsible for decision-making and management of ITO contracts. Some of their responsibilities include decision-making analyst, contract management, risk management, vendor relationship management, compliance management, governance management and IT auditing.

Using the purposive sampling, participants were chosen based on their expertise and experience in managing ITO contracts or projects in their organisation. These participants included executive managers such as directors, IT risk and governance managers, IT managers, and other management and operational staff such as project managers, risk practitioners and auditors who have a stake in the decision-making or management of ITO functions or contracts in their organisations. In addition, snowball sampling technique was used to get access to participants. Snowball sampling, also referred to as chain sampling, is when research participants enrol potential participants of similar characteristics for a study (Bhattacherjee, 2012). In this study, the researcher requested participants to recommend other colleagues who have the same or similar job responsibility in the organisation.

According to Patton (1990), there are no specified rules for measuring the sample size in a qualitative research. He further explained that the qualitative sample size depended on the dimension (depth or breadth) the researcher seeks to inquire. Considering the research method (qualitative methodology) for this study, data was collected from twelve respondents. An interview was used as the data collection instrument for this study because the study is qualitative. In-depth interviews were conducted with respondents because it aligns with the exploratory design of the study. This type of interview allowed for the exploration of the phenomenon by allowing the researcher to ask and probe responses from the participants (Marshall *et al.*, 2014). Interviews were analysed using NVivo software and the type of analysis used was thematic analysis. The thematic analysis is a qualitative analytic/analysis method used by researchers to gain insight and generate knowledge from a data set when a qualitative research method is used (Braun *et al.*, 2006).

1.10 Limitations of the study

The main limitation of this study was the accessibility and availability of participants. This was due to the position and level of potential participants (as key decision makers) in their respective organisation. This limitation was managed by establishing a good rapport with the secretary/personal assistant of potential participants who monitor their schedule. In addition, interview sessions were arranged at participants' convenience, with reminders sent to them a day before the interview and on the day of the interview, to re-confirm their availability. Another limitation encountered during this study is the limited access to journal articles on ITSP risk management practices. To overcome this limitation, the literature on risks and risk management practices in other fields such as finance and safety were considered, and organisational reports and policies were also helpful in this regard.

1.11 Layout of dissertation

This dissertation comprises of six chapters. These chapters are ordered in the sequence the research was carried out. A brief of the chapters is presented below.

Chapter one is the introductory chapter of this study. It presents a brief background and evolution of ITO. The chapter also presents the research problem, motivation for this study, research questions and objectives, and a brief on the methodology used in achieving the research objectives.

Chapter two presents the review of the literature on ITO. Studies on outsourcing, ITO, risks involve in ITO, reasons why organisations engage in ITO, challenges and success factors of ITO were reviewed in this chapter.

Chapter three presents the review of the literature on risks, ITO risks and risk management practices. Studies with similar objectives to this study were also reviewed in this chapter.

Chapter four is an elaboration on the research methodology highlighted in chapter one. This chapter presents the research methods, approaches and data collection techniques used in achieving the objective of this study.

Chapter five presents the findings and discussion of this study in relation to achieving the objectives of this study.

Chapter six presents the summary, conclusion, and recommendation of this study. Future research areas were also presented.

1.12 Conclusion

This chapter presents an overview of this study. An introduction to the study phenomena “IT outsourcing” was established. It was established that ITO is becoming the common practice of organisations as they lean towards reducing cost and using external expertise to achieve internal objectives. ITO however, comes with risks, which could lead to unsatisfactory/futile engagement. The operational risk, business continuity risk, information privacy risk and compliance risk of ITSP have been established as the common risks of ITO. It is therefore apparent that organisations develop an ITSPRM framework to ensure that the risks associated with their ITSP are identified, assessed and treated effectively. The next chapter presents the review of the literature on ITO types, motivations, challenges, management and practices.

CHAPTER 2: LITERATURE REVIEW – INFORMATION TECHNOLOGY OUTSOURCING

2.1 Introduction

In the previous chapter, an overview of this study was presented. This chapter presents an overview of outsourcing and a review of the literature on ITO. In the literature, different aspects of ITO have been explored that have contributed to the development of ITO practices. This chapter presents the key areas on ITO. The chapter also covers the evolution of ITO in relation to the understanding of the background and risks involved in ITO practices. See Figure 2-1 for a diagrammatic representation of this chapter.

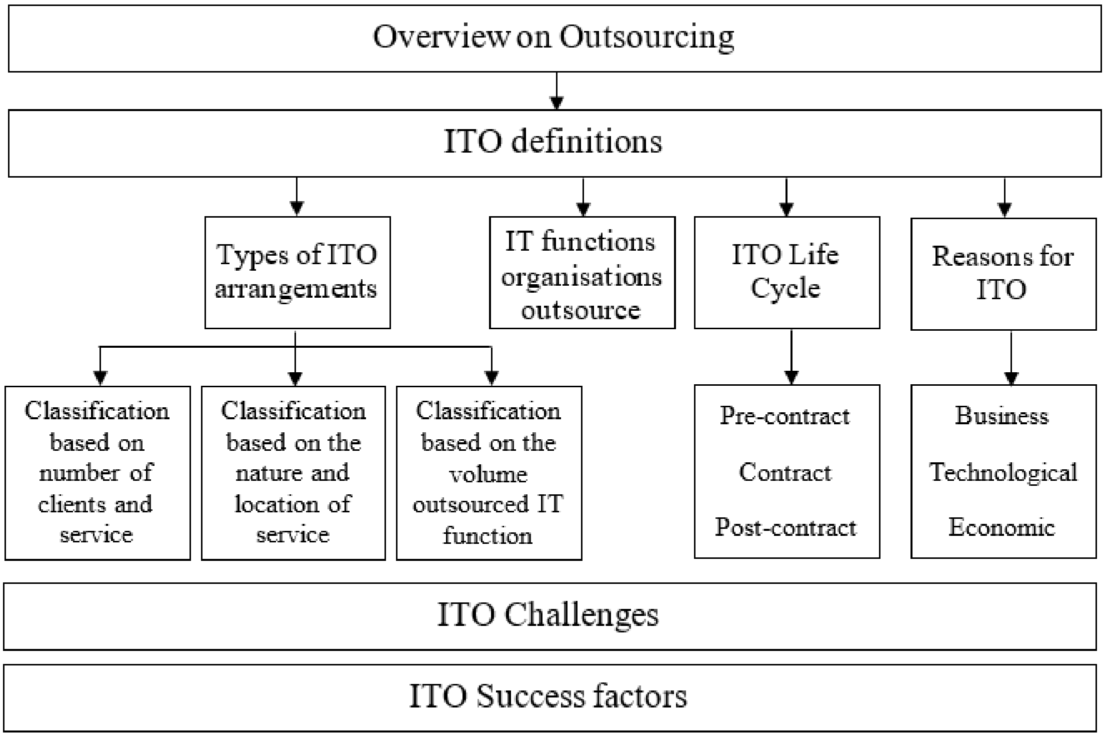

Overview on Outsourcing
ITO definitions
Types of ITO arrangements
IT functions organisations outsource
ITO Life Cycle
Reasons for ITO
Classification based on number of clients and service
Classification based on the nature and location of service
Classification based on the volume outsourced IT function
Pre-contract
Contract
Post-contract
Business
Technological
Economic
ITO Challenges
ITO Success factors

Figure 2-1: Structure of chapter two

2.2 Overview of outsourcing

Outsourcing is a management buzzword that emanated in the 19th Century (Hätönen *et al.*, 2009). Since then, it has evolved and has become a household strategy in today's organisational settings. Outsourcing is a management strategy that allows organisations to delegate business activities that were previously done in-house to a third-party expert (Demaria, 2011). It could also be defined as the contracting out of business operations or tasks to an external specialist who has the capability to do the task better, cheaper and faster (Tayauova, 2012). In essence, outsourcing is the handing over of business activities to a service provider (either domestic or offshore), so as to allow organisations to utilise external resources to achieve internal business objectives (Iqbal *et al.*, 2013).

Before the advent of outsourcing, business units used to be vertically integrated (Kakabadse *et al.*, 2002; Lonsdale *et al.*, 2000), which means that activities in every link of an organisation's value chain were managed internally (Hätönen *et al.*, 2009). Today, reasons such as diversification, globalisation and business flexibility are requiring that business functions/units are contracted out to service providers (Handfield, 2008; Leavy, 2001). IBM is an example of an organisation that has adopted outsourcing in order to become flexible and competitive. Previously, IBM used to manufacture computers that come with their own operating system (OS) and peripherals. However, today, IBM computers are made up of units manufactured by other organisations. While IBM now focuses on IT service delivery (Hätönen *et al.*, 2009). Organisations outsource functions such as logistics, human resources, customer services, information technology and manufacturing, with the intent of leveraging production to achieve economy of scale and at the same time cutting the cost of production (Hätönen *et al.*, 2009; Iqbal *et al.*, 2013).

Globally, small, medium and large-scale organisations in both private and public sectors are adopting outsourcing for reasons such as reducing the cost of labour and production (Davis *et al.*, 2004; Gonzalez *et al.*, 2009). A study by Gonzalez *et al.* (2010), however, showed that economic reasons are no more the key motivation for outsourcing. Organisations are now outsourcing for strategic reasons such as improving business efficiency (Iqbal *et al.*, 2013), focusing on core competencies (Johnston *et al.*, 2009), accessing global talent and market (Iqbal *et al.*, 2013) and avoiding certain costs such as taxes (Statista, 2015). Outsourcing has increased the opportunity for organisations to tap into an external resource base, add value to processes and mitigate business risks (Statista, 2015). Outsourcing comes with benefits, however, it presents challenges such as complexity and risks to organisations (Gottschalk *et al.*, 2005; Lonsdale *et al.*, 1997).

Outsourcing is complex because of the series of interwoven processes involved in its implementation and management (Vaxevanou *et al.*, 2015). The complex nature of outsourcing gives rise to various managerial and administrative dilemmas (Vaxevanou *et al.*, 2015). Executives are being faced with uncertainty with regards to sourcing strategy decisions, which includes whether or not to outsource; what business functions to outsource; what outsourcing strategy to adopt; and selecting the appropriate service provider (Iqbal *et al.*, 2013). This state of uncertainty has resulted in the development of various outsourcing theories such as transactional cost economics (TCE), core competency theory, relational theory, resource-based theory, and agency theory (Vaxevanou *et al.*, 2015). Researchers have adopted these theories in exploring and investigating issues pertaining to outsourcing. The results of their studies have contributed to the development of good practices and standards for managing outsourcing relationships. Aside from the complexity of outsourcing, organisations are dealing with risks. Some of these risks include but are not limited to security breaches, loss of control, hidden cost and loss of expertise and knowledge (Jimmy Gandhi *et al.*, 2012; Lonsdale *et al.*, 1997).

Despite the complications and risks involved in outsourcing, organisations are still contracting out business functions and units to service providers, most especially IT (Davis *et al.*, 2004; Ramanujan *et al.*, 2006). This is because IT is expensive, evolving rapidly, cross-functional and a support function to other business units (Meyer *et al.*, 2005; Prado, 2011).

2.3 Information Technology Outsourcing definition

According to Samantra *et al.* (2014, p. 4010), ITO is the "utilisation of third-party capabilities to successfully deliver IT-enabled business processes, application services and infrastructure solutions for a cost-effective business outcome". Thus, it is the allocation of in-house IT functions to a service provider (Bradley *et al.*, 2012). It involves arranging with an ITSP who is expected to deliver IT as a service to the organisation, at most a cheaper price. This arrangement is usually bound by a contract detailing the agreement between the outsourcing organisation and the service provider (De Sá-Soares *et al.*, 2014)

2.4 Types of Information Technology Outsourcing arrangements

There are various classifications of ITO arrangements. These classifications are based on different criteria such as the number of clients and service providers in the outsourcing deal, nature and location of the service provider; and volume of the outsourced function (Meyer *et al.*, 2005). Each of these arrangements has their pros and cons, which are highlighted in the sections below.

2.4.1 Classification based on the number of clients and service providers

There are different types of ITO arrangements that are based on the number of clients and service providers involved in the outsourcing engagement. Gallivan *et al.* (1999) identified four types of these arrangements, which are simple relationship; multi-vendors relationship; co-sourcing relationship, and complex relationship. See Figure 2-2 for illustration.

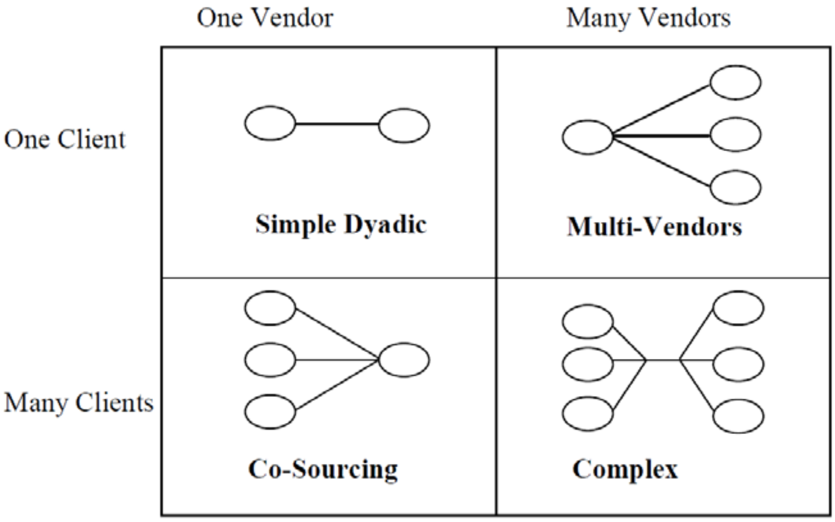


Figure 2-2: Types of ITO - based on number of clients and vendors (Gallivan *et al.*, 1999)

2.4.1.1 Simple relationship (one client, one service provider)

Simple relationship is also referred to as one to one or a dyadic relationship (Gallivan *et al.*, 1999; Oshri, 2010). In this type of outsourcing arrangement, one client relies on the expertise and capabilities of one ITSP to satisfy its outsourcing needs (Oshri, 2010). A simple relationship is a straightforward outsourcing arrangement because of the less complex process involved in the management and monitoring of the outsourcing contract. However, clients involved in a simple relationship are vulnerable to risks such as vendor lock-in and lack of transparency (Gellings, 2007). Previously, a simple relationship was considered the most popular type of outsourcing arrangement because there were few service providers that were capable to deliver as expected. However, in recent times, the presence of many other service providers now gives organisations the option to experiment with other forms of outsourcing such as multi-vendor relationships.

2.4.1.2 Multi-vendors relationship (one client, many service providers)

Multi-vendors relationship is also referred to as one to many relationship (Gallivan *et al.*, 1999). In this type of ITO arrangement, one client relies on the capabilities and expertise of more than one ITSP to satisfy its outsourcing needs. The multi-vendors relationship is a complex and costly type of outsourcing arrangement because of the processes involved in the management and monitoring of multiple service providers (Lee *et al.*, 2009). The processes involved in managing and monitoring of multi-vendors relationship is usually complicated due to interconnected activities, which brings about client coordination burden to the ITSPs (Gallivan *et al.*, 1999). However, engaging in a multi-vendors relationship also comes with some benefits such as gaining access to a wider scope of talent and mitigating the risk of vendor lock-in (Eileen, 2014). A typical example of a multi-vendors relationship is the outsourcing arrangement between Kodak and BusinessLand, IBM and DEC (Applegate *et al.*, 1991).

2.4.1.3 Co-sourcing relationships (many clients, one service provider)

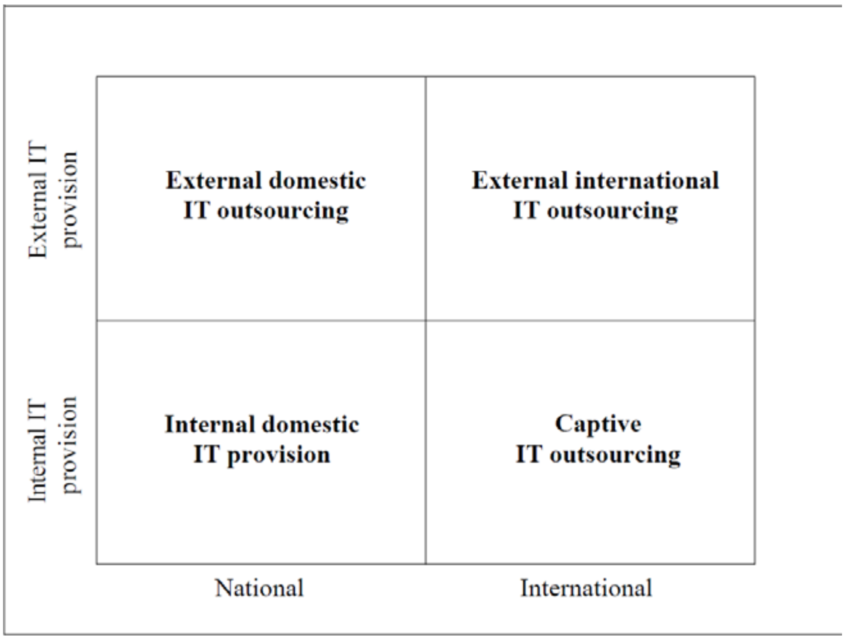
The co-sourcing relationships is a many to one type of outsourcing arrangement (Gallivan *et al.*, 1999). In this type of ITO arrangement, more than one independent client collaborate to contract one ITSP to satisfy their collective needs (Chakrabarty, 2006; Willcocks *et al.*, 1999). This type of outsourcing arrangement is peculiar with organisations in the same industry who seek similar IT solutions (such as systems development and infrastructure) for their business transactions (Gallivan *et al.*, 1999). According to Gallivan *et al.* (1999), organisations adopt the co-sourcing relationship as a strategy to leverage on benefits such as risk sharing and reduction, buyer economies of scale, and increased bargaining power. In most cases, organisations consider the co-sourcing relationships when the IT system or solution involved is operational and less strategic to the business (Choudhury, 1997). A typical example of a co-sourcing relationships is an alliance formed by seven independent hospitals in Australia, who jointly contracted one systems integrator to develop hospital management software with the aim of saving time and money (Sharma *et al.*, 1996).

2.4.1.4 Complex relationships (many clients, many service providers)

Complex relationships is also referred to as a many-to-many type of outsourcing arrangement (Gallivan *et al.*, 1999). In this type of outsourcing arrangement, more than one independent client collaborate to contract more than one ITSP so as to satisfy their needs. The complex relationships could be regarded as a merger of co-sourcing and multi-vendor relationships (Gallivan *et al.*, 1999). This is because its characteristics are a mix of that of co-sourcing and multi-vendors relationships. Similar to the co-sourcing relationships, complex relationships bring about benefits such as sharing and reducing business risks, increase bargaining power, save time and money, and leverages buyer economies of scale. However, the cons of co-sourcing and multi-vendor exist in complex relationships, which includes complexity, excessive monitoring and client coordination burden (Beulen *et al.*, 2002).

2.4.2 Classification based on the nature and location of the service provider

ITO arrangements are also classified based on the nature of the relationship (i.e. internal or external) and location of the ITSP (i.e. national or international). According to Meyer *et al.* (2005), there are four types of ITO (Figure 2-3) based on this classification, which are external domestic ITO, internal domestic ITO, external international ITO, captive ITO.



	National	International
External IT provision	**External domestic IT outsourcing**	**External international IT outsourcing**
Internal IT provision	**Internal domestic IT provision**	**Captive IT outsourcing**

Figure 2-3: Type of ITO arrangement – based on the nature and location of the service provider (Schaaf, 2004, p. 3)

2.4.2.1 External domestic Information Technology Outsourcing

External domestic ITO is also referred to as onshore outsourcing (Erik *et al.*, 2006). In this setting of ITO, the client and ITSP are located in the same country. Meyer *et al.* (2005) mentioned that external domestic ITO could be considered the first type of ITO arrangement because Kodak's ITO deal with IBM was domestic but external. The pros of external domestic ITO are ease of access and communication due to proximity and the major con is the high cost of service.

2.4.2.2 External international Information Technology Outsourcing

External international ITO is also referred to as offshore outsourcing (Erber *et al.*, 2005; Kliem, 2004). In this type of outsourcing arrangement, the client and ITSP are located in different countries or geographical areas. This type of ITO became possible as a result of the development of the internet and which led to the reduction in communication cost (Meyer *et al.*, 2005). According to Optimus (2016), organisations that engage in external international ITO benefits from the reduced cost of services, however, they are prone to risks such as loss of control and access.

2.4.2.3 Internal domestic Information Technology Outsourcing

In this setting of ITO arrangement, the ITSP is within the same organisation (Meyer *et al.*, 2005). Organisations that adopt the internal domestic ITO arrangement have their IT department operate independently of other units in the organisation. In this case, the IT department, which could be a shared service center is responsible for the provisioning of IT services to other units in the organisation (Meyer *et al.*, 2005). Internal domestic ITO is usually adopted by government organisations. In this type of setting, the IT shared service center delivers IT as a service to other government departments (Bradley *et al.*, 2012).

2.4.2.4 Captive Information Technology Outsourcing

The Captive ITO is similar to the internal domestic ITO in the sense that both client and ITSP are within the same organisation. However, in the case of captive ITO, the client and ITSP are located in different countries or geographical location (Meyer *et al.*, 2005). In this type of outsourcing arrangement, the IT department of an organisation also referred to as the Captive unit, operate independently of other units in the organisation. It is usually in form of a subsidiary unit located in another country (Schaaf, 2004). The Captive unit leverage on the internet and low communication cost in delivering IT as a service to the other units within an organisation.

2.4.3 Classification based on the volume of outsourced Information Technology

The last category of ITO arrangement identified in the literature is based on the volume or magnitude of the IT functions outsourced. Researchers have identified two types of outsourcing based on this classification, and they are – total outsourcing and selective outsourcing.

2.4.3.1 Total outsourcing

Total outsourcing is the contracting out of the entire IT functions in an organisation to a third-party service provider (Barthélemy *et al.*, 2004). In this setting, the client transfers more than 80% of its internal IT asset and staff to a service provider, who in return delivers IT as a service to the client based on contract agreement (Lacity *et al.*, 1996). Total outsourcing, which is usually long-term, comes with benefits such as cash infusion, low cost of vendor management and economics of scale, (Barthelemy, 2001; Clark Jr *et al.*, 1995). However, Lacity *et al.* (1996), Hirschheim *et al.* (1997) and Barthélemy *et al.* (2004) indicated that organisations that engage in total outsourcing are prone to risks such as vendor lock-in, loss of control, loss of IT expertise and service provider inflexibility to change (Doran *et al.*, 2004). These risks have resulted in, Lacity *et al.* (1996) and Barthélemy *et al.* (2004) to recommend the selective IT outsourcing approach.

2.4.3.2 Selective outsourcing

Selective outsourcing is the contracting out of part or bits of the entire IT functions of an organisation to a third-party service provider (Lacity *et al.*, 1996). In this type of outsourcing arrangement, the client keeps 20 to 80% of the entire IT function in-house and transfers selected IT functions to the third-party service provider (Lacity *et al.*, 1996). The criteria for selecting the IT functions to be outsourced varies in different organisations (Barthélemy *et al.*, 2004). Most organisations outsource operational IT functions (also referred to as commodity items) that are repetitive in nature such as help desk and network maintenance, while they retain strategic IT functions such as research and development in-house (Davis *et al.*, 2004; Lynda *et al.*, 2009). The process of selecting or deciding on the IT function to outsource is usually systematic and has resulted in selective outsourcing being the most productive and satisfactory outsourcing arrangement (Lacity *et al.*, 1996). However, risks such as vendor management costs and multiple contract evaluation need to be managed (Doran *et al.*, 2004).

2.5 Information Technology functions organisations outsource

The IT functions organisations outsource has evolved over time (Bradley *et al.*, 2012). Initially, organisations outsource traditional or auxiliary functions such as development and maintenance of back-office systems, recently, organisations outsource high-end functions and strategic activities such as research and development. The extent to what organisations outsource varies, depending on the organisational level (strategic, operational or support) the IT function supports or enables (Bradley *et al.*, 2012). In a study by Barthelemy (2001), the findings (Figure 2-4) show that infrastructure maintenance such as data center operations, and network management, and user support are the most outsourced IT functions in organisations.

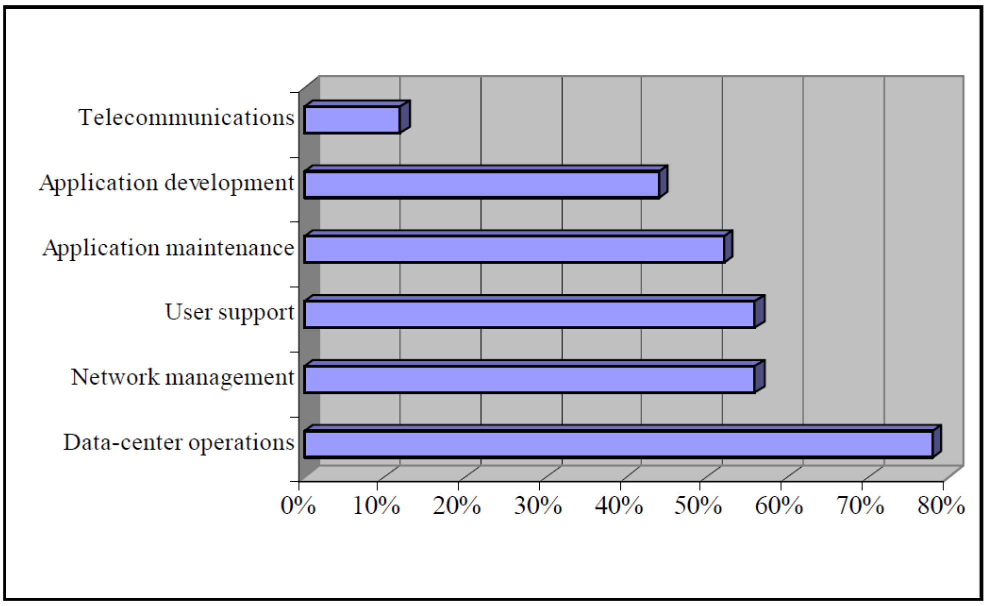


Figure 2-4: Most outsourced IT functions (Barthelemy, 2001, p. 62)

Bradley *et al.* (2012) indicated that the most outsourced IT functions are – infrastructure management, independent testing, and validation, application development and maintenance, help desk, systems integration, managed security, data center management, research and development, and cloud computing.

2.6 Information Technology Outsourcing life cycle

A life cycle is the illustration of all activities a subject matter is involved in from the beginning to the end of its existence (David *et al.*, 2009). Hence, ITO life cycle is the illustration of the sequence of processes involved in the outsourcing of IT functions/department (David *et al.*, 2009). Different authors have described the ITO lifecycle differently. Hirschheim *et al.* (2002) indicated that the ITO life cycle starts with the decision to outsource, continues with the outsourcing relationship and ends with the cancellation or expiration of the outsourcing relationship, while David *et al.* (2009) stated that the ITO life cycle starts with the search for a need to outsource and ends when the contract is completed. According to David *et al.* (2009), the ITO life cycle is in three sequential phases, which are – pre-contract phase, contract phase, and post-contract phase (See Figure 2-5).

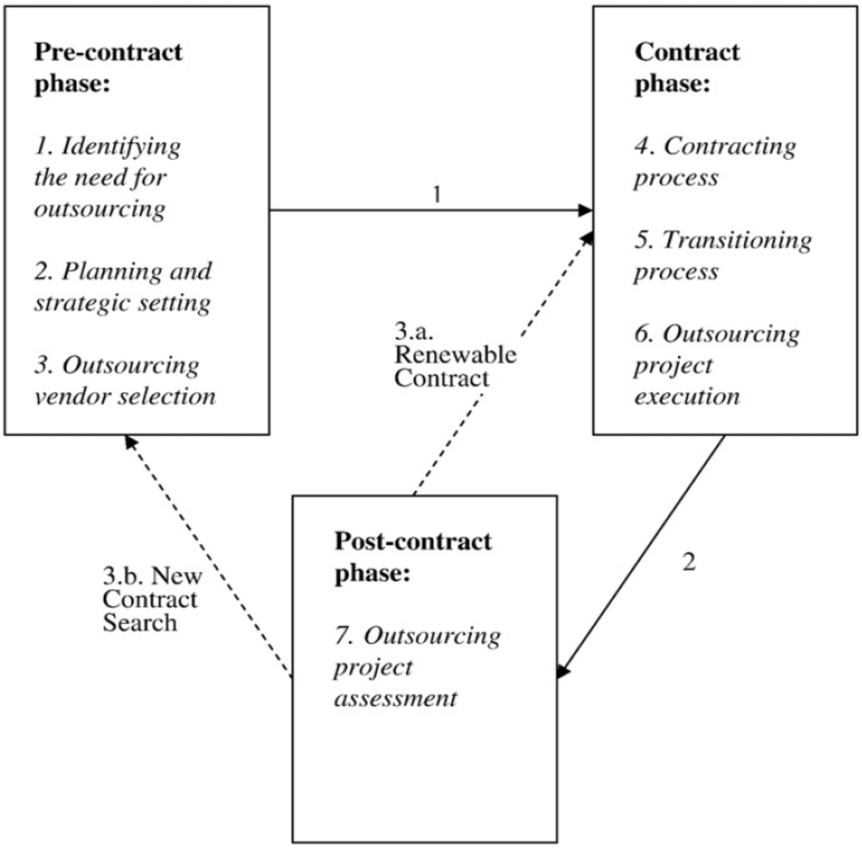

Pre-contract phase:
1. Identifying the need for outsourcing
2. Planning and strategic setting
3. Outsourcing vendor selection
1
Contract phase:
4. Contracting process
5. Transitioning process
6. Outsourcing project execution
3.a. Renewable Contract
2
3.b. New Contract Search
Post-contract phase:
7. Outsourcing project assessment

Figure 2-5: ITO life cycle (David *et al.*, 2009)

2.6.1 Pre-contract phase

This phase comprises of series of activities carried out before the contracting of a service provider. According to David *et al.* (2009), there are three sub tasks under this phase:

a) ***Identifying the need for outsourcing*** – during this process, the executives, by conducting a study or developing a business case to establish a rationale for outsourcing, justifies why ITO is an appropriate strategy for the organisation (Davis *et al.*, 2004);

b) ***Planning and strategic setting*** – this process involves establishing an alignment between ITO initiative and the organisation's corporate plan and strategy; and

c) ***Outsourcing vendor selection*** **–** this stage involves activities that guide the selection of a service provider, which includes reviewing of a request for proposal (RFP) and project justification (Lynda *et al.*, 2009). The expected outcome of these activities is the selection of the most appropriate service provider who fits into the organisation strategy.

2.6.2 Contract phase

This phase comprises of contractual and vendor relationship activities from the time a contract is signed until the contract expires. According to David *et al.* (2009), this phase consists of three sub tasks, which are:

a) ***The contracting process*** **–** this stage involves activities that leads to the signing of an agreement between the client and the service provider. David *et al.* (2009) recommend that before an agreement is signed with a service provider, organisations should ensure that every element such as budget, pricing, legal features, penalties, compensations, and service level agreement (SLA), of the project/service are explicitly defined, to avoid disputes between both parties.

b) ***The transitioning process*** **–** this stage involves the planning and preparation towards implementing the outsourcing agreement. Robinson *et al.* (2005) indicated that this stage is one of the complicated phases of the ITO life cycle because it involves many fundamental workloads required for the implementation of project/service. These workloads include documentation of all activities, workflows, technologies, and people that will be involved in the implementation exercise.

c) ***The project execution*** – this stage involves the actual implementation of an outsourcing contract. At this stage, all contents of the contract and SLA would be delivered and implemented as agreed (David *et al.*, 2009). Robinson *et al.* (2005) termed this stage as a “contract governance stage” that comprises of project management, change management, relationship management, and risk management.

2.6.3 Post-contract phase

This phase comprises of activities carried out after contract expiration. The fundamental activity in this phase is the project assessment exercise, which then serves as the basis for future outsourcing initiative (David *et al.*, 2009). The project assessment exercise involves assessing the deliverables of a concluded outsourcing contract. According to David *et al.* (2009), after the completion of an outsourcing contract, a client must measure their satisfaction level and evaluate the quality of the service delivered by the service provider. Furthermore, the result of the evaluation should serve as the basis of decision making as to whether the contract should be renewed or not.

2.7 Reasons for Information Technology Outsourcing engagement

Many researchers have investigated and identified different reasons why organisations engage in ITO. These reasons could be categorised broadly into three, which are economic, business, and technological reasons. Economic reasons have been identified as the main motivation for outsourcing IT. Lacity *et al.* (2009) indicated that the primary reason organisations outsourcing IT is to gain economic benefits. Such benefits include overhead staff reduction, reduction of production and technology cost, to improve cost control, restructuring of the IT budget, and cash infusion. However, findings from a study by Davis *et al.* (2004) shows that 60% of executive managers are not outsourcing for economic reasons per say. The responses from some of the executives showed that they do not believe in attaining economic benefit from outsourcing IT. A survey by Gonzalez *et al.* (2009) supported Davis *et al.* (2004)’s findings with cost savings being one of the lowest reasons for outsourcing IT (as shown in Figure 2-6).

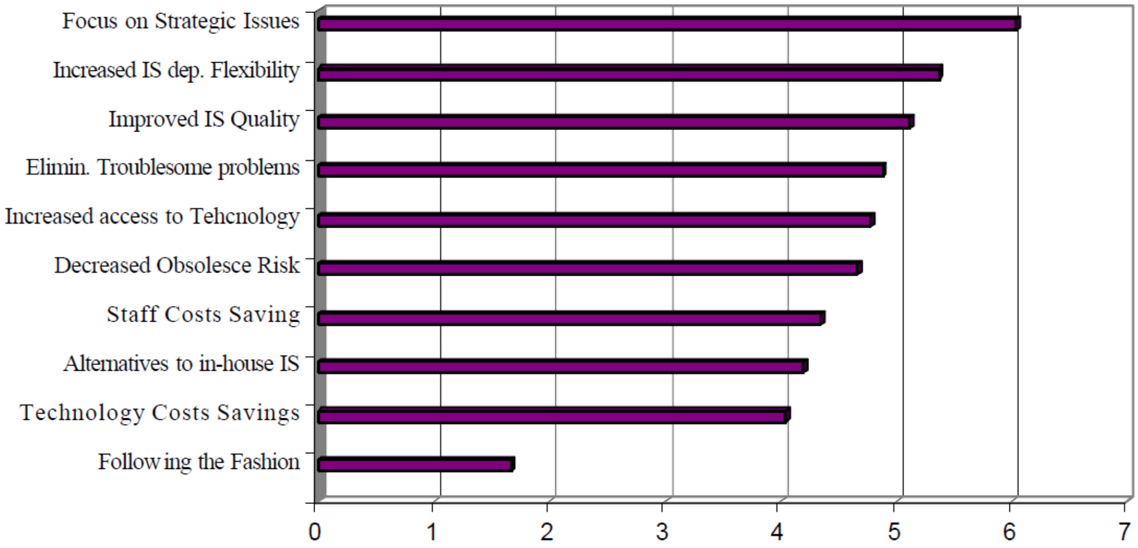


Figure 2-6: Reasons for outsourcing (Gonzalez *et al.*, 2009, p. 186)

From the business perspective, organisations are outsourcing to become more competitive and flexible (DiRomualdo *et al.*, 1998). Consequently, IT support functions that are usually routine, repetitive and less strategic are outsourced, so as to concentrate internal resources on core competence (Lynda *et al.*, 2009). Other business reasons for outsourcing IT are to – create alternatives for IT, improve quality of IT services (Gonzalez *et al.*, 2009), and manage business risk (Davis *et al.*, 2004). For technological reasons, organisations are outsourcing IT to service providers so as to gain access to the required level of expertise and IT specialist at a minimal cost (Gonzalez *et al.*, 2009). Organisations outsource IT to meet the pace of technological advancement and to acquire latest technologies through the service providers (Gonzalez *et al.*, 2009). Davis *et al.* (2004) and Patricia (2014) indicated that the need to share technological risks such as the risk of obsolescence are other reasons for outsourcing IT.

In the literature, two other reasons for outsourcing IT were sparingly mentioned. These are political and environmental reasons (Davis *et al.*, 2004; McFarlan *et al.*, 1995). According to Davis *et al.* (2004), organisations outsource IT for political reasons when faced with business challenges or dilemma. Environmental factors such as industry and economic trends (McFarlan *et al.*, 1995) and intense vendor pressure (Smith *et al.*, 1998) contributes to reasons why organisations outsource IT.

2.8 Information Technology Outsourcing challenges

ITO comes with promising benefits, however, organisations are facing challenges with harnessing the benefits of ITO or attaining their objectives of outsourcing IT. Jackson *et al.* (2001) indicated the challenges organisations face with outsourcing IT are around decision-making and implementation. This is because management needs to make the right choice from varieties of outsourcing options, management strategies, and technology requirements. Davis *et al.* (2004) identified transitional arrangements (in or out) as a major issue because transitioning relies on proper workload distribution, service design, and project design, which are usually costly and tedious. Philip *et al.* (2004) highlighted four common challenges of ITO after conducting a survey of outsourcing practices and their effectiveness. These challenges are – difficulty in identifying or understanding hidden risk; end-user satisfaction; attaining cost savings; and monitoring service performance. In another study, Dhar *et al.* (2006) investigated the challenges two large organisations face with global IT outsourcing. These authors found that different organisations face similar ITO challenges but in varying degrees, because of differences in their management practices. The main challenges Dhar *et al.* (2006) identified are – decisions on what to outsource; selecting the right vendor; formulating scope; deciding the budget and schedule time; developing a governance model; cultural barriers; contract design; and commitment. These challenges of ITO have necessitated the exploration of factors in determining a successful ITO engagement.

2.9 Information Technology Outsourcing success factors

Different researchers have explored the causes of unsuccessful ITO engagements and have identified success factors that could help in attaining the benefits and objectives of ITO. Researchers such as David *et al.* (2009) and Hodosi *et al.* (2015) have identified that the prior identification of the success factors of an ITO initiative is a factor to establishing a successful ITO engagement. David *et al.* (2009) suggested organisations use a bottom-up approach towards achieving a successful ITO engagement. The authors indicated that organisations must identify the success factors of the outsourcing initiative before contracting the IT service. Executives must use these factors as a guide towards making the appropriate strategic and management plans for the ITO deal. In a comparative study of ITO success factors for large size and medium size organisations, Hodosi *et al.* (2015) found that organisation size influences the order of implementing ITO success factors.

Furthermore, it was found that a well-established relationship between the outsourcing organisation and the service provider is a critical factor to a successful ITO engagement. The ITO success factors identified in the literature serve as best practices and standard operating procedures for successful ITO engagement. Some of these ITO success factors are presented in Table 2-1.

Table 2-1: ITO Success factors

Success factors	Sources
• Appropriate project management and risk management	(David *et al.*, 2009)
• Adopt ITO best practices	(David *et al.*, 2009)
• There should be clear understanding of outsourcing goals, scope, objectives, budget and the timeframe of ITO project	(David *et al.*, 2009; Hodosi *et al.*, 2015)
• Strictly define outsourcing strategies most especially areas such as level of integration, performance monitoring, control allocation	(David *et al.*, 2009)
• Understand legal requirements associated with contract negotiation and signing	(David *et al.*, 2009)
• Communicate outsourcing plans with employees and stakeholders	(David *et al.*, 2009; Hodosi *et al.*, 2015)
• Select an appropriate service provider and then communicate corporate outsourcing goals	(David *et al.*, 2009; Hodosi *et al.*, 2015)
• Fix broken or unclear IT function before outsourcing	(Hodosi *et al.*, 2015)
• Develop flexible contract that allows for regular review and update	(Hodosi *et al.*, 2015)

2.10 Reasons for Information Technology Outsourcing failures

Studies have shown that most organisations terminate their ITO contract on a dissatisfactory note due to the challenges of contract management. Researchers have identified different lapses from outsourcing organisation that often results in unsatisfactory ITO outcome. In an article titled “the seven deadly sins of outsourcing”, Barthelemy (2003) highlighted seven reasons for ITO failures. Philip *et al.* (2004) and Artunian (2006) also identified different causes of ITO failures. Philip *et al.* (2004) and Barthelemy (2003) shift the majority of blames on outsourcing organisations for the failure of ITO contracts. This is because, organisations are usually eager to attain the benefits of outsourcing, but unfortunately fail to pay attention to the risks and management of outsourcing contracts. In this case, organisations fail to identify the potential risks that could lead to an unsuccessful ITO engagement. According to Philip *et al.* (2004), outsourcing an unknown function or a complex function is one of the significant offences of ITO. This is because outsourcing uncertainty will expose the organisation to a variety of risks such as opportunism and vendor lock-in. Organisations failing to adopt a risk management approach in outsourcing IT is a contributing factor for ITO failure. A summary of these reasons is presented in Table 2-2, as the Deadly Sins of ITO.

Table 2-2: The Deadly Sins of ITO

Reasons for ITO failure	**Sources**
• Outsourcing a broken or unclear function	(Philip *et al.*, 2004)
• Neglecting the hidden cost of ITO	(Artunian, 2006)
• Outsourcing strategic IT functions that are closely related to the core business	(Artunian, 2006)
• Over expectation	(Artunian, 2006)
• Over outsourcing	(Artunian, 2006)
• Poor governance	(Artunian, 2006)
• Selecting wrong service provider	(Barthelemy, 2003)
• Developing rigid SLA	(Artunian, 2006)
• Misinterpreting the SLA	(Philip *et al.*, 2004)
• Adoption of inadequate strategic sourcing process	(Philip *et al.*, 2004)
• Inadequate contract management	(Philip *et al.*, 2004)
• Inadequate understanding of total cost structure and expected value from the contract	(Philip *et al.*, 2004)
• Lack of upfront risk assessment	(Philip *et al.*, 2004)
• Myopic contract	(Artunian, 2006)
• Lack of exit plan	(Artunian, 2006)
• Disregarding personnel issues	(Barthelemy, 2003)
• Loss of control over outsourced function	(Barthelemy, 2003)

2.11 Conclusion

This chapter presented a review of the literature on ITO, which includes the background of outsourcing, definitions of ITO, IT functions organisations outsource, types of ITO arrangements, ITO lifecycle, drivers of ITO, ITO success factors and challenges of ITO. The chapter highlighted some of the risks associated with different types of ITO arrangements, which shows that irrespective of the type and form of ITO arrangement, risks are involved. Hence, establishing the need to identify, assess and treat the risks involved in any ITO engagement. The next chapter presents the review of risks, ITO risks, and risk management practices.

CHAPTER 3: LITERATURE REVIEW – INFORMATION TECHNOLOGY OUTSOURCING RISKS AND RISK MANAGEMENT

3.1 Introduction

The preceding chapter presented the literature on ITO. It was established that ITO brings benefits to organisations. However, just like in every other business endeavours, ITO also comes with risks (Aubert *et al.*, 1999). This chapter presents the literature on the definition and conceptualisation of risk from different domains. Different forms of risks were reviewed and are presented in this chapter, with particular attention on the risks involved in outsourcing IT to third-party service providers. A review of risk management practices on general outsourcing and ITO are presented in this chapter. The diagrammatic representation of this chapter is presented in Figure 3-1.

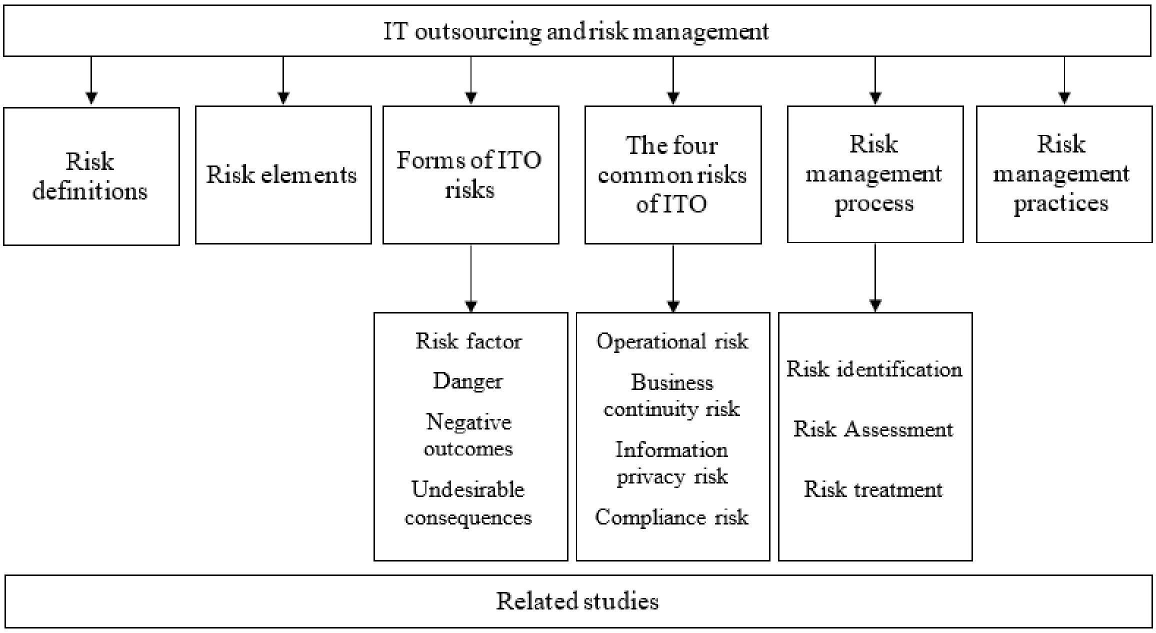


Figure 3-1: Structure of chapter 3

3.2 Risk definitions

Risk is one of the most common buzzwords used (Bahli *et al.*, 2003). However, it is conceptualised differently in the literature. For example, some researchers conceptualised it as a probability, while others conceptualised it as a dangerous activity, a consequence, and an activity or technological threat (Slovic, 1999). These conceptions have influenced how researchers and risk professionals understand and define risk (De Sá-Soares *et al.*, 2014).

In the literature, there is no consensus for the definition of risk (Spikin, 2013). Some researchers, practitioners and institutions have defined risk from a general point of view (regardless of negativity or positivity). For example, the Institute of Risk Management (IRM, 2002) defined it as uncertainty, consequences (negative and/or positive) or the combination of both. Similarly, Spikin (2013, p. 95) defined it as "the distribution of possible deviations from expected results and objectives due to events of uncertainty, which might be internal or external to the organisation". Although, contrarily, some researchers and practitioners have defined it contextually (with negative expectation). For example, Willis (2007) and Campbell (2005) defined it to be the likelihood of an adverse outcome or an equivalence to expected loss.

From the literature, it is observed that context is one of the factors that has influenced diversity in the use and understanding of risk (De Sá-Soares *et al.*, 2014; IRM, 2002). In some fields such as Safety and IT, risk is understood to be a threat that causes harm or negative outcomes to certain events. From an IT perspective, risk entails negative outcomes (such as downtime of services and degradation in system performance) and the factors causing such negative outcomes (such as lack of expertise and insufficient infrastructural capabilities) (ISACA, 2017). Some other fields such as finance, however, understands risk as an opportunity that presents benefits, organisational innovation and competitive advantage for an organisation (Banham, 2009).

3.3 Risk elements

Exploring the definitions of risk has shown that there are different applications of risk. However, in order to assess and control risk effectively, it is essential to understand risk from a general and contextual perspective (Purdy, 2010). From a general view, Alberts (2006) indicated that there are four core elements of risks. These four elements are context, action, condition and consequences (negative or positive).

- ***Context* -** could be defined as the environment, basis, situation or background from which risk is viewed (Purdy, 2010). Context is one of the important elements of risk that needs to be determined first before embarking on risk analysis and planning (H. Berg, 2010). This is because context serves as a guide on what actions, conditions, and consequences are to be considered during the risk management planning. A typical example of context is the industry from which risk is assessed (e.g. IT, finance and safety) (H. Berg, 2010).

- ***Action –*** is an event or activity that provokes risk (Laurie, 2004). According to Alberts (2006), action is the active element that stimulates all forms of risks. However, a specific condition (i.e. the state of being vulnerable) is required for risk to be present.
- ***Condition –*** defines the current situation or position that could lead to risk. Alberts (2006) indicated that condition is a passive element of risk that can result in a consequence or generate an outcome when combined with a definite triggering action.
- ***Consequences –*** is the potential outcome or effect (either positive or negative) of an action **(**i.e. the combination of an action with a specific condition) (Purdy, 2010).

From an ITO perspective, De Sá-Soares *et al.* (2014) identified five elements of risks, these are danger, risk factors, negative outcome, mitigation action, and undesirable consequence. De Sá-Soares *et al.* (2014) developed a conceptual scheme (see Figure 3-2) to explain the relationship between these elements.

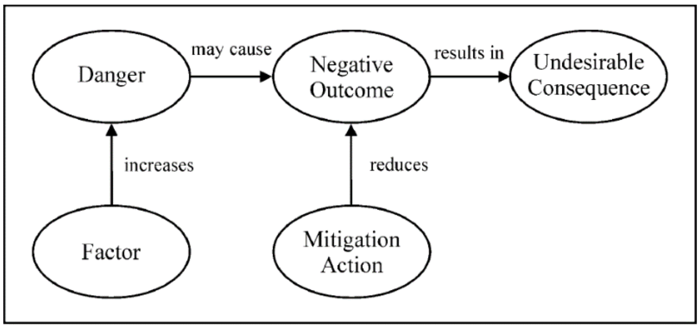


Figure 3-2: Risk conceptual scheme (De Sá-Soares et al., 2014, p. 625)

- ***Risk factor*** – is any attribute or characteristics of an event that increases the exposure of an entity to danger (Ongwattanasirikul *et al.*, 2013).
- ***Danger*** – is a possible source of a negative outcome (Spikin, 2013). According to De Sá-Soares *et al.* (2014), danger is not by itself a damage, but the cause of a damage which may influence negative outcomes. For example, an environmental

disaster is a danger that causes destruction (damage) and leads to loss of business infrastructures (negative outcome).

- ***Negative outcome*** – is an unfavourable result of an engagement that may lead to undesirable consequences (Ongwattanasirikul *et al.*, 2013). Consequently, costing an organisation explicit loss of tangible and intangible assets or opportunities of reaping the expected benefit.
- ***Mitigation action*** **–** is an activity established to attenuate the impact of a negative outcome (ISACA, 2017).
- ***Undesirable consequence*** **–** is the potential effect or impact of a negative outcome or adverse result of an event (De Sá-Soares *et al.*, 2014).

De Sá-Soares *et al.* (2014) explained that the risk factor and mitigation action are mediating elements that influences the intensity or likelihood of a damage occurring. To be more specific, Laurie (2004) stated that the risk factor increases risk severity and mitigation action reduces risk ferocity. Hence, Power (2009) suggested that for risk to be managed to an acceptable level, risk managers must establish mitigating actions or take care of risk factors.

3.4 Forms of Information Technology Outsourcing risks

Risks influences negative and undesirable ITO outcomes (Fan *et al.*, 2012). In the context of ITO, risk means danger (Richie, 2015; Samantra *et al.*, 2014). The risks associated with ITO need to be managed to prevent futile experience. De Sá-Soares *et al.* (2014) indicated that both the service provider and clients involved in an ITO deal could be exposed to risks. However, most studies, like this study, have focused more on investigating client-side risks. This is because the clients suffers more setbacks than the service provider whenever things go wrong with an ITO deal (Ramsaran, 2004; Syed *et al.*, 2007). Researchers and practitioners have identified different forms of risks associated with ITO. They are risk factors; potential dangers; possible negative outcomes; and undesirable consequences (De Sá-Soares *et al.*, 2014).

Risk factor – A risk factor is any action that stimulates risk or increases risk exposure (Fan *et al.*, 2012). In an ITO deal, risk factors could stem from the client, service provider and contract arrangement (Aubert *et al.*, 2005; De Sá-Soares *et al.*, 2014). Fan *et al.* (2012) suggested that in managing the risks associated with an ITO, the risk factors associated with the outsourcing organisation, potential service provider and transactional procedures must be identified. Li *et al.* (2007) identified risk factors identification as the necessary first step to managing ITO risks helps decision makers establish effective plans to address potential risks that could lead to futile ITO engagement.

Researchers have given recommendations on risk factor identification. Fan *et al.* (2012) recommended that risk practitioners must understand the interrelationship between identified risk factors. This is because risk factors are in most cases interrelated, which could result in one risk transitioning to, or facilitating, another risk (Ramachandran *et al.*, 2010). For instance, the interrelationship between technological complexity and requirement confusion could result in the transition of market risk to operational risk (Fan *et al.*, 2012). It is recommended that risk practitioners categorise risk factors according to their source (Bahli *et al.*, 2005). This helps to make effective and efficient decisions in addressing risks. Based on their source, the three categories are the client; service provider; and contract.

Many risk factors associated with ITOs have been identified. De Sá-Soares *et al.* (2014) indicated that most ITO risk factors stem from the client, followed by the transaction agreement, and then the service provider. The major risk factor that stems from the client is lack of expertise in outsourcing management and operations of the outsourced service (Ongwattanasirikul *et al.*, 2013). Similarly, inexperienced staff in contracted service, contract management (Ongwattanasirikul *et al.*, 2013), and opportunistic behaviour (Chauhan *et al.*, 2017; Tho, 2012) are risk factors linked with service providers. Many risk factors are associated with contract agreements. The major ones are uncertainty, task relatedness, asset specificity, and service quantification (Ongwattanasirikul *et al.*, 2013).

Danger – risk factors cause danger (De Sá-Soares *et al.*, 2014). A danger is any threatening attribute or component of an ITO deal that could cause negative outsourcing outcome (Bahli *et al.*, 2003). Some prominent ITO dangers includes unadaptable contract, inadequate communication of service requirements, environmental disaster, unsuitable choice of service provider, poor change management, hostility from internal staff, and non-compliance with regulation (De Sá-Soares *et al.*, 2014). It is necessary for organisations to identify these threatening attributes at an early stage of their ITO engagement so as to be able to quickly establish mitigation plans (Aubert *et al.*, 2005) or they could lead to negative outcomes (Spikin, 2013).

Negative outcome – negative outcome is a result of risk factors or dangers exploiting vulnerabilities in ITO deals (De Sá-Soares *et al.*, 2014). It prevents organisations from attaining their ITO objectives (Ongwattanasirikul *et al.*, 2013). Researchers have identified different negative outcomes that could be encountered from ITO deals. Most of the negative outcomes are often associated with faults in the services rendered, outsourcing relationships, personnel of the parties involved, organisational faults, and contract issues (De Sá-Soares *et al.*, 2014). Some of the prominent negative outcomes of ITO are delay or non-delivery of service; bad quality of service (Ackermann *et al.*, 2011; Jimmy Gandhi *et al.*, 2012); service provider lock-in; outrageous cost of service; and dispute and litigation (Ongwattanasirikul *et al.*, 2013). These negative outcomes need to be identified and catered for; else, they might lead to undesirable consequences (De Sá-Soares *et al.*, 2014).

Undesirable consequences – An undesirable consequence is the impact or effect of negative ITO outcomes on clients. ITO undesirable consequences could be categorised as financial and non-financial. Some of the non-financial undesirable consequences of an ITO include service debasement, lose of capabilitity, reputational damage, drop in employees morale, loss of in-house acute skills, strategic misalignment between business and IT, loss of control on information systems (IS) decisions and failure of internal controls (De Sá-Soares *et al.*, 2014; Gonzalez *et al.*, 2009). The major financial undesirable consequences includes unanticipated transition costs, extra budgeting costs, exorbitant transactional costs (Lacity *et al.*, 2009), and outrageous switching cost (David *et al.*, 2009).

3.5 The four common risks of Information Technology Outsourcing

Deloitte (2012) stated that the operational, business continuity, information privacy and compliance risk of the ITSP are the four common risks of an ITO. Vasant *et al.* (2017) confirms that these risks of an ITO are common and severe, hence, necessitating the need for the effective management of ITSP's risks. From Kaplan *et al.* (2012)'s classification of risks, the ITSP's risk is an external risk because they are not directly under the control of the organisation. External risks are usually severe and cannot be addressed by rule-based risk management approach, but requires alternative approaches such as dialogue (open discussion). The four common risks of ITO (operational, business continuity, information privacy and compliance risk of the ITSP) have been engaged in other research domains like Finance, Safety, and Enterprises Risk Management; however, only a few researchers have investigated these risks in the ITO domain.

3.5.1 Operational risk

Operational risk is also referred to as transactional risk. These are damages caused by a breakdown in internal operations (Alberts, 2006). In the context of ITO, operational risk occurs due to failure in the internal processes of the ITSP, which could lead to failure of service delivery or degraded service (Basu *et al.*, 2006). This ripples on to the ITSP's clients, causing failure in their operations and service delivery (Basu *et al.*, 2006). Aron *et al.* (2005) indicated that factors such as complex operations, geographical distance and an unclear line of communication increase the likelihood of operational risks occurring. Deloitte (2012) suggested having a thorough understanding of the service operations, identifying possible point of failure upfront, and establishing recovery channels to reduce the impact of operational risks on organisations.

3.5.2 Business continuity risk

Business continuity risk is anything that threatens the continuous flow of business operations (Wijnia *et al.*, 2007). Some organisations outsource IT to mitigate business continuity risks. However, these risks could still be inherited from service providers who are exposed to business continuity risks (Brandabur, 2013). Business continuity risks are usually caused by high-risk impact events such as natural disasters, fire incident, theft and power outage (K. Paul, 2011). Although, these events are most times uncontrollable, however, clients can avoid inheriting them from service providers by putting in place measures to either avoid or reduce their occurrence and impact. Deloitte (2012) advised organisations to assess potential service providers' business continuity strategy to be sure they have established plans to recover timeously should an uncontrollable event occur. Furthermore, organisations should simulate risk scenarios periodically to observe the effectiveness of service providers' business continuity strategy. Organisations must also establish exist plans to reduce the impact of service provides totally failing or going out of business.

3.5.3 Information privacy risks

Information privacy risks are anything that could alter the confidentiality and integrity of business information. Information privacy risks of ITSPs is a big concern because ITO involves the transfer of business data, software, and information infrastructure to the service provider (Basu *et al.*, 2006; Cheng, 2012). If a service provider is compromised there is a high chance that their clients' data and intellectual properties will be divulged (Chandra, 2005). This will result in high impact outcomes such as reputational damage, litigation, loss of revenue and loss of customers (Deloitte, 2012). Chandra (2005) indicated that information privacy risks could be subjective or objective. Subjective risk refers to the intentional breach or misuse of client's information, while objective risk refers to the accidental breach or misuse of client's information by a service provider. In order to prevent both forms of risk, organisations must identify potential risk factors and implement mitigation measures to address them (Basu *et al.*, 2006).

It was found that the lack of proper inspection of service providers' data protection protocol, network security, internal management/organisation culture, and regulations contributes to information privacy risks (Basu *et al.*, 2006; Cheng, 2012). Basu *et al.* (2006) suggested that clients must establish supervision mechanism and line of communication to enable regular monitoring of service providers' information system. Deloitte (2012) proposed that clients should conduct an occasional visit to service providers' site to assess their security and data protection systems (Cheng, 2012). Clients must assess the service provider's service organisation control (SSAE16/SOC) report, which must have an auditor's description, evaluation, and comments on the service provider's security and data protection control.

3.5.4 Compliance risks

Compliance risk is the possibility and consequences of not conforming to certain regulatory acts, policies or standards. According to Basu *et al.* (2006), compliance risk is the danger of having a service provider violate rules, internal policies, laws, ethical standards and regulations. The United States of America (USA) Board of Governance of the Federal Reserve System (BGFRS, 2013, p. 1) describes compliance risk as the situation when "services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations". Most often, when organisations outsource IT, regulatory responsibilities are shifted to the service provider's organisation. However, if the service provider fails to conform to regulations, the clients are held liable should a risk event be encountered (Deloitte, 2012). In view of this, organisations need to always check that their service providers are compliant at all times in order to reduce the probability of being exposed to the consequences of compliance risk (Robert, 2014). Robert (2014) indicated that organisations must conduct a proper assessment to check that their potential service providers are conforming to required regulations. Deloitte (2012) also suggests that organisations conduct regular checks on the compliant status of the service provider throughout the duration of the contract.

3.6 Risk management process

In the literature, some researchers have defined risk management as the process of identifying, assessing and treating risk, while some described it to be a decision making process towards achieving certain objectives. According to the Institute of Risk Management (IRM, 2002, p. 2), risk management is the "process whereby organisations methodically address risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities". Kliem (2004) defined risk management as the process of reacting to scenarios that present negative and positive outcomes, with the aim of attenuating the loss from negative outcomes. H. Berg (2010, p. 81) claimed that one of the most accepted descriptions of risk management is, "a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues".

As explained by the Institute of Risk Management, risk management involves three defined processes that are collectively known as the risk management process. These processes are –

- ***Risk identification*** – this is the first stage in the risk management process. It involves the identification of potential risks that could prevent achieving certain objective (Fan *et al.*, 2012; IRM, 2002).
- ***Risk assessment*** – this is the process of analysing and evaluating the likelihood of occurrence or impact of the identified risks (Gary *et al.*, 2002; ISO, 2009).
- ***Risk treatment*** – this is the establishment of cost-effective measures to attenuate the impact of a risk or reduce the likelihood of its occurrence (Gary *et al.*, 2002; ISO, 2009).

The three risk management processes have been the basis of almost all risk management practices (Aris *et al*., 2008; Syed *et al*., 2007). Practitioners and researchers have adopted and contextualised these processes in developing proprietary risk management protocols such as risk policies, frameworks, and standards that suit their environment and objectives. The adoption of the risk management processes has resulted in its evolution. H. Berg (2010) and Aris *et al.* (2008) in their study extended the risk management processes to include components such as establishing context, risk monitoring and review, and documentation (see Figure 3-3). These extended features of the risk management process contribute to the effectiveness and efficiency of the risk management endeavour.

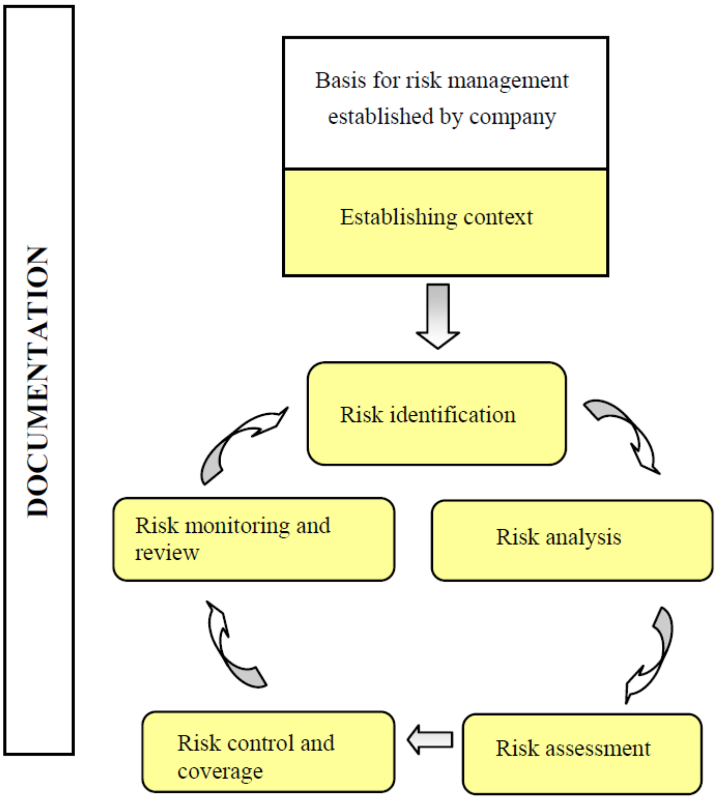

DOCUMENTATION
Basis for risk management established by company
Establishing context
Risk identification
Risk monitoring and review
Risk analysis
Risk control and coverage
Risk assessment

Figure 3-3: Risk management lifecycle (H. Berg, 2010, p. 83)

3.7 Risk management practices

This comprises of standards, methods, tools and approaches used in identifying, assessing and treating risk. Deloitte (2014b) suggested that organisations must ensure that the risks of ITO are managed before concluding an outsourcing deal. Syed *et al.* (2007) indicated that the necessary first step in managing risk is to constitute a Risk Committee who will be responsible for the effective identification, assessment and treatment of ITO risks

(Vasant *et al.*, 2017). Philip *et al.* (2004) indicated that organisations must incorporate risk management practices into ITO life cycle because risk management is a significant contributor to successful ITO engagement. Researchers have used different risk management methods, approaches and tools in identifying, analysing, assessing, treating and monitoring the ITO risks.

3.7.1 Risk identification

This is the process of identifying the potential risks associated with outsourcing an IT function to a service provider. Risk must be identified at an early stage of the ITO initiative (Deloitte, 2014b). This allows the organisation to be aware of threats and danger that needs to be addressed (Ho *et al.*, 2015). Deloitte (2014b) noted that it is most appropriate to identify risks during ITO strategy-planning phase. During this phase, risk practitioners are required to gather service and risk-related information through different means such as administering questionnaires, brainstorming, scenario analysis, inspection of the ITSP, and roundtable discussion with users and stakeholders that requires the service (IRM, 2002; Syed *et al.*, 2007).

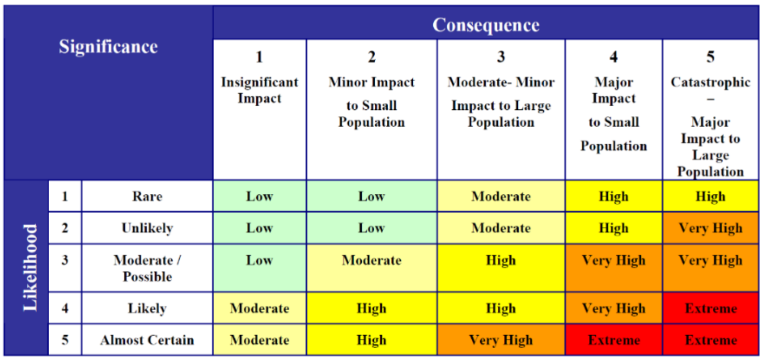
According to the Institute of Risk Management (IRM, 2002), developing a risk profile is an essential part of the risk identification phase. A risk profile is a representation of an organisation's risk posture. Meaning, it exhibits an organisation's risk exposure. To ensure an effective risk management process, Vasant *et al.* (2017) indicated that the ITO risk identification process should be driven towards developing a complete risk profile of the service provider. The risk profile of the service provider must comprise of a risk register where inherent risks for outsourcing the IT service and contracting the service provider would be recorded (King III, 2009). The risk register must also contain details and description of the identified risks that can be used for the purposes of tracking and referencing.

3.7.2 Risk analysis

According to ISACA (2017), risk analysis involves estimating the risk exposure of an entity. Risk exposure could be described as the probability of an undesirable outcome occurring and the loss associated with the undesirable outcome (Aubert *et al.*, 1999). The literature shows that there are different means of estimating the probability of occurrence and impact of risks. According to ISACA (2017) the occurrence and impact of risk can be estimated based on past experience or historical information. However, where there is no historical information about a risk event, risk can be estimated using the risk factors associated with the event.

Risk could be analysed by either using a quantitative, qualitative or semi-quantitative method (ISACA, 2017). The quantitative method expresses the analysis in numerical format, the qualitative method presents the analysis in narratives, and the semiquantitative method represents the analysis as a combination of numbers and narratives. These analysis methods are the bases of different risk analysis techniques. Some risk analysis techniques based on quantitative method are Monte Carlo simulation, decision tree analysis, cost-benefit analysis and sensitivity analysis (ISACA, 2017). Risk analysis techniques based on qualitative method are business impact analysis (BIA), Strength weakness opportunity and threat (SWOT) analysis, and probability analysis (IRM, 2002; Syed *et al.*, 2007). According to ISACA (2017), the technique to adopt depends on the criticality of the outsourced IT service and severity of the identified risks. H. Berg (2010) noted that high impact risks are usually subjected to expensive techniques based on quantitative method while moderate or lower risks are analysed using analysis methods based on qualitative or semi-quantitative method.

The risk matrix is one of the popularly used tools for risk analysis. According to Alexander *et al.* (2006), a risk matrix is a simple tool that makes it easy to assign metrics or values to risks. The risk matrix is usually a semi-quantitative analysis tool, where standard quantitative and qualitative values are assigned to the impact (consequence) and probability (likelihood) of occurrence axis. Each risk is assigned their respective quantitative or qualitative value of probability of occurrence and impact, which will then be plotted on the risk matrix to generate the overall risk exposure value. According to H. Berg (2010), different criteria (such as low, moderate, insignificant impact, rare as shown in Figure 3-4) could be used to define each value to suit the organisational context. However, the graph must be readable, understandable and precise because the results from the risk matrix will serve as the basis for risk evaluation and treatment (IRM, 2002).



Significance			Consequence				
			1 Insignificant Impact	2 Minor Impact to Small Population	3 Moderate- Minor Impact to Large Population	4 Major Impact to Small Population	5 Catastrophic – Major Impact to Large Population
Likelihood	1	Rare	Low	Low	Moderate	High	High
	2	Unlikely	Low	Low	Moderate	High	Very High
	3	Moderate / Possible	Low	Moderate	High	Very High	Very High
	4	Likely	Moderate	High	High	Very High	Extreme
	5	Almost Certain	Moderate	High	Very High	Extreme	Extreme

Figure 3-4: Example of risk matrix (H. Berg, 2010, p. 86)

3.7.3 Risk assessment

Risk assessment is the process of evaluating risks (Gonzalez *et al.*, 2010; Samantra *et al.*, 2014). This involves prioritising analysed risks in the order of most-to-least-critical (Richie, 2015). Risk prioritisation is the systematic organisation of risks in the preference of probability of occurrence and impact (ISACA, 2017). According to H. Berg (2010), the organisation of risks, allows for the categorisation of risks into acceptable and non-acceptable; aids effective allocation of resource; and facilitates the adoption of risk response strategy. As illustrated in Figure 5, the risk matrix allows for the easy assignment of severity levels to risks (low, moderate, high, very high and extreme) (H. Berg, 2010). Panthi *et al.* (2007) noted that the risk matrix also facilitates the adoption of appropriate risk response strategies during the risk treatment phase. In this regard, the risk matrix is structured as a graph with four quadrants (i.e. avoidance, mitigation, acceptance and transference) as illustrated in Figure 3-5 (Alexander *et al.*, 2006). The probability and consequences values of analysed risks are plotted on the graph to identify the appropriate risk response strategy to adopt (Alexander *et al.*, 2006).

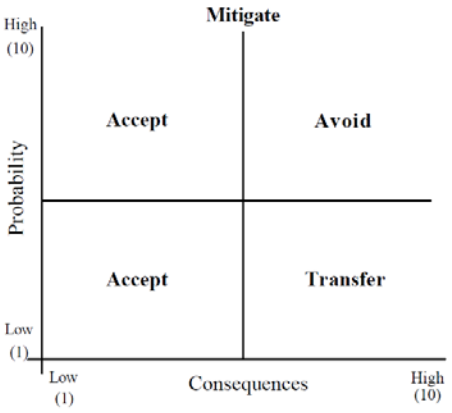


Figure 3-5: Generic risk matrix (Alexander *et al.*, 2006, p. 2)

3.7.4 Risk control and coverage

According to H. Berg (2010), not all risks are acceptable. Unacceptable risks need to be treated. The criteria for acceptable risks are – severity level is adequately low and treatment is economical; treatment is not available; the benefit of the risk event overweighs the level of threat (ISO, 2009). On the other hand, unacceptable risks are risks that are greater than the acceptable/tolerable risk level of the organisation/project.

Organisations need to treat unacceptable risks until they are tolerable. Basu *et al.* (2006) argued that risks cannot be totally eliminated because of factors such as cost and business changes; however, appropriate risk treatment could bring risk to an acceptable level. Risk treatment is about developing cost-effective controls to address or modify unacceptable risk by reducing their impact or likelihood of occurrence (IRM, 2002). According to Boehm (1991), risk treatment involves the design of response plans to eliminate or reduce risks to acceptable level.

Risk response planning is the process of deciding on the appropriate risk response strategy to adopt (PMBOK3, 2004). There are four common risk response strategies identified in the literature, these are – acceptance, mitigation, transference, and avoidance (ISACA, 2017). H. Berg (2010) noted that these risk response strategies are not mutually exclusive. However, whichever combination a risk practitioner plans to adopt must be assessable, actionable, achievable, appropriate, agreed, affordable and allocated (PMBOK3, 2004). Vaughan (1997) categorised the four risk response strategies into two – risk financing and risk control methods. Risk control methods consist of risk avoidance and mitigation; they are methods used for minimising organisational risks through preventive and control measures (IRM, 2002; Vaughan, 1997). Risk financing methods include risk transference and acceptance; they are generally methods focused on ensuring the availability of funds to cover for losses that may occur (Vaughan, 1997).

- ***Risk avoidance*** – this is the aversion from activities or sources of risk (Spikin, 2013). This is usually the case when the consequences of risk occurrence are high.
- ***Risk transference*** – this is the transfer of risk or risk management responsibility to a third-party who can handle/manage the occurrence of risk (ISO, 2009). According to Spikin (2013), this is most likely the best option when the impact/consequence of risk is high.

- ***Risk mitigation*** – this is the appropriate response strategy in cases where risk avoidance and transfer is not an option due to circumstances such as high expected profit and confidentiality (Panthi *et al.*, 2007). Hence, organisations will have to bear the cost of mitigating the risk by either –
    - reducing the likelihood of occurrence through measures such as preventive maintenance, quality assurance, and business process re-engineering (H. Berg, 2010).
    - reducing the impact or consequence on the business through measures such as contingency planning, derogating exposure, and relocating resources to a less risky location (H. Berg, 2010).
- ***Risk acceptance*** – this is doing nothing to the identified risk (Spikin, 2013). According to Alexander *et al.* (2006), in almost every business endeavour, unanticipated risks are accepted however planned for. These authors further explained that one-way organisations plan for such risk is by saving during the good times regarded as "raining day funds", in order to cover up for the consequences of such risk (Alexander *et al.*, 2006, p. 3).

3.7.5 Risk monitoring and reviewing

The dynamic nature of risks is requiring for continuous monitoring and reviewing of treated risks (ISO, 2009). H. Berg (2010) indicated that there is a need for regular monitoring and checking of previous assumptions on risk (risk factors, probability and consequences) and the effectiveness of treatment mechanisms. This is to ensure validity and compliance of risk management protocols with the changing environment. H. Berg (2010) further noted that a review process must follow the monitoring of risks. Every effective risk management process must include a review process to ensure that established risk management procedures are appropriate or require improvement (ISACA, 2017). The review must take into consideration processes, practices, organisation activities and regulations that have changed over time. Organisations must establish a communication and reporting system for proper capturing of past and present risk information (ISO, 2009). H. Berg (2010) suggested organisations establish a communication and reporting framework that allows stakeholders report about risks and risk management procedures and their impact on business operations.

3.7.6 Documentation

Documentation is required in every risk management endeavour in order to prove that a systematic approach was established and for the sustainability of the process (ISACA, 2017). H. Berg (2010) suggested that risk practitioners compose risk management handbook. The handbook must comprise of fundamental policy, risk categories and risk management process and organisation. The risk management handbook must be distributed and communicated to all organisational stakeholders for proper comprehension and implementation.

3.8 Related studies: Information Technology Outsourcing Frameworks

Studies have established risk management outsourcing practices, which is adaptable in the ITO domain. Some of such studies have focused on specific areas of risk management and outsourcing. While some have focused on risk management and outsourcing as a whole. This section discusses those studies that have engaged risk management with outsourcing/ITO to develop risk management outsourcing/ITO protocols.

In a study on risk management of outsourcing, Benvenuto *et al.* (2005) developed a supplier risk impact assessment framework. This framework was developed to facilitate periodic assessment of a supplier’s risk profile. As illustrated in the framework (see Figure 3-6), organisations should establish a set of risk criteria (such as mission-critical, high monetary value and vendor reliance) that will be used as a benchmark to evaluate suppliers’ risk profile. The framework facilitates the generation of suppliers’ risk ranking and assist risk practitioner in making decisions such as selecting an appropriate supplier and developing an SLA. In the case where the most suitable supplier in terms of outsourcing capabilities is rated as high risk, managers will be aware of the need for rigorous risk management processes or strategies when drafting contract terms (Philip *et al.*, 2004).

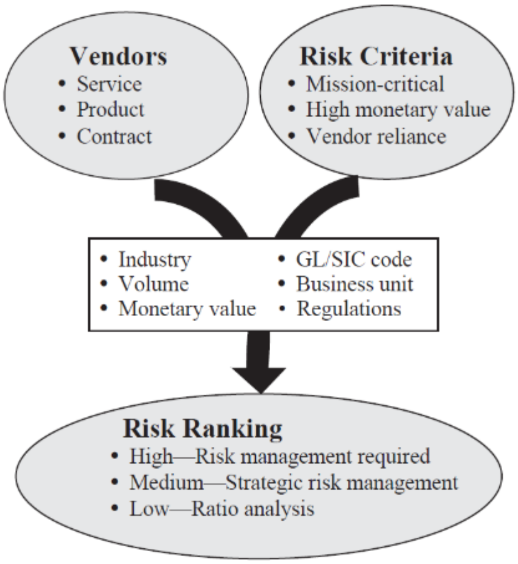


Figure 3-6: Risk impact assessment (Benvenuto *et al.*, 2005, p. 2)

In another study on ITO risk management, Aubert *et al.* (1999) developed a framework to manage the risks associated with ITO. This framework consists of similar components of a risk matrix, with the importance of potential loss on the x-axis and probability of an undesirable outcome on the y-axis (see Figure 3-7). This framework facilitates the allocation of response strategies for managing ITO risks. The framework helps risk practitioners make better decisions as regards risk evaluation and treatment.

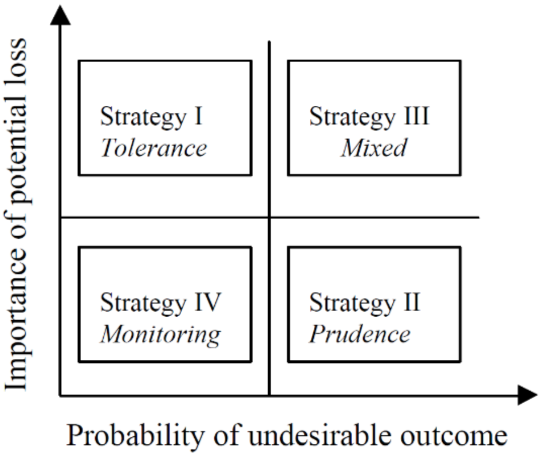


Figure 3-7: Risk management framework (Aubert *et al.*, 1999, p. 4)

Deloitte (2014b) indicated that the "lifecycle approach" is one of the most effective approaches to developing outsourcing/ITO risk management framework. This is because the lifecycle approach helps organisation attain outsourcing goals, as well as ensuring effective contract and relationship management between the client and vendor. Using the life cycle approach requires an integration of the ITO lifecycle and risk management processes (Aris *et al.*, 2008; Philip *et al.*, 2004). Deloitte (2014b), Bradley *et al.* (2012), Aris *et al.* (2008) and Syed *et al.* (2007) have used the life cycle approach to develop ITO risk management protocols. In a critical review study of risk management of ITO, Syed *et al.* (2007) developed a structured process for ITO risk management. This structured process as illustrated in Figure 3-8, is a process flowchart showing the relationship between all the phases of the proposed risk management of ITO process. These phases include – Risk Management Committee creation, strategic analysis of outsourcing decision, due diligence to select a service provider, contract management, and on-going monitoring. Similarly, Deloitte (2014b) proposed an ITO risk management process with the following phases – define strategy and operating model, develop solution and request for proposal, evaluate the deal and manage the transaction, execute transition and transformation, manage on-going operations.

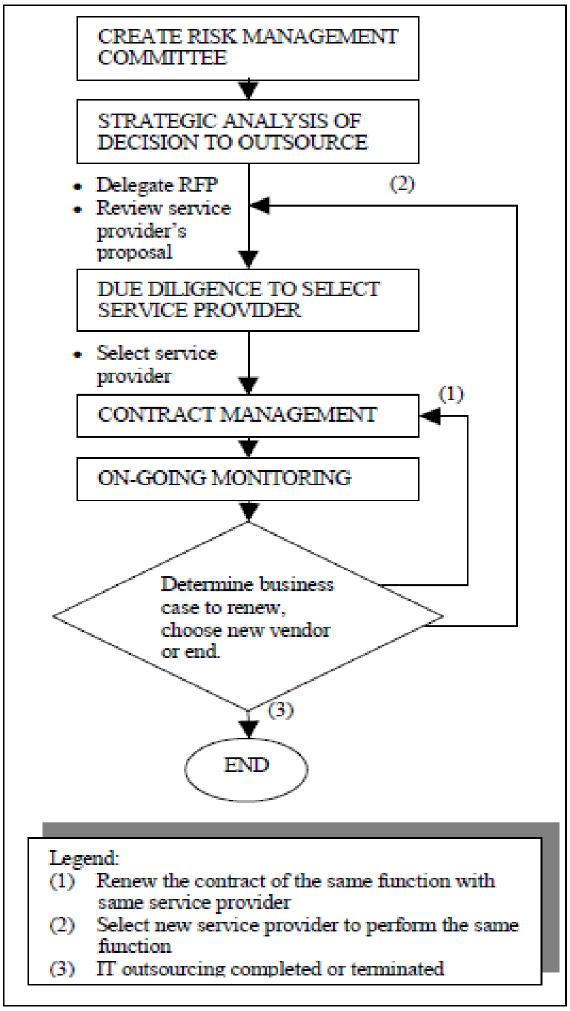

CREATE RISK MANAGEMENT COMMITTEE
STRATEGIC ANALYSIS OF DECISION TO OUTSOURCE
• Delegate RFP
• Review service provider's proposal
(2)
DUE DILIGENCE TO SELECT SERVICE PROVIDER
• Select service provider
(1)
CONTRACT MANAGEMENT
ON-GOING MONITORING
Determine business case to renew, choose new vendor or end.
(3)
END
Legend:
(1) Renew the contract of the same function with same service provider
(2) Select new service provider to perform the same function
(3) IT outsourcing completed or terminated

Figure 3-8: Process of Risk Management in ITO

Benvenuto *et al.* (2005) described outsourcing risk management as a continuous process that consists of three components – SLA management, supplier and contract management and billing accuracy. According to Benvenuto *et al.* (2005), SLA management involves the establishment of contract requirements, agreements and performance metrics of the outsourcing contracts. The supplier and contract management involve the process of monitoring and keeping of performance statistics and records relating to an outsourcing relationship. The billing accuracy is the continuous review of billing by the outsourcing party to ensure compliance with SLA (Benvenuto *et al.*, 2005; Philip *et al.*, 2004). Philip *et al.* (2004) suggested that organisations must develop flexible SLAs that caters for periodic review and update of billing accuracy because it is usually the source of outsourcing issues/disputes.

After carrying out a survey on outsourcing risk management practices and their effectiveness, Philip *et al.* (2004) developed a generic outsourcing risk management framework to guide and inform managers and decision makers on risk management processes that should be considered when outsourcing. This framework (see Figure 3-9) is sectioned into three risk management phases, which are – project management risk, contract management risk, and performance management risk. Philip *et al.* (2004) argued that almost every outsourcing engagement is a project. This is because most organisations adopt project management approaches towards establishing successful outsourcing arrangement (PMBOK3, 2004). According to Philip *et al.* (2004), project management activities are usually centered around establishing an appropriate sourcing strategy that aligns with the organisation's corporate strategy. Philip *et al.* (2004) suggested that to mitigate project management risks, organisations must constitute a cross-functional project team, conduct due diligence in selecting the supplier, adopt an established outsourcing and risk management methodology.

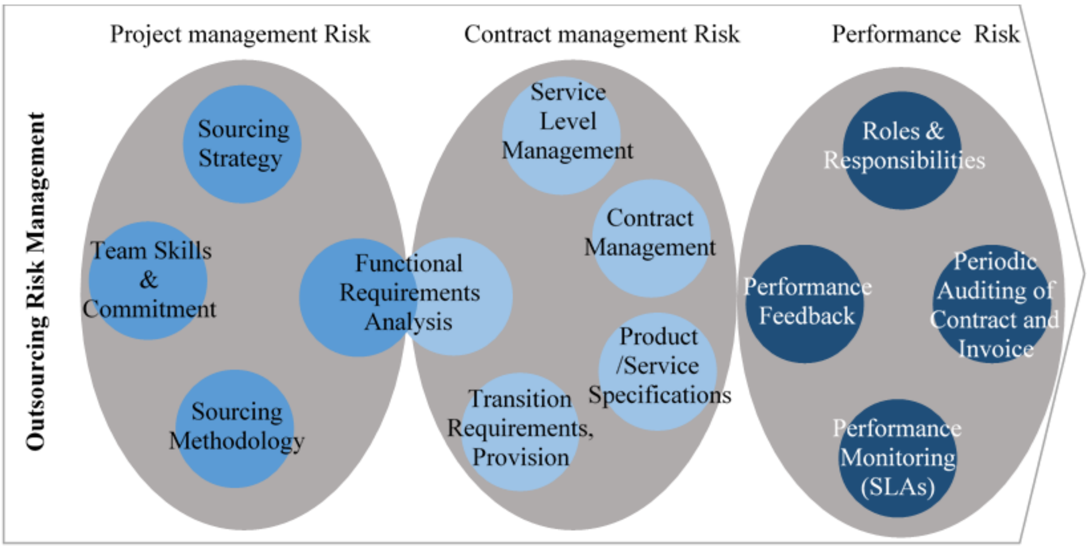


Figure 3-9: Outsourcing risk management framework

Philip *et al.* (2004) indicated that every outsourcing engagement includes a contract management phase. This aspect of the outsourcing arrangement is focused on establishing and documenting formalities and agreements of the service to be outsourced (Syed *et al.*, 2007). Philip *et al.* (2004) suggested that in order to mitigate contract management risks, organisations must develop a contract and negotiation plan and ensure that all aspects of the agreement are intensively documented.

According to Philip *et al.* (2004), outsourcing arrangement must include a performance management phase where services delivered by a vendor is evaluated according to a contract agreement. Philip *et al.* (2004) proposed that to mitigate performance management risks, the outsourcing contract must make provision for performance feedback system, periodic contract and invoice audits, and performance monitoring of the SLA. Clarity of roles and responsibilities is significant to ensure effective contract management as it will support the achievement of an efficient contract and supplier management process and control objective (ISACA, 2017).

3.9 Conclusion

This chapter presented a review of the literature on risks and risk management in relation to generic outsourcing and ITO practices. The concept of risk and risk management was explored from a broad and contextual perspective. Different forms of ITO risks were identified and a basic insight into the four common risks of ITO was presented. It was established that most studies on ITO risk management have focused on developing segmented frameworks for specific areas of ITO risk management. However, the severity of the risks of the ITSP on organisations requires for the development of an ITSP risk management framework. The next chapter presents the research methods, designs and data analysis used to achieve the objectives of this study.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

The preceding chapter presented a review of the literature on risks and ITO risk management practices. This chapter will present the research methodology, comprising of the research approach, design and methods employed in achieving the objectives of the study. Research methodology can be referred to as the theory of how research is being conducted (Saunders *et al.*, 2011). According to Rajasekar *et al.* (2013), it is a systematic approach towards solving a specific research problem. Research methodology encompasses the procedures, step by step approach and techniques a researcher employs to achieve research objectives (Rajasekar *et al.*, 2013). Figure 4-1 presents the outline of the research methodology chapter of this study.

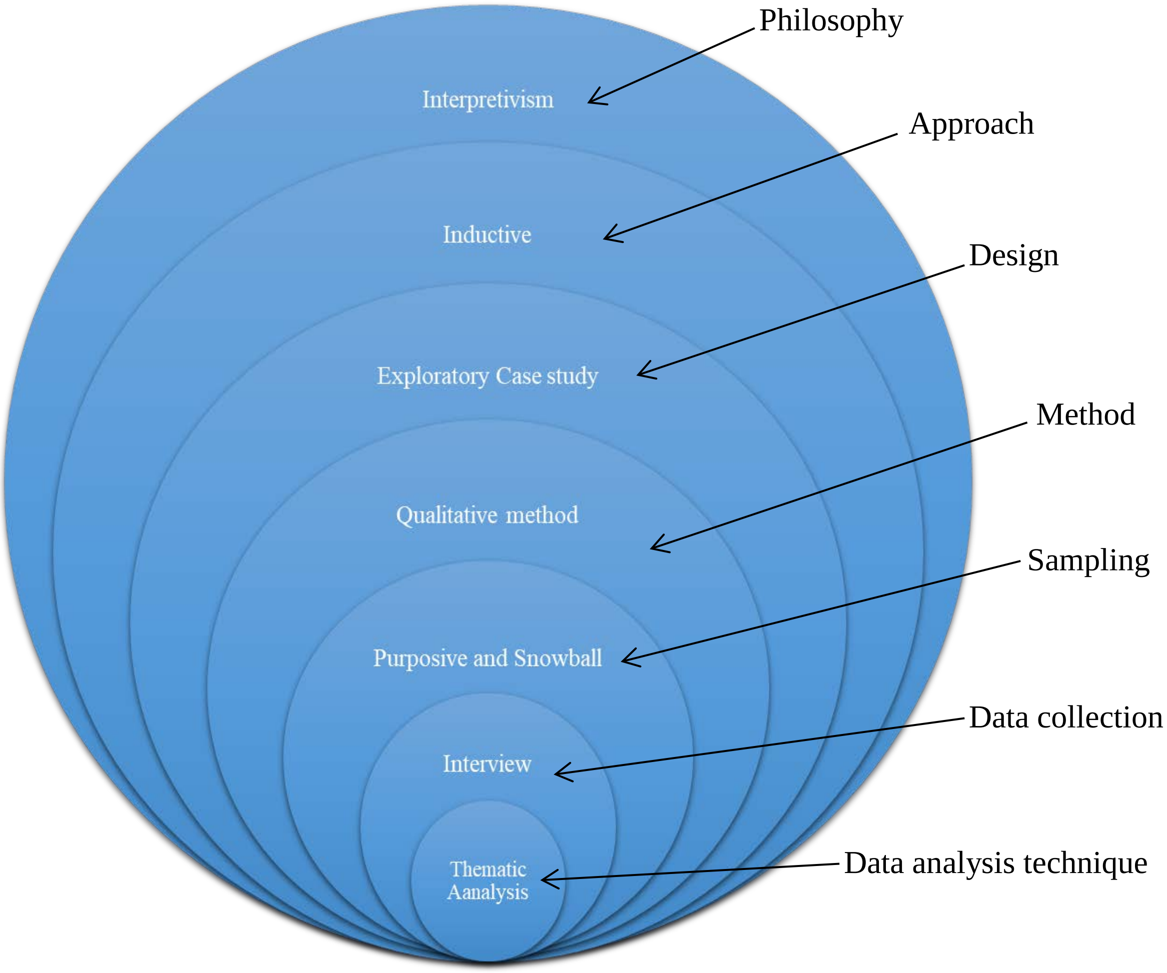


Figure 4-1: Outline of research methodology chapter

4.2 Researcher’s worldview

According to Guba *et al.* (1994), a researcher’s worldview is fundamental to the approach, design and methods to be adopted in a study. A researcher’s worldview refers to the philosophical positioning of the researcher regarding the nature of reality and what institutes acceptable knowledge in a specific domain. Saunders *et al.* (2011) argued that the researcher’s worldview is profound when planning to undertake a research project because it influences the approach, strategies and methods that will be adopted in achieving the research objectives and how knowledge will be developed during the course of the study. In addition, the researcher’s worldview is necessary as it dictates the goal of the research, which is either to understand how social phenomena relates to reality or how the contextual environment shapes the action of the people (Saunders *et al.*, 2011).

In the context of this study, the researcher took an interpretive approach to understand how large organisations manage risks of service providers. As an interpretive researcher, the goal is to understand and interpret reasons, motives, subjective experience, and meanings of human actions within a certain time and context (Neuman, 2002). According to Saunders *et al.* (2011), interpretive research is usually qualitative research, thereby the researcher conducts in-depth interviews for a small sample of people who are capable of giving useful data to answer the research questions. For this study, the researcher explored how large organisations in South Africa manage the risks of ITSP by conducting in-depth interviews with staff involved in managing the risks of ITO in the organisations used as study sites. The analysis of the interviews helped to understand how large organisations within South Africa manage risks of ITSP (Bhattacherjee, 2012).

4.3 Research approach

According to Bhattacherjee (2012), there are two approaches to research; these are the inductive and deductive approach (Saunders *et al.*, 2011). The inductive approach involves constructing theoretical patterns or concepts from an empirical observation, while the deductive approach involves the testing of hypothesises or theories (Bhattacherjee, 2012; Saunders *et al.*, 2011). The inductive approach is appropriate when there are limited or no theoretical frameworks to drive the course of a study. The researcher will have to develop a conceptual framework that would be used to guide the data collection process towards answering the research questions or achieving the research objectives (Bhattacherjee, 2012; Saunders *et al.*, 2011). On the other hand, the deductive approach is appropriate when the research objective is towards testing available hypothesises or to validate known theories. Easterby-Smith *et al.* (2012) argued that it is important to identify the research approach in every study as it allows the researcher to make a better-informed decision on the research design and strategies to adopt.

The inductive approach was adopted for this study because of limited frameworks to guide the course of the study. However, these frameworks are not sufficient to explore how large organisations in South Africa manage the risks of ITSPs. Using the inductive approach, the International Organisation for Standardisation (ISO) 31000 risk management framework (ISO, 2009) was adopted as a conceptual framework to guide the development of the interview guide used for data collection. The inductive approach allowed the researcher to explore the field without constricting factors, which led to the generation of themes used in developing a governance framework of ITSP risk management.

4.4 Research design

Research design is the blueprint that details the procedures and techniques that will be used by a researcher to acquire and analyse applicable data towards answering specific research questions (Bhattacherjee, 2012). In other words, research design enunciates the type of data needed, the methods required to collect and analyse the data and how the defined processes connect to answer the research questions or attain the research objectives (Saunders *et al.*, 2011). Research design encompasses the sampling method, data collection and instrument development process.

Different authors have identified various types of research design. Some of the most popular research designs includes experimental studies, field survey, secondary data analysis, case research, focus group research, action research and ethnography (Bhattacherjee, 2012). Saunders *et al.* (2011) noted that no research design is inferior or superior to the other. The choice of a research design is dependent on the research questions and objectives. Consequently, the research design varies by studies and is subject to the approach a researcher adopts to achieve the objectives of their study (Bhattacherjee, 2012). For example, the research design that is to be adopted in an inductive study, where the observation of a phenomenon leads to theory generation, will be different from deductive research, where the aim of a study is to validate or test a theory. For this study, because the approach used is inductive, the case research design was adopted.

4.4.1 Case study research design

To achieve the objectives of this study vis-a-vis answering the research questions, the case study research design was adopted. According to Bhattacherjee (2012), a case study research allows for the in-depth investigation of a phenomenon or problem in one or more real-life context over a certain period of time. Yin (1989, p. 14) indicated that "the distinctive need for case study arises out of the desire to understand complex social phenomenon while preserving the holistic and meaningful characteristics of real-life events – such as individual life cycles, organisational and managerial processes, and international relations amongst others". The findings in the study by Prado (2011), which shows that there is a relationship between organisation characteristics such as the size and industry type and the depth of risk analysis practices justifies why ITO risks management practices will differ in different organisational context. Hence, the case study research design allowed the researcher to conduct an in-depth investigation on how ITSP risks are identified, assessed and treated in the context of large organisations in South Africa, with the aim of developing an ITSP risk management framework.

According to Yin (2003), the approach to a case study research design could be exploratory, explanatory or descriptive, depending on the purpose of the inquiry. Exploratory research design allows for a clear and systematic search for new insights on a phenomenon being investigated (Robson, 2002). It also gives room for further investigation and understanding of a research problem, thereby providing the researcher with a clearer picture of the research problem (Saunders *et al.*, 2011). Explanatory research design looks at the why and how questions about a phenomenon, which allows a researcher inquire the reasons of occurrence about a phenomenon or problem, mostly in the form of causal connection and relationships (Bhattacherjee, 2012). Descriptive research design looks at the what, where and when about a phenomenon being investigated, which allows for careful observation and documentation of the phenomenon (Bhattacherjee, 2012). It gives the researcher the space to create an accurate profile about events, people and situations; hence, it is mostly adapted as an extension for exploratory and explanatory research (Robson, 2002; Saunders *et al.*, 2011).

For the purpose of this study, exploratory research design was adopted as the primary research design; and the descriptive research design was used as a complementary research design. Exploratory research allowed for an in-depth understanding of how large organisations within South Africa manage the risks of ITSP. Complementarily, descriptive research design allowed for the profiling and documentation of the ITSP risk management practices established by large organisations in South Africa.

Case study research comprises two dimensions, the single case and multiple cases (Bhattacherjee, 2012; Yin, 2003). A single case study is the observation of a phenomenon in one setting. The single case study is appropriate when the phenomenon under research or the research problem is peculiar to a certain context also referred to as a unique case (Saunders *et al.*, 2011). Hence, findings from a single case study are specific to the case. On the other hand, a multiple case study is the observation of a phenomenon through various contextual lenses. The multiple case study is appropriate when the phenomenon under study or research problem is common amongst various contexts (Yin, 2003). Hence, the findings from a multiple case study are usually more reliable and strong (Bhattacherjee, 2012; Gustafsson, 2017; Saunders *et al.*, 2011). The multiple case was adopted in this study in order to establish more valuable findings from both cases; hence, developing a more reliable ITSP risk management framework.

4.5 Research methods

Research methods refers to the schemes, algorithms and systematic procedures used by a researcher for the collection and analysis of data for a particular study (Rajasekar *et al.*, 2013; Saunders *et al.*, 2011). The choice of a research method determines the type of data that will be collected and the data collection and analysis technique to use during the course of the study. Authors such as Bhattacherjee (2012) and Saunders *et al.* (2011) identified two types of research methods, which are quantitative and qualitative methods. Quantitative methods allow for the collection of numerical data, which requires the use of statistical methods such as descriptive and correlation analysis to extract meaning from the data, and the presentation of results in graphs (Bhattacherjee, 2012; Saunders *et al.*, 2011). Quantitative methods are used to investigate a phenomenon or research problem from a broader scope while using a systematic sampling technique to select representative samples from an entire population (Rajasekar *et al.*, 2013). Qualitative methods allow for the collection of non-numerical data such as texts, pictures and videos. It requires the use of text analysis methods such as content and thematic analysis to analyse data and present results in narratives (Bhattacherjee, 2012; Saunders *et al.*, 2011). Qualitative methods involves the use of interviews, focus groups, observations and document reviews to carry out an in-depth investigation of a phenomenon or a research problem (Rajasekar *et al.*, 2013). The results and findings generated when using qualitative research methods are not usually generalisable to a larger population (Patton, 1990).

The quantitative and qualitative methods could be used singly in a study, which is referred to as mono-method; however, they could also be used to complement each other in a study, which is referred to as the multiple method (Bhattacherjee, 2012; Saunders *et al.*, 2011). For the purpose of this study, the qualitative method was used because it allowed for the in-depth investigation of how large organisations in South Africa manage risks of ITSPs. It also allowed the researcher to explore and analyse the data for new insights concerning ITO risk management practices in large organisations.

4.6 Study site

A study site is a physical location or place where data will be collected. The study sites (multiple case study) for this study were two large organisations. Large organisations were chosen because studies such as that of Prado (2011) indicated that large organisations (more than 500 employees) are more involved in risk analysis and management than small and medium enterprises. The large organisations used as study site are in the retail and telecommunication industry within South Africa. There is no specific reasons for choosing the retail and telecommunication companies. However, some other features of these organisations that were considered to have made them appropriate for this study include their dependence on technology, the severity of their outsourced IT functions, duration of ITO practices and listing on the Johannesburg Stock Exchange (JSE). These criteria were used on the basis that organisations listed on the JSE (strict application of the King III principles), highly dependent on technology, outsource business critical IT functions and practicing ITO for several years would engage in best practice ITO risk management practices. Also, potential participants from these organisations would have acquired training, certification and experience over the years of service to answer the research questions sufficiently. Table 4-1 presents the profile of the study site used for the study and the selection criteria.

Table 4-1: Profile of the study sites

Characteristics	Telecom	Retail
Employee head count	> 1000	> 1000
Listing on JSE	Yes	Yes
Dependence on technology	Strategic, management and operational	Strategic, management and operational
Severity of outsourced IT functions	High on strategy, management and operation	High on strategy, management and operation
Duration of ITO practice	> 4 years	> 4 years

4.7 Population of the study

The population of a study could be referred to as the total number of units, people or individuals present in a geographical location or in the study site where data will be collected (Lavrakas, 2008). During data collection, a subset of the population known as the target population is focused on. According to Burns *et al.* (1997), the target population is the total number of units, people or individuals present in a certain area or location that are of great interest to the researcher due to certain attributes or expertise they possess. For this study, the target population were the staff involved in the risk management of ITO functions in the study site. Some of the responsibilities or characteristics of the targeted staff were the years of experience involved in ITO risk management, training on risk management, certifications or qualifications around outsourcing and risk management and job description.

4.8 Sampling methods

Sampling is the strategy used in selecting participants for a study. The sampling method used in a study is determined by the research method adopted. Probability or random sampling method is used for quantitative studies, while non-probability or non-random sampling methods are used for qualitative studies. Since this study is qualitative, the non-probability sampling method was used to select the participants of the study. The non-probability sampling method is a subjective type of sampling method which allows the researcher to select the participants of the study based on a non-random criteria (Bhattacherjee, 2012). Hence, some of the units in the population will have a zero chance of being selected (Saunders *et al.*, 2011). There are different types of non-probability sampling methods including quota, convenience, snowball and purposive. The purposive sampling method was adopted as the main sampling strategy and was complemented with a snowball sampling technique.

4.8.1 Purposive sampling

The purposive sampling method is a non-probability also referred to as selective, subjective and judgemental sampling (Patton, 2001). The purposive sampling relies on the judgement of the researcher to select participants who will best answer the research questions (Saunders *et al.*, 2011). The researcher identifies and focuses the data collection process on certain individuals from the total population due to specific criteria such as experience and expertise in the area of inquiry. There are different strategies of selecting individuals of interest, which includes typical case sampling, critical case sampling, extreme case sampling, homogeneous sampling, maximum variation and expert sampling (Patton, 2001; Saunders *et al.*, 2011). The expert sampling strategy was used for this study because it allows for the selection of individuals who have particular expertise or knowledge around the basis or problem of the study (Bhattacherjee, 2012). According to businessdictionary.com (2018) an expert is someone who has acquire knowledge and skills in a specific domain through study and practice over the years. Using the expert sampling strategy, interviews were conducted for twelve participants who were staff from the two organisations used as the study site. Each of the participants had more than four years of experience in engaging in the risk management of ITO and had acquired professional certifications or had undergone training in the area of risk management or outsourcing.

4.8.2 Snowball sampling method

The snowball sampling, also known as the chain sampling is a sampling strategy that allows for the access or selection of participants through referral (Saunders *et al.*, 2011). The researcher utilises the connection or network of one or two key informants or participants who have a great deal of knowledge around the research inquiry to get access to other individuals of same characteristics (Patton, 1990). The snowball sampling method was used in this study because of the difficulty in getting access to staff members with the necessary expertise of interest in the study site. During the data collection exercise, staff members who participated in the study were persuaded to refer other colleagues in their team or unit to participate in the study. This was achieved through email referrals, which helped to gain immediate access to potential participants.

4.9 Sample size and sample

A sample is a subset of a population whose characteristics when studied, is duly representative of the entire target population (Cherry, 2015). According to Yin (2003), the sample size of a study is the total number of observations or respondents that have been selected to participate in the study. The rules for selecting the number of respondents to partake in a study depends on the research methodology. According to Patton (1990), there are no specified rules for measuring the sample size in qualitative research; it is dependent on the dimensions (depth or breadth) in which the researcher seeks to inquiry. There was no specified sample size for this study; however, the researcher stopped the interview process after the twelfth participant because the data collection process had reached data saturation, as there was no or limited new insights around the research inquiry (Saunders *et al.*, 2011). Hence, the sample size for this study is 12, which conforms with Guest *et al.* (2006), who indicated that 12 participants suffice for a qualitative study using in-depth interviews for data collection from a homogenous population.

4.9.1 Participants' Demographics

In order to achieve the objective of this study, selected participants from two large organisations in South Africa were interviewed. Table 4-2 presents the profile of the participants of this study.

Table 4-2: Profile of participants

Organisational level	Pseudonyms	Quantity	Experience	Qualifications
Executive	**(ExPart)	2	15 – 20 years	All the participants of this study had undergone training and attained certifications in one or
Management	**(MaPart)	4	10 – 16 years	

Operations	**(OpPart)	6	5 – 10 years	more IT management fields including IT governance, Enterprise risk management, IT auditing, IT security. Participants are also certified in at least one of the following certifications; Certified information systems auditor (CISA), Certified information systems security professional (CISSP), Certified in risk and information systems control (CRISC), Control objectives for information and related technology (COBIT), Information technology infrastructure library (ITIL), Certified in the governance of enterprise IT (CGEIT) and Certified information security manager (CISM).

** ExPart (1-n), MaPart (1-n) and OpPart (1-n) represent the pseudonyms used for participants during data analysis and presentation of findings.

4.10 Data collection methods

Data collection methods refer to the technique and procedures used in gathering required data for a study. The data collection method used in a study is determined by the research method adopted for the study. According to Saunders *et al.* (2011), there are different types of data collection methods for both quantitative and qualitative studies. A survey is the popularly used quantitative data collection method, which is a structured or unstructured questionnaire administered to participants of a study either on paper or electronically. On the other hand, interviews, focus groups, observation and secondary documents are common qualitative data collection methods (Bhattacherjee, 2012).

Since this study is qualitative, interviews were used for data collection. An interview is a purposive discourse between two or more people (Saunders *et al.*, 2011). It is a flexible tool for data collection that gives the researcher the room to probe for in-depth responses concerning the research phenomenon or problem (L. Cohen *et al.*, 2013). There is no formal procedure for conducting interview-based research, however, the seven stages of planning and conducting interview-based research suggested by Kvale (1996) was used in this study.

4.10.1 Interview-based research planning and execution

The seven stages of planning and conducting an interview-based research suggested by Kvale (1996) was adopted in order to use a systematic approach for the planning and execution of this study. The stages are as follows:

a) ***Thematising*** – this is the preliminary stage of an interview-based research, where ideas are conceptualised and refurbished into a researchable entity. At this stage, the research aims, objectives and questions are identified and fine-tuned. Furthermore, the appropriate research methods that will drive the collection of appropriate data that will answer the research questions are adopted.

b) ***Designing*** – this is the stage where the interview schedule is developed. At this stage, the research questions and framework are used to guide the crafting and formulation of the interview questions and the structure of the interview schedule. The choice of the type of questions (open-ended) was influenced by the purpose of inquiry (exploratory).

c) ***Interviewing*** – this is the data collection stage where participants are engaged in interview sessions with the aim of collecting the necessary data that would help to answer the research questions. At this stage, series of activities were carried out in order to get access to participants. Gatekeeper’s letters were obtained from the organisations used as study site. Ethical clearance was obtained from the University of KwaZulu-Natal’s Registrar’s Office. Then communication was established with potential participants in order to identify possible interview dates, times, and venue/ medium at the participants’ convenience. Lastly, the interview sessions were recorded with the consent of the participants.

d) ***Transcribing*** – this is the process of converting the audio recording into text. In this study, transcribing was done by the researcher to get familiar with the data set in preparation for the analysis phase.

e) ***Analysing*** **–** this is the process of extracting meaning from the data set using a qualitative analysis technique. At this stage, the thematic analysis was used to generate codes, categories and themes that were relevant to answer the research questions. The NVivo qualitative data analytics software was used to facilitate the generation and management of codes, categories and themes for this study.

f) ***Verifying*** **–** this is the process of validating the results of the data analysis stage. The analysed data is sent to each participant to verify the conformity of their views to the analysed data.

g) ***Reporting*** **–** this includes the presentation of findings and discussion. The researcher reports the findings of the study by bringing the data to life and supporting each finding with participants quotes.

4.10.2 In-depth interview

An in-depth interview is one of the common qualitative data collection methods. It is a purposive conversation with participants that allows for thorough investigation about a phenomenon (Saunders *et al.*, 2011). The in-depth interview was adopted in this study as it allowed for the thorough exploration of how large organisations manage the risks of ITSPs. There are different types of in-depth interviews that are used depending on the purpose of inquiry, this includes structured, semi-structured and unstructured interviews (Saunders *et al.*, 2011). Saunders *et al.* (2011) indicated that structured interviews are used for explanatory or descriptive studies, semi-structured for explanatory and exploratory studies, and unstructured interviews are used for exploratory studies. Since the purpose of inquiry for this study is exploratory and descriptive, the semi-structured in-depth interview was used.

A Semi-structured in-depth interview is a type of interview that allows for thorough discussion about a complex phenomenon or research problem using a systematic approach (Marshall *et al.*, 2014). It allows researchers to unpack and explore a participants' view about a research phenomenon or problem (Saunders *et al.*, 2011) by asking participants open-ended questions and then probing where necessary in order to collect key rich data to answer the research questions (Marshall *et al.*, 2014). The semi-structured in-depth interview was used for this study because it allowed for systematisation and control when exploring how large organisations within South Africa manage the risks of ITSPs. A total of 12 semi-structured in-depth interviews were conducted. The duration of the interview sessions ranged between one and two hours and were recorded with the participants' consent and approval to capture every detail of the interview. Notes were taken to highlight important points or areas that needed clarification or probing.

4.10.2.1 Interview guide approach

There are three approaches to conducting in-depth interviews, which are the informal conversation, the interview guide approach and standardised open-ended interview (Patton, 1987). The informal conversation is an unstructured way of eliciting information from participants; here, questions are spontaneous and are driven by the participants' context. The interview guide approach is a semi-structured manner of extracting information; here, the researcher asks the participants predetermined open-ended questions and probes further to gather more useful data for the research. Lastly, the standardised open-ended interview is structured; the researcher drafts a set of open-ended questions that participants respond to sequentially. For this study, the interview guide approach was adopted for consistency purpose across all study site.

The interview guide approach is the crafting and use of an interview schedule (a document that comprises of predetermined questions) to guide the interview process of a study. The interview guide approach is used to establish some degree of consistency and systematisation in a multiple case study (Marshall *et al.*, 2014). Since the multiple case study was adopted for this study, the interview guide approach was appropriate to effect some degree of consistency and systematisation in the interview process across all study sites. While the interview guide approach brings about structure to the interview process, the exploratory objective of the study was preserved by making the question and answer process flexible such that participants were allowed to skip some of the questions they feel have already been addressed from previous responses and additional questions evolved from probing some of their responses.

4.10.2.2 Interview schedule

The interview schedule is a document used by a researcher to guide an interview process (Morehouse, 1994). It could comprise of different types of questions including fixed alternatives, open-ended and scale items (Kerlinger, 1970), which could be grouped into sections of different criteria such as experience, demographics, knowledge and descriptive (Patton, 1980). The questions in the interview schedule of this study were crafted in line with the research framework that was adopted to guide the data collection process. A pilot study was conducted with two risk practitioners to assess the coherence of the questions to the research framework and the clarity of the questions. The questions were revised according to the feedback received from the pilot study and received approval from the University of KwaZulu-Natal (UKZN) Ethics Committee.

The interview schedule (see Appendix C) comprised of fixed alternative and open-ended questions that was grouped into three sections, as follows:

a) ***Job & Experience*** **–** this section comprised of job-related questions, which gave an insight into the participants' role and experiences in managing ITO risks in their organisations. In addition, questions about the participants' qualifications in terms of certification and training were incorporated in this section.
b) ***Risk management practices in ITO*** **–** this section comprised of questions about the risk management practices of ITO. These questions were mainly focused around how the four common risks of ITSP (identified to be operational risks, business continuity risks, information privacy risk and compliance risks) are been managed in large organisations in South Africa. These questions allowed the researcher to explore how large organisations identify, assess and treat the risks of ITSPs.
c) ***General risk management practices*** **–** this section comprised of general risk management practice questions. These questions focused on how large organisations ensure effective risk management of ITO risks, and the role of stakeholders in enabling and ensuring effective ITO risk management.

4.10.3 Interviewing strategy

For this study, the elite interviewing was used as the strategy to conduct the in-depth interviews. According to Marshall *et al.* (2014) elite interviewing involves conversing with "elites". Elites are professionals with specific expertise in a certain domain. They are usually prominent and influential in their organisation or environment. Interviewing elites come with benefits, such as access to valuable information about the research phenomenon or problem, and acquisition of detailed and comprehensive representation of their organisation, which is usually the research study site. However, there are challenges involved with interviewing these calibre of people as they are usually difficult to access or contact because they are usually busy people who work under demanding time constraints within their organisation. They are usually in control and want to be in control in what they do, which requires that the researcher dance to their tune. For this study, the participants included executives, directors and managers in the study site, who have earned different certification in domains around IT risk, security and governance, and are involved in IT policy-making and management in their various organisations. In order to manage the challenges involved in interviewing these set of participants, the researcher did the following.

- Distributed the research proposal on a professional social media such as LinkedIn.
- A request for participation proposal was sent to potential participants' email through professional certification body like the Information Systems Audit and Control Association (ISACA).
- Connected to participants through referrals from colleagues in their organisation.
- Fixed an interview schedule at the participants' convenience. Some interviews were conducted on weekends as requested by the participant.
- Re-confirm participants' availability a day before the interview schedule.
- Allowed participants to choose the medium of the interview. Some interviews where face to face and others were internet-mediated such as Skype and WhatsApp call.
- Interview schedules and other research documents were sent to participants a few days prior to the interview, so as to make them aware of the area and scope of inquiry and to familiarise themselves with the questions. This approach is referred to as the interview guide approach **(Marshall *et al.*, 2014)**.

4.11 Data quality

In any study, an essential issue to be considered during the course of the study is that of data quality. In quantitative research, internal and external validity, reliability, and objectivity are criteria for data quality, while in a qualitative research, trustworthiness criteria, which includes credibility, transferability, confirmability and dependability are used to ensure data quality (Lincoln *et al.*, 1985). According to Erlandson (1993, p. 132), "trustworthiness is established in a naturalistic inquiry by the use of techniques that provide truth value through transferability, consistency through dependability, and neutrality through confirmability". In order to demonstrate data quality, avoid bias and increase the trustworthiness of the data collected in this study the following were considered:

4.11.1 Transferability

Transferability is a way of achieving generalisation in a qualitative research. Although, generalisation is said to be limited in qualitative studies, however, the research methods and context need to be explicit enough in order for the reader to determine the adoptability of the study in their own context. Erlandson (1993) and B. Berg (1998) recommended that thick description and purposive sampling are ways of increasing transferability of a qualitative research. Thick description aids transferability as it requires for the explicit definition of the research methods, perspectives and context of the study. The purposive sampling adopted for this study increases transferability by allowing the researcher to select only specific experts who have experience around the research phenomena or questions.

In this study, thick description and purposive sampling were used to increase the transferability of the study. The methodologies, scope and context of the study were explicitly described and only staff who have experience in the risk management of ITO in the study site were engaged as participants of the study.

4.11.2 Credibility

Credibility is the degree of confidence that the findings of a study are true and accurate. According to Lincoln *et al.* (1985), the methods that could be used to increase the credibility of a study are persistent observation, prolonged engagement, member checking and triangulation. Persistent observation requires that the researcher identify the characteristics that are most relevant to the objective of the study and focus on them. Prolonged engagement demands that the researcher spends sufficient time engaging the respondents in order to increase the rapport and trust between both parties. Member checking is the participants' validation of a researcher's inferences. Triangulation is the simultaneous use of different types of research elements such as data sources, methods or theories in verifying and proving the accuracy of the findings of the study.

In this study, member checking was used to increase the credibility of the research findings. According to Lincoln *et al.* (1985), it is a method used by researchers to increase the trustworthiness of the results of a study by returning the analysed data or findings to respondents to check for validity. Member checking was applied in this study by sending the analysis of the interviews back to the participants to give feedback on areas of agreement and divergence.

4.11.3 Confirmability

Confirmability is the extent to which the findings of the study is neutral and not influenced by the researchers' bias, interest or motivation (Lincoln *et al.*, 1985). According to D. Cohen *et al.* (2006), confirmability can be assured by providing an audit trail, which is the archiving of all materials and instruments used during the investigation. In order to ensure the confirmability of this study, the following have been securely archived for record and recall purposes:

a) ***Raw data*** – all raw data, field jotters and interviews records.
b) ***Data reconstruction products*** – notes from coding the interviews transcripts, findings and conclusions and a final report including connections to existing literature and an integration of concepts, relationships, and interpretations.
c) ***Process notes*** – all jottings relating to the methodology (procedures, design plan and rationale), trustworthiness notes (pertaining to credibility, dependability and confirmability) and audit trail notes.
d) ***Materials pertaining to study purpose and dispositions*** – including the researcher's jottings on personal thoughts, expectations and motivation.
e) ***Instrument development information*** – pilot interview schedule and versions of the revised interview schedule.

4.11.4 Dependability

Dependability is the extent to which the study is consistent and repeatable. One of the major ways of improving the dependability of a study is through an external audit (Lincoln *et al.*, 1985). An external audit is having an independent researcher review the methods and activities used in achieving the objective of the study. In order to assure the dependability of this study, an independent researcher (selected based on experience and expertise in qualitative research) examined the research process, which includes the analysis of the interviews, findings and conclusions. The examination was to evaluate the accuracy and coherence of the interviews, findings and conclusion.

4.12 Data analysis

Data analysis is the process of extracting meaningful information from a data corpus. The data collected for this study were analysed using the thematic analysis. The thematic analysis is a qualitative analytic/analysis method used by researchers to gain insight and generate knowledge from a qualitative data set (Braun *et al.,* 2006). Using the thematic analysis for this study, the collected data from the interviews were analysed and reported in sections of identified patterns known as themes.

The thematic analysis could be inductive or deductive in approach. The deductive approach is the use of a theoretical framework to inform and guide the generation of codes and themes from a dataset; while the inductive approach, is content driven, such that the codes and themes are generated from the dataset and not underpinned by a theoretical framework. The inductive analysis is deemed appropriate for this study as it allows the researcher to explore the interview transcript without using a defined framework, hence, facilitating the development of a governance framework for ITSPRM.

4.12.1 Data analysis phases

The six steps of conducting qualitative data analysis as identified by Strauss *et al.* (1998) and Braun *et al.* (2006) was adopted for this study. These steps are as follows:

a) ***Familiarisation with the data*** – this is the process of associating oneself with the collected data. According to **Lacey *et al.* (2001)** a researcher is required to get acquainted with the collected data so as to have an in-depth understanding of the data. Researchers can achieve this by transcribing the interviews themselves and re-reading the data corpus/set over again **(Lacey *et al.,* 2001)**. Should the researcher outsource the transcription of the interviews, then they have to crosscheck the accuracy of the transcript by listening to the interview when reading the transcript. To have in-depth knowledge of the dataset of this study, the researcher transcribed the interviews, and read the interview transcript repeatedly.

b) ***Coding –*** this is the generation and extraction of ideas, patterns and relationship from the data corpus/set (Saldaña, 2015). The generation of ideas, patterns and relationships should be driven by the research objectives or questions and labelled for better understanding. This process could be done manually or facilitated by a qualitative data analytics software such as NVivo or Atlas (Saldaña, 2015). In this study, NVivo was used to facilitate the generation of labels that identify important features of the data relevant to answering the research question. After coding the interview transcripts, relevant codes and excerpt were collated.

c) ***Searching for themes*** – this is the process of reviewing the generated labels for a broader meaning. At this stage, some irrelevant labels are discarded while redundant labels are merged and given higher-level descriptions as temporary themes. In this study, initial labels were examined for redundancy, irrelevancy and relationships. The revised labels were renamed as candidate themes.

d) ***Reviewing themes*** – this is the process of examining the candidate themes to determine if they need further revision by refining, splitting, combining or discarding. For this study, candidate themes were examined for appropriateness. Mind maps and hierarchical chart were used to conceptualise the pattern and relationships between the candidate themes.

e) ***Defining and naming themes*** – this is the final check on the appropriateness of the themes and their relationships. At this stage of this study, candidate themes were re-examined for appropriateness and final themes and sub-themes of the study emerged. A detailed analysis of the themes was composed in relation to how they answer the research questions.

f) ***Writing up*** – this is the process of composing a discursive narrative of themes in relation to the study's objectives and existing literature. In this study, the analysis of the emerging themes was discussed using existing literature on ITO risk management and risk management practices from other domains.

4.12.2 Coding the dataset

Coding is the use of labels to identify patterns or meaning in a dataset. According to Saldaña (2015) coding could be done in two phases, the first cycle and second cycle coding. The first cycle coding is the preliminary labelling of ideas or patterns from the dataset as relating to the research questions or objectives. The second cycle coding is the categorisation and conceptualisation of the labels identified in the first cycle coding towards the development of a theory or framework. Figure 4-2 illustrates the sequence of how the codes were used to generate the themes and framework.

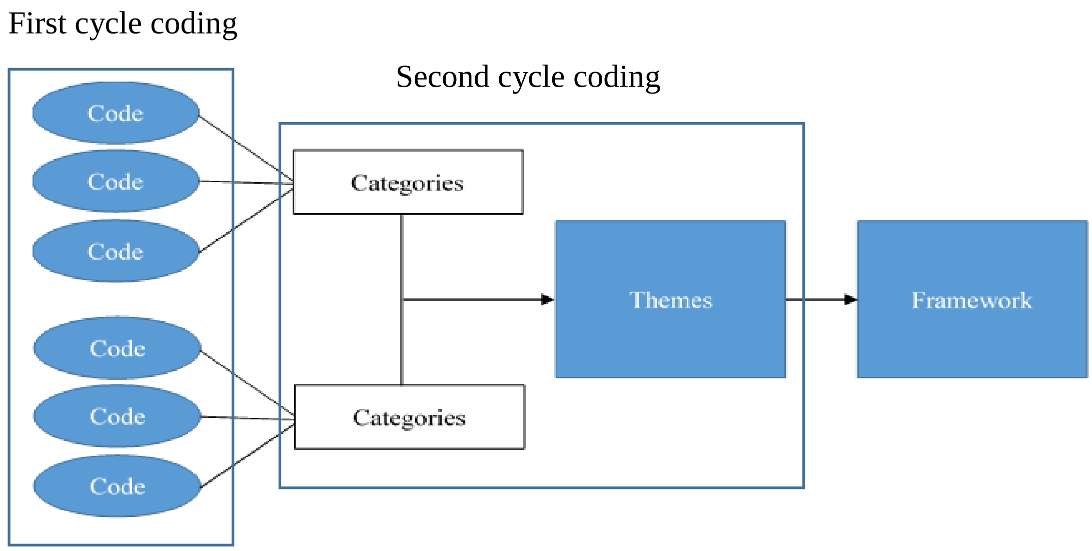


Figure 4-2: Data analysis process

4.12.2.1 First cycle coding

There are different coding methods such as in vivo coding, initial coding, and value coding that could be adopted during first cycle coding. These methods are used to identify and present labels from a dataset that are related to the research questions and objectives. The choice of the coding method to use is determined by the researcher's worldview, paradigm, research methods or approach. According to Saldaña (2015), a single coding method or multiple coding methods (hybrid coding) could be adopted during the first cycle coding.

In this study, the hybrid coding (combination of initial coding, process coding and in vivo coding methods) was adopted in identifying and presenting ideas and patterns generated from the interview transcripts. The initial coding, previously known as open coding (Saldaña, 2015), is an open-ended review of a qualitative dataset that requires the researcher to be open to all possible theoretical directions generating from the dataset (Charmaz, 2006). The process coding is the search for ongoing actions and processes in the interview transcript and allows for the use of gerund (-ing words) in a label (Corbin *et al.*, 2008). The in vivo coding, also known as the verbatim coding requires the use of participants' terminologies and phrases as a label. The combination of these three coding methods allowed for the identification, preservation and presentation of activities, dimensions and practices on how large organisations manage the risks of ITSPs towards developing a framework or theory (Saldaña, 2015).

4.12.2.2 Second cycle coding

The second coding cycle is a high-level coding phase that requires the analytical and conceptual knowledge of the researcher in categorising and thematising the labels generated during the first cycle coding (Saldaña, 2015). There are different methods such as the pattern coding, focused coding and axial coding that could be used for the second cycle coding (Saldaña, 2015). These methods serve the same purpose but are implemented differently.

In the study, the axial coding method was used in the second cycle coding. Axial coding is the re-categorisation of the labels with similar features or properties such as dimensions and activities that were generated from the first cycle coding (Charmaz, 2006; Corbin *et al.*, 2008). The axial coding method was adopted in this study because it allowed for the categorisation and conceptualisation of the practices and activities large organisations use in managing the risks of ITSP, which guided the generation of the themes and the framework of the study.

4.13 Theoretical Framework

This study adapted the ISO 31000 Risk Management Framework (ISO, 2009) in order to explore how large organisations manage the risks of ITSPs. The Framework serves as the basis to most risk management studies (Aris *et al.*, 2008; Syed *et al.*, 2007) and practices (ISACA, 2017; King III, 2009; Prince 2, 2017), and has evolved based on different context and domain. Using this Framework, the process of identifying, assessing and treating the risks of ITSPs in large organisations within South Africa was explored and presented. The Framework consists of three main constructs, which are risk identification, assessment and treatment.

1st Construct – Risk Identification – This is the first step in most Risk Management Framework (Fan *et al.*, 2012; IRM, 2002). The process of risks identification helps to reveal the what, when and how questions about risks, threats and vulnerabilities. This construct allowed for the investigation of how large organisations identify potential risk factors, threats and vulnerabilities of ITSPs.

2nd Construct – Risk Assessment – Risk assessment is the process of analysing, evaluating and ranking risks according to their probability of occurrence and impact

(Gary *et al.*, 2002; ISO, 2009). This construct allowed for the investigation of how large organisations analyse the probability of occurrence and the impact of ITSP's risks.

3rd Construct – Risk Treatment – This process encompasses the management strategies involved in bringing risk to an acceptable level (Gary *et al.*, 2002; ISO, 2009). This construct allowed the researcher to investigate the strategies and methods organisations use in addressing ITSP's risk.

4.14 Ethical issues

The ethical approval to conduct this study was obtained from the Ethics Research Committee of the University of KwaZulu-Natal. A Gatekeeper's letter was obtained from the two organisations used as study sites. Participants were given an introduction and informed consent letter to notify them of the objectives of the study and inform them that their participation is voluntary and can withdraw at any point of the interview if they feel uncomfortable. The participants' privacy, anonymity and confidentiality were preserved by not associating them with any organisation and using a pseudonym when presenting their narrations in the findings section.

4.15 Conclusion

This chapter presented the researcher's worldview, research methodology and design, sampling techniques and analysis methods that was used to achieve the objectives of the study. The research protocol and criteria were carefully selected and carried out in a systematic way. The exploratory case study design and qualitative method were used in exploring how large organisations in South Africa manage the risks of ITSPs. Qualitative data were collected using interviews, and the purposive and snowball sampling were used to select the right participants that were interviewed to collect rich data to answer the research questions. The NVivo data analysis software was used to facilitate the thematic analysis of the interview transcripts. The findings and discussion from the analysis are presented in the next chapter. The next chapter also present the framework that was developed from the findings of the study.

CHAPTER 5: PRESENTATION AND DISCUSSION OF FINDINGS

5.1 Introduction

The preceding chapter presented the research methodology and data analysis techniques used in this study. As indicated in chapter one of this study, this study focuses on ITSP's risks of ITO because these risks are the most severe and common risks of ITO, as identified in the literature. This chapter presents the findings and discussion on how large organisations identify, assess and treat the risks of ITSPs. This chapter is divided into three sections as illustrated in Figure 5-1. The first section expands on the theoretical framework underpinning this study. The second section presents the demographics of the participants of this study. The last section presents the findings of the study in relation to achieving the objectives of the study.

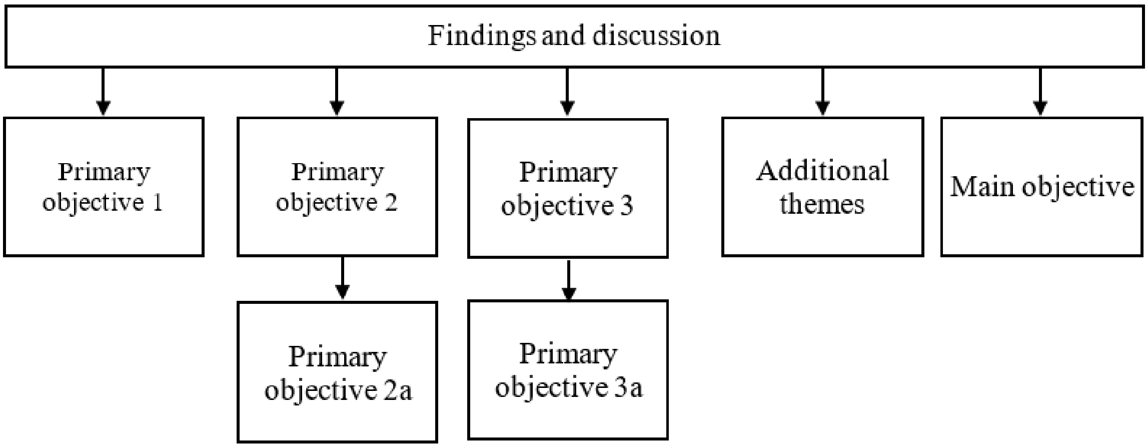


Figure 5-1: Structure of chapter

5.2 Findings and discussion

This section presents the findings of this study, as well as the discussion around the findings of this study. The section also addresses the objectives of the study in relation to the analysed data. As such, the main themes and their respective sub-themes relating to the primary objectives of this study were first presented, followed by the additional themes that emerged from the analysis. These themes, in relation to the primary objectives of this study, were further used to discuss and address the main objective of the study.

As presented in the chapter one of this study, below are the objectives of this study.

The main objective of this study is:

- To propose an IT Service Provider Risk Management Framework that can help organisations effectively manage IT Service Provider's risks.

In order to achieve the main objectives, the primary objectives are:

1. To explore how large organisations identify IT Service Provider's risks.
2. To understand how large organisations assess IT Service Provider's risks.
    a. To highlight the impacts of the four common IT Service Provider's risks on large organisations.
3. To understand how large organisations treat IT Service Provider's risks.
    a. To explore the mitigating controls large organisations, have in place to manage IT Service Provider's risks and highlight the controls to manage the four common risks of ITO.

5.3.1 Primary objective 1

To explore how large organisations identify IT Service Provider's risks

To achieve this objective, participants were asked questions about how ITSP's risks are being identified in their organisation. From the analysis of the participants' responses, it was understood that in any ITO engagement, there are three types of ITSP's risks that needs to be identified. These risks are *inherent risks*, *current risks* and *residual risks*. Table 5-2 presents the description of these risks as defined in the Certified in Risk and Information Systems Control Review Manual (ISACA, 2017). Further analysis of the interview shows that the three types of ITSP's risks are often identified at different stages of the ITO risk management process. The inherent risks are often identified at the initial stage of the ITO initiative; the current risks are often identified during the risk assessment phase; and the residual risks are often identified after treating the current risks of the ITSP. The risk identification process presented in this section focuses on identifying inherent risks of the ITSPs. The risk identification process in identifying the current and residual risks of ITSPs will, however, be presented in the section that discusses the assessment and treatment of ITSP's risks

Table 5-2: Description of the three types of ITSP risks

Types of ITSP risks	Description
Inherent risks	These are the default risks, vulnerabilities and threats associated with outsourcing an IT service.
Current risks	These are the present risks associated with outsourcing an IT service.
Residual risks	These are the risks left after risk response strategies have been applied on the inherent and current risks

As illustrated in Figure 5-2, four sub-themes emerged under the identification of ITSP's risks. These sub-themes and their relationship to this study's objectives are presented below.

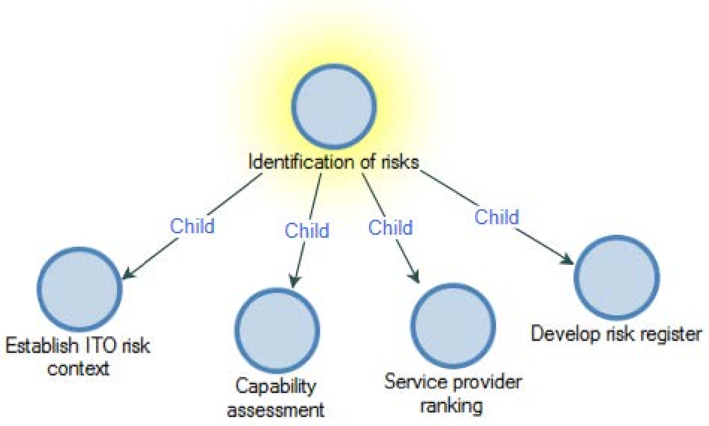


Figure 5-2: Identification of ITSP's risks

5.3.1.1 Establish Information Technology Outsourcing risk context

Participants of this study explained that establishing ITO risk context is important because it involves and initiates the process of defining the risk criteria and parameters needed for risk management. This explanation is in line with the study of H. Berg (2010), where it was identified that establishing a risk context is the preliminary stage in the management of risk. Establishing risk context is essential because it allows for the determination of the scope of the risk management process. It also helps to determine the risk criteria, which must be determined on the outset of any risk management endeavour

As illustrated in Figure 5-3, two sub-themes emerged as important criteria in establishing an ITO risk context. These sub-themes are presented below.

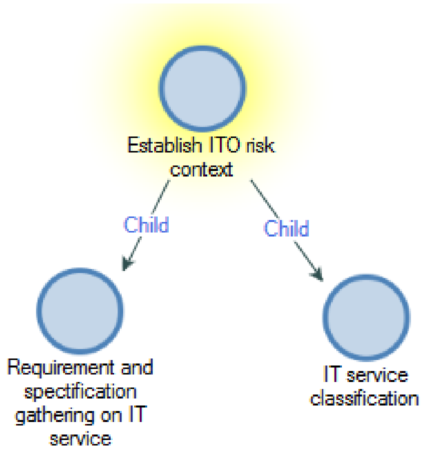

Establish ITO risk context
Child
Child
Requirement and specification gathering on IT service
IT service classification

Figure 5-3: Establish ITO risk context theme

<u>Requirement/specification gathering</u> – the findings of this study shows that it is important that organisations collect and analyse the requirements/specifications of the IT services to be outsourced to establish the context of the ITO initiative. As identified by this study's participants, some of these requirements/specifications includes the department/users of the IT services to be outsourced, the expected time of delivery of the IT services from the ITSP, the criticality of the services to the organisation, and the amount of risk the organisation is ready to accept while using the service. According to one of the participants, after collecting these requirements/specifications, organisations

> *"…are required to review the gathered information so as to identify possible risk criteria and parameters that will define the scope of the ITO risk management process." (MaPart1)*

During the interviews, participants identified different methods of gathering the requirements/specification of the IT service to be outsourced. Some of the methods identified are brainstorming and roundtable discussions. Roundtable discussions was, however, the most mentioned method. Participants of this study indicated that stakeholders in the organisation that require the IT service to be outsourced should be invited to a roundtable discussion to understand and document the service requirements and scope. The roundtable discussion is also considered effective by participants because, it by its nature involves stakeholders of the organisation. The use of a roundtable discussion to gather information is related to the risk-focused meeting method identified in the risk identification and assessment methodologies for security regulators report by the Board of the International Organisation of Securities Commissions (OICV-IOSCO, 2014). In this report, regulatory authorities are advised to conduct risk-focused meetings and maintain a regular dialogue with key market participants to identify new and emerging risks from the financial market, and possibly, through this means, find ways of mitigating these risks. Brainstorming is also used to facilitate risk identification; however, it is more of an idea generation tool for a small group of personnel (S. Paul, 2011).

Service classification – as part of the process of establishing the context of ITO, participants indicated that it is essential to classify the IT services to be outsourced into level of criticality. The classification of IT services, according to one of the participants,

> *"…will help in identifying the priority that needs to be associated with the service. This will then inform the type or level of assessment that needs to be conducted. It will also inform the risk response preference that should be associated with such services" (OpPart3)*

The classification of IT services, as found in this study to being important in establishing the context of ITO, is similar to the support ticketing scheme used by Kayesa (2016) for customer service management. Kayesa (2016) classified customer support into four levels - critical impact, significant impact, normal/minor impact, low/informational impact. This classification allows for the timeous and cost-effective management of customers' queries.

5.3.1.2 Capability assessment

Capability assessment is the process of examining the competence of an entity in achieving an objective. Many of the participants indicated that the competency of potential ITSPs be examined using the service requirements/specifications as a benchmark. This examination allows the Committee to identify the strengths and weaknesses of each potential ITSPs in the delivery and maintenance of services. The weaknesses of each potential ITSP should then be recorded as possible risk factors, threats and vulnerabilities that will be associated with outsourcing the IT service the ITSPs. This is similar to the capability assessment policy of the Northern Virginia communities, in the USA. In this policy, the technical, administrative, fiscal, and planning and regulatory capabilities of the communities in Northern Virginia are to be assessed based on an established framework in order to identify the gaps, weakness and threats that will hinder achieving the communities' objectives (NOVA, 2010). The assessment of capabilities, as identified in this study's analysed data, also allows for the identification of already established controls that needs to be tested for effectiveness.

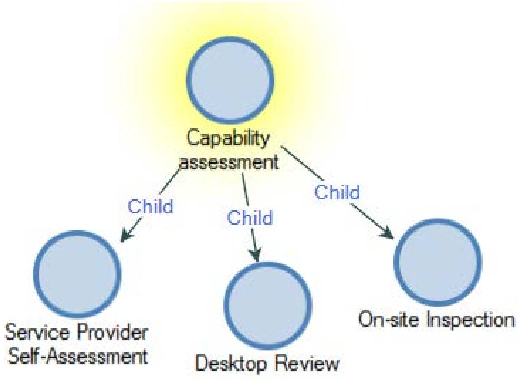


Figure 5-4: Capability assessment theme

As illustrated in Figure 5-4, three sub-themes emerged under the capability assessment theme. These sub-themes represents the activities involved in conducting capability assessment of potential ITSPs. According to participants of this study, these activities are sequential. With the first being service provider self-assessment, followed by a desktop review, and then an on-site inspection. These activities are presented below:

Service provider self-assessment – a self-assessment exercise is the process where potential ITSPs evaluate their ability to deliver required services. Participants indicated that it is important to subject potential ITSPs to self-assessment exercises using questionnaires and requesting for supporting documents. According to one of the participants,

> *"…the questionnaires should comprise of risk related questions guided by the requirements of the IT service to be outsourced."* (OpPart3)

The self-assessment exercise helps organisations obtain competency related information from potential service providers. The subjection of service providers to self-assessment identified in this study is related to the service provider validation process of the Payment Card Industry Data Security Standard (PCI DSS) (PCISSC, 2016). This Standard stipulates that organisations must administer questionnaires to service providers, which would grant the organisation access to necessary information to examine the competency of the service provider in delivering payment card services to the organisation.

Desktop review – a desktop review is the examination of information/documents for specific reasons. Many of the participants indicated that it is necessary for organisations to conduct a desktop review of the information/documents gathered from the self-assessment exercise. Hence, the desktop review is considered by most of the respondents as being the next stage of action after the self-assessment is completed. According to one of the participants, it is important to a conduct desktop review because,

> *"…it helps to determine if the potential service provider has the required capability, in form of having good financial background, sufficient resources in terms of people and fund to run the required services, and some sought of track records." (MaPart2)*

The review exercise would help organisations gain insight on the weaknesses of potential service providers. Allowing organisations to establish potential risk factors, threats and vulnerabilities of each potential ITSPs. Conducting a desktop review as a necessary part of risk identification is highlighted in the Federal Contract Compliance Manual of the USA Department of Labour (OFCCP, 2014). In the Manual, auditors and compliant officers are required to examine an entity's supporting documents in order to identify their compliance status to certain standards. It was further indicated in this Manual that areas of non-compliance should be identified as threats and vulnerabilities that needs to be addressed.

Some of the participants of this study identified key areas or terms of reference for conducting desktop reviews of potential ITSPs. The two prominent areas identified are reputational standing and operational viability. To conduct these reviews, some of the documents and information to examine are the financial documents, client attestation, personnel curriculum vitae (CV), security standards, policies and procedures of the ITSP. Reviewing a potential ITSP's reputational standing would provide an insight on the quality of service obtainable from the ITSP. Likewise, reviewing operational viability would demonstrate the competence of the ITSP in delivering the service adequately. These key areas indicated by the participants of this study are similar to the key factors to consider when selecting a service provider as identified in the study of Aris *et al.* (2008). In the study, nine factors must be consider when selecting a service provider.

These factors include the ITSP's experience, reputation and performance, personnel expertise, usage of third-party supplies, access to latest technology, standard, policies and procedures practices, security practices, responsibility towards disaster recovery plan, and financial stability. All of these factors identified by Aris *et al.* (2008) could be categorised under the operational viability, except for reputation and performance which falls under the reputational standing of the ITSP as identified in this study.

On-site inspection – an on-site inspection is the thorough examination of potential ITSP's site. This is considered by most of the respondents as being the next stage of action after the desktop review is completed. Participants of this study indicated that it is important for organisations to delegate a team to visit the site of potential ITSPs' for inspection. According to one of the participants,

> *"...after reviewing potential service providers' proposal, the Risk Committee needs to send out a team to perform an inspection of service provider's site just to verify that the key aspects and the minimum requirements do actually exist." (OpPart4)*

The on-site inspection is a necessary requirement to confirm the status of the capabilities required to deliver the IT service. The need for an on-site inspection in ITO, is also highlighted in a report on IT vendor management (PWC, 2015), where it is recommended that organisations should visit the site of the service provider's organisation as part of the review processes before selecting a service provider. According to Surak *et al.* (2007), the objective of an on-site inspection should be to verify if an entity meets up with stated requirements. Furthermore, its focus should be to find facts rather than faults.

Further analysis of this study's data shows that it is important to define the scope of a site inspection before visiting the ITSP's site. According to one of the participants this is because,

> *"…it would prevent an onerous process for both the organisation and the ITSP, as the inspection exercise will be focused and straightforward" (OpPart5)*

The scope of the site inspection should be determined based on the established ITO risk context and scope of the risk management process. The need to define the scope of a site inspection is also discussed in the study of Bachlechner *et al.* (2014), where auditors are recommended to define the scope of an IT audit before going to client's site. Bachlechner *et al.* (2014) indicated that defining the scope of the IT audit would help to prevent an exhausting engagement. Defining the scope of a site inspection is also linked to the need to develop and use a checklist during inspection (Shawn, 2013). According to Shawn (2013), developing an inspection checklist is a way of defining the scope of the inspection exercise. The inspection checklist helps to focus the inspection exercise to specific requirement, which prevents scope creep. It also serves the purpose of assurance and accountability during an inspection exercise.

5.3.1.3 Service provider ranking

Service provider ranking is the grading of service providers based on certain criteria. Participants of this study indicated that, as part of the risk identification process it is essential to grade potential ITSPs based on the criticality of the service they will be delivering and their degree of risk exposure and response. According to one of the participants, this is important because,

> *"…it will aid the selection of the lowest risk ITSP and determination of the level of assessment to conduct during risk assessment" (OpPart4)*

The importance of ranking service providers is also emphasised in the study of Richard (2009), where it was stated that risk practitioners must rank service provider into tiers of high-risk, medium-risk and low-risk. The author explained that the ranking of service provider is necessary to determine the depth of risk assessment to be conducted. It is also important in the development of the method that will commensurate with the risks involved. David *et al.* (2009) also emphasised that ranking the service providers according to their risk exposure is an appropriate ITSP selection strategy.

5.3.1.4 Develop risk register

From the interviews, participants indicated that as part of the risk identification process, organisations must develop a risk register. A risk register is a structured database of potential risk factors, threats and vulnerabilities associated with an event (Patterson *et al.*, 2002). It is an effective tool that enables structured record keeping of risk-related information such as risk source, classification and current controls of identified risks

(ISACA, 2017). One of the participants indicated that it is essential that organisations record all risk related information in a risk register because,

> *"…the risk register would make it easy to track what has been done and also serve as a guide or point of reference on what next needs to be done." (OpPart5)*

The importance of developing a risk register during risk identification is stressed in the study of Patterson *et al.* (2002), where a risk register management system is recommended as a tool that facilitates the tracking of project risks in the automotive industry. The authors recommended that risk practitioners adopt the use of a risk register as it aids coordination and allows for easy recording, tracking, monitoring and reporting of risks throughout the risk management cycle. The use of a risk register is also emphasised in the King Report on Governance for South Africa (King III, 2009), where it is stated that management must create a risk register for record and reporting purposes.

5.3.2 Primary objective 2

> *To understand how large organisations assess IT Service Provider's risks.*

In order to achieve this research objective, participants were asked questions about how they assess the risks of ITSP. From the analysis, as illustrated in Figure 5-5, four sub-themes emerged under the assessment of risks theme.

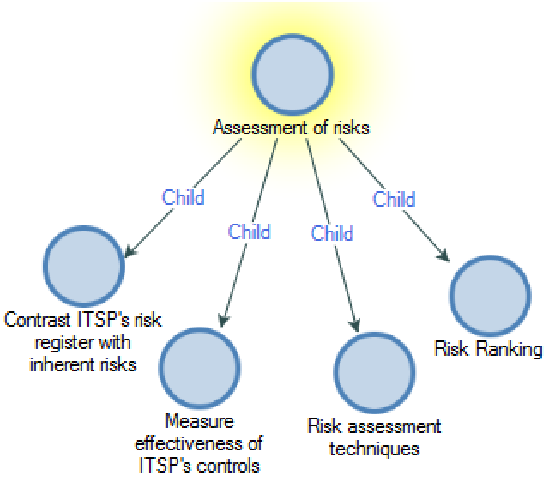

Assessment of risks
Child
Child
Child
Child
Contrast ITSP's risk register with inherent risks
Measure effectiveness of ITSP's controls
Risk assessment techniques
Risk Ranking

Figure 5-5: Assessment of risks theme

The findings of this study showed that the assessment of ITSP’s risks involve a series of examinations and evaluation activities. These activities are explained in the below sub-sections.

5.3.2.1 Contrast ITSP’s risk register with inherent risks

Participants recommended that it is necessary to commence a risk assessment exercise by requesting for the ITSP’s internal risk register and compare it with identified risks. The essence of this comparison is to identify the inherent risks that have been addressed by the ITSP, as well as the available controls used. This allows the organisation to set the basis and priority for the assessment exercise. The concept of comparing the ITSP’s risk register with identified risks was also recommended by ISACA (2017). ISACA (2017) recommends that a risk practitioner should gather valuable information from a third-party’s risk document to guide the dynamics of a risk assessment exercise.

5.3.2.2 Measure effectiveness of Information Technology Service Provider’s controls

Many of the participants of this study indicated that organisations must measure the effectiveness of the ITSP’s controls to identify the current risks of the service provider. The current risks of the ITSP are the present risks that needs to be addressed after considering the effectiveness of the ITSP’s control. Participants of this study identified control testing as an appropriate method to measure the effectiveness of an ITSP’s controls. Control testing is done by simulation and observation. The need to measure the effectiveness of control during risk assessment is emphasised in the CRISC Review Manual (ISACA, 2017), where risk practitioners are requested to assess the current state of controls to identify the present risks that needs to addressed. Vulnerability assessment such as penetration testing is one of the ways identified in the CRISC Review Manual (ISACA, 2017) to assess the current state of controls. Using penetration testing, the risk practitioner is required to simulate a risk event using standard tools or risk parameters and observe the extent to which the control will address the risk event.

Participants of this study indicated that organisations should adopt best practice frameworks such as the COBIT Framework as a baseline for measuring the effectiveness of an ITSP’s controls. This is necessary because best practice frameworks are established standards for implementing effective controls. Similarly, in the study of Bachlechner *et al.* (2014), IT auditors are recommended to adopt a governance framework such as

COBIT in evaluating an ITSP's internal controls. The COBIT Framework is an IT governance best practice framework that comprises of control requirements, specifications and metrics that help to measure the adequacy of controls established to mitigate risks.

5.3.2.3 Risk assessment techniques

As illustrated in Figure 5-6, three sub-themes emerged under risk assessment techniques. Participants of this study emphasised on conducting maturity assessment and BIA in examining the probability of occurrence and impact of an ITSP's risks on an organisation. These techniques are presented below.

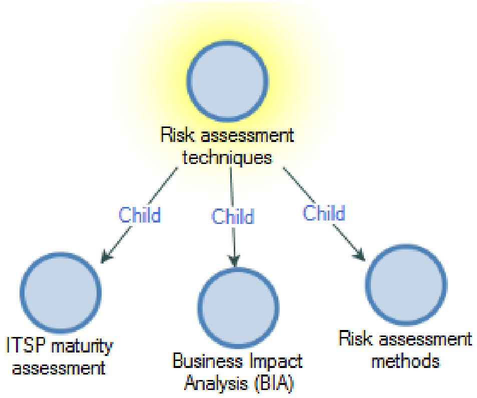


Figure 5-6: Risk assessment techniques theme

<u>ITSP maturity assessment</u> – maturity assessment is the examination of an organisations' progress in terms of capability, competency, and level of sophistication based on best practice standards or models (De Bruin *et al.*, 2005). Some of the participants noted that organisations must examine how an ITSP has matured over time in delivering similar services to other clients. In this regard, organisations will be able to gain insight into how the ITSP has developed and improved the processes and capabilities involved in delivering and maintaining the required IT service. One of the participants explained that:

> *"…examining the maturity of the ITSP in delivering the required service would expose how far and well the ITSP have come in developing and maintaining controls, and also, in dealing with incidents associated with the service. This will reflect on the possibilities of risks occurring in the ITSP's organisation." (MaPart4)*

Maturity assessment models are identified in the study of De Bruin *et al.* (2005) as tools for measuring organisational development. It shows how effective an organisation is in managing risks. ISACA (2017) emphasised that it is essential that risk practitioners evaluate an organisations' risk management program using best practice maturity models. This will give the risk practitioner insight on the organisation's "evolutionary improvement path from ad hoc, immature processes to disciplined, mature processes with improved quality and effectiveness" (ISACA, 2017, p. 86). Some of the key areas to be considered when examining the maturity of ITSP includes support for staff, the existence of policies, procedures and standards, training of staff and availability of a current business impact analysis (ISACA, 2017).

Business impact analysis – BIA is the "process of analysing business functions and the effect that a business disruption might have upon them" (Tjoa *et al.*, 2008, p. 3). Some of the participants of this study indicated that organisations must conduct BIA to evaluate the impact of an ITSP's current risks on the organisation. BIA could be operationalised by analysing the impact of identified risk events on organisational processes and business units, as well as the resultant consequences on the organisation as a whole. Tjoa *et al.* (2008) also identified BIA as an essential assessment used in evaluating how the loss, disruption or interruption of business processes would affect an organisation.

Risk assessment methods – risk assessment method refers to the format of analysing and presenting risk assessment exercises. From the analysis of the interviews, it was understood that the format in which the outcome of a risk assessment exercise is presented is of great significance to effective risk ranking and treatment. This is because the format of presentation contributes to how easy it will be to interpret and understand the outcome of the assessment. Participants of this study indicated that organisations need to define and evaluate risks either in quantitative or qualitative format. One of the participants explained that,

> *"…you have to tie risk back to a monetary amount, to say that a risk below a million rand is medium. In areas you cannot quantify, you qualify to say this is going to lead to bad customer experience, loss return business. This enables stakeholders to understand the outcome of a risk assessment exercise and eases the process of ranking and prioritising risks…" (ExPart2)*

The essence of using an assessment method during risk assessment is highlighted in the study of H. Berg (2010), where risk practitioners are required to analyse and evaluate risks using the quantitative, qualitative or semi-quantitative method. H. Berg (2010) indicated that defining the impact or probability of occurrence of risks in terms of numbers or/and narratives allows for effective ranking and prioritisation.

5.3.2.4 Risk ranking

From the analysed interviews, many of the participants of this study indicated that after assessing ITSP's risks, it is essential to rank risks according to their probability of occurrence and impact on organisation. This is because risk ranking facilitates effective risk treatment. Participants suggested the use of a Risk and Control Matrix (RACM) to facilitate risk ranking. This is because RACM allows for the consolidation and recording of the output of the risk assessment process in one database. The RACM, however, is not only a documentation tool but a decision-making tool, as explained by one of the participants who said that,

> *"…it allows organisations rank and prioritise ITO risks as high, medium or low by cross-tabulating the impact of the risk against the probability of occurrence…the matrix then informs the risk response strategies to be adopted and the order of preference to mitigate risks." (OpPart5)*

The need to rank risks according to their probability and impact is emphasised in the Risk Management Principle and Guideline Manual of ISO (2009). In this Manual, risk practitioners are requested to rank risks according to probability and impact in order to determine the preference in which risks are to be treated. Alexander *et al.* (2006) and Panthi *et al.* (2007) recommended the use of risk matrix to facilitate risk ranking. Panthi *et al.* (2007) noted that the RACM is a simple, yet effective tool that also allows for the systematic documentation of the risk assessment process. Alexander *et al.* (2006) identified risk matrix to be a strategic tool because it allows for the prioritisation of risks and determination of the risk response strategy to adopt.

5.3.3 Primary objective 2a

To highlight the impacts of the four common IT Service Providers' risks on large organisations

To achieve this research objective, participants were asked about the impact of operational risks, information privacy risks, business continuity risks and compliance risks of ITSP on organisations in South Africa. Table 5-3 presents the findings on the impact of the four common ITO risks on large organisations in South Africa as indicated by participants of this study. This finding shows that the impact of the four common risks of ITO is interrelated and severe. The common impacts of these risks are reputational damage and lost revenue, which Catherine (2004) identified as risk consequences that could cause major harm to any organisation.

Table 5-3: Impact of the four common risks of ITO

ITO risks	**Impact on large organisations**	
Operational	• Failure or delay in service delivery • Lost business productivity	• Lost revenue • Reputational damage
Business continuity		
Data privacy	• Litigation	
Compliance	• Regulatory fines • Business failure	

5.3.4 Primary objective 3

To understand how large organisations treat IT Service Provider's risks

In order to achieve this research objective, participants were asked questions about how ITSP's risks are being treated. From the analysis, as illustrated in Figure 5-7, two sub-themes emerged. These are the adoption of risk response strategies and the factors determining the choice of response strategy.

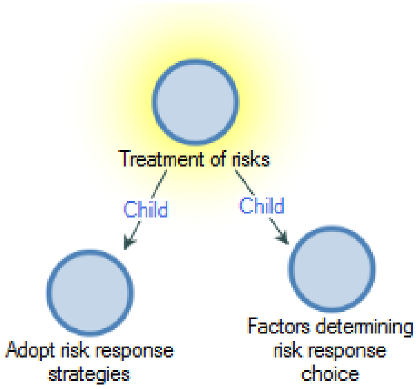

Treatment of risks
Child
Child
Adopt risk response strategies
Factors determining risk response choice

Figure 5-7: Treatment of risks theme

5.3.4.1 Adopt risk response strategies

From the analysis of the interviews, it was understood that organisations treat ITSP's risks by adopting appropriate risk response strategies until the risks are tolerable. These risk response strategies as explained by one of the participants are:

> *"…acceptance, doing nothing to the risk; remediation, to mitigate the probability of occurrence and impact of risk; transference, shifting risk to a third-party; and avoidance, keeping away from the risk..." (ExPart1)*

The adoption of appropriate risk response strategies in treating risk is mentioned in most risk management studies, standards and best practices. According to ISACA (2017), H. Berg (2010) and IRM (2002), risk practitioners are required to treat risks by adopting risk response strategies, which are mitigation, acceptance, transference or avoidance. Mitigation is the use of controls to reduce the probability of occurrence or impact of risk, acceptance is doing nothing to address the risk, transference is moving risk or sharing risk with another entity, and avoidance is boycotting the event that is associated with the risk.

Further analysis showed that organisations could adopt more than one risk response strategy to treat a risk. The concept of adopting more that one risk response strategy to treat a risk is mentioned in the King III Report on Governance for South Africa (King III, 2009). It was stated in the Report that the board of directors could integrate different risk response strategies in order to ensure that risks are appropriately treated or brought to an acceptable level.

5.3.4.2 Factors determining risk response choice

From the interviews, participants identified factors that determines the choice of risk response strategies. As illustrated in Figure 5-8, choosing a risk response strategy should be determined by the outcome of the risk assessment exercise and the risk tolerance and appetite of the organisation. These sub-themes are presented below.

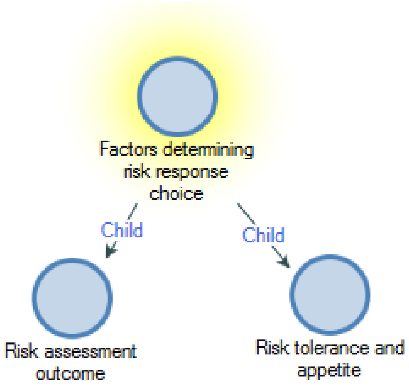

Factors determining risk response choice
Child
Child
Risk assessment outcome
Risk tolerance and appetite

Figure 5-8: Factors determining risk response choice theme

Risk assessment outcome – responses from participants of this study showed that senior management relies on the outcome of the risk assessment process to decide on the risk response strategy to adopt. One of the participants expatiated on this point using a possible occurrence of a Tsunami, as an example of risk an organisation in Durban needs to assess; he explained that:

> *"…due to the low chances of Tsunami occurring in Durban, the organisation may decide to ignore the risk of Tsunami happening. However, because of the high impact of Tsunami they may adopt mitigating strategies from areas that have experienced [a] Tsunami before" (Expart1)*

This explanation implies that organisations need to give necessary attention and adequacy to the assessment of ITSP's risk because it determines the adoption of appropriate risk response strategies. The significance of risk assessment outcome in selecting appropriate risk response strategy is demonstrated in the studies of Panthi *et al.* (2007) and Alexander *et al.* (2006), where a risk matrix developed during the risk assessment phase is leveraged in selecting the appropriate risk response strategy. In these studies, the risk matrix is developed as a four-quadrant graph with the probability of occurrence on the y-axis and impact of risk on the x-axis, as illustrated in Figure 3-5. According to Panthi *et al.* (2007) and Alexander *et al.* (2006), this graph could be leveraged to find the appropriate risk response by plotting each risk on the graph. Any risk that falls on the left two quadrants should be accepted, on the top-right quadrant should be avoided, on the bottom-right quadrant should be transferred, and anywhere on the mid-point of the impact axis should be mitigated.

Risk tolerance and appetite – risk tolerance is the "acceptable level of variation that management is willing to allow for any particular risk" (ISACA, 2017, p. 20) and risk appetite is the "amount of risk an entity is willing to accept in pursuit of its mission" (ISACA, 2017, p. 19). Many of the participants of this study indicated that the risk tolerance and appetite of an organisation must be considered when deciding on the risk response strategy to adopt. According to one of the participants,

> *"…the risk tolerance or appetite of an organisation, which could be in the form of monetary value should guide on if to accept or mitigate risk" (ExPart2)*

The need to consider the risk tolerance and appetite when selecting risk response strategy is consistent with the study of Prince 2 (2017), where project managers are recommended to consider the project appetite when selecting risk response strategy in project risk management. As stated by Prince 2 (2017), project managers are required to be aware of how much risk could be afforded or how much loss is acceptable during the course of a project. Project managers are recommended to accept and monitor risks that are below project risk tolerance, mitigate or share risks above project risk tolerance or avoid the risk if it is way beyond the project risk tolerance level (Prince 2, 2017).

5.3.5 Primary objective 3a

> *To explore the mitigating controls large organisations, have in place to manage IT Service Provider's risks*

In order to achieve this research objective, participants were asked about the mitigating controls available to reduce the probability of occurrence and impact of an ITSP's risks on organisations. From the analysis, two sub-themes emerged, as illustrated in Figure 5-9. The findings of this study showed that there two types of mitigating controls organisations use in managing the probability of occurrence and impact of ITSP's risks. These mitigating controls are technical and administrative controls. These controls are presented below.

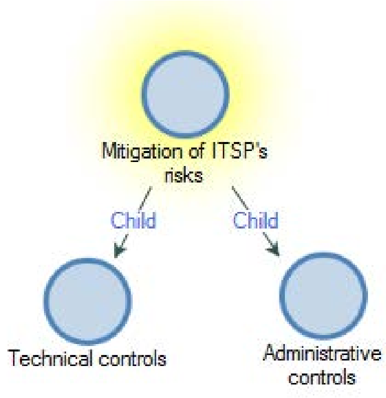


Figure 5-9: Mitigation of ITSP’s risk theme

5.3.5.1 Technical Controls

Technical controls are usually operational and technology-related measures (ISACA, 2017). The analysis of the interviews showed that most technical controls large organisations implement are focused on mitigating ITSP’s risks relating to data security, business operations and business continuity. Some of the technical controls identified by participants are presented below.

- ***Contingency Planning*** **–** is a fall-back arrangement in the case an actual plan fails. From the interviews, contingency plans are used to reduce the impact of ITSP’s risks on organisations. Participants indicated that organisations should make provision for contingency plan most especially if the service is critical to the organisation. Some of the contingency plans participants highlighted include developing in-house IT capabilities or secondary sites, and contracting multiple service providers or having a standby service provider. Contingency planning is recommended in the studies of Kleindorfer *et al.* (2005) and Tomlin (2006) as an effective mitigation technique. Kleindorfer *et al.* (2005) indicated that contingency plans such as backup systems increase the level of readiness to mitigate the impact of a disruptive risk. Tomlin (2006) suggested that contingent rerouting, a strategy of sourcing from two suppliers at different volumes is an effective way of mitigating disruption risk as it reduces cost and increases the time of recovery.

- ***End to end encryption (E2EE)*** **–** is a secured mechanism that enciphers the data transmitted between two-communication ends. Many of the participants indicated that organisations should ensure that the data communication channel between their organisation and the ITSP is encrypted. This will help to reduce the impact of information security threats such as hackers and malwares on the organisation. The intruder will only have access to the cipher text, which will not be readable or useful. The use of E2EE to manage information security threats is one of the recommendations made in the study of Zissis *et al.* (2012). Zissis *et al.* (2012) recommended that the use of cryptography to facilitate end-to-end communication between an organisation and a third-party is an ideal solution in preserving the integrity, confidentiality and authenticity of data.

- ***Network segmentation*** **–** is the partitioning of a large network into sub-networks to increase performance and security. Participants suggested that organisations must ensure that their corporate network is segmented into sub-networks. These sub-networks should be configured with security measures that commensurate the criticality of the systems and data residing on each sub-network. According to participants, network segmentation will reduce the impact of intrusion on the organisation should their systems or a service provider's network is compromised. Becky (2017) suggested that organisations must segment their network to harden the networks' security and secure confidential data from hackers and malwares. The author further noted that network segmentation is one of the popular threat mitigation mechanism organisations should have in place to protect corporate information from curious insider, customers and suppliers.

- ***User access management tools*** **–** are systems/applications that manages the privilege and rights users have on a network/service. Some participants recommended that organisations deploy user access management tools such as Active Directory, Microsoft New Technology File System (NTFS) security and Security Inventory Management (SIM) tools to implement least privilege policy. According to participants of this study, implementing a least privilege policy would ensure that ITSP's personnel do not gain access to confidential information. The use of user access control systems in mitigating information risks is supported by the study of Gusmeroli *et al.* (2013), where it is indicated that a user access control is an effective measure to mitigate the risk of cyber threat. In another study, Gabor (2017) indicated that it is essential for organisations to control and monitor the access of third-party service providers on their corporate network by giving them access to only the information they require to deliver their services using a privileged access management system. This is because cyber attackers usually exploit the service provider's access to get to their client's system or network.

5.3.5.2 Administrative controls

Administrative controls are managerial strategies such as policies and standard operation procedures devised by organisations to enforce certain business practices (ISACA, 2017). From the interviews, it was understood that administrative controls serve as a deterrent control that discourages the ITSP from failing to deliver the IT service as required. According to participants, organisations must design and implement different forms of administrative controls to reduce the probability of occurrence and impact of ITSP's risks on the organisation. Some of the administrative controls identified by participants are presented below.

- ***Contractual agreement*** – A contract is a written agreement between an organisation and an ITSP. Many of the respondents of this study indicated that organisations must ensure that a comprehensive contract of mutual benefits between the organisation and the ITSP must be drafted and signed by both parties. The signed contract serves as a deterrent control that would compel the ITSP to work within an acceptable level of risk. The contract will also serve as a regulator and a point of reference should the service provider plan to or defaults the contract terms. The use of a contractual agreement as a mitigating control was discussed in the study by Vasant *et al.* (2017), where contract agreement is identified as an essential administrative control for mitigating ITO risks. The authors suggested that the approach to contract negotiation should be on the basis of mitigating ITO risks. Furthermore, all required details regarding the service level must be documented in the contract and signed by both parties for reference purposes.

- ***Service level agreement*** **–** is a statement that defines the expected level of service to be received by a client. Participants of this study referred to the SLA as a deterrent control that prevents the service provider from defaulting the contract terms. Participants also indicated that organisations must ensure that an elaborate

SLA is included in the contract. The SLA must stipulate the performance metrics of the agreed level of service, and must include how and when the service must be delivered. The inclusion of an SLA in an ITO contract is similarly emphasised by Sue (2012). She indicated that it is necessary to include an SLA in ITO contracts, as it will prevent the service provider from delivering bad services; reducing the likelihood of risk occurrence. Stephanie *et al.* (2017) indicated that the inclusion of an SLA in a service contract is to expatiate on the service requirements, reduce disputes between the client and ITSP and to ensure that the client gets the expected level of performance from the ITSP.

Another important point raised by participants of this study is the intensity of strictness and detailing that should be included in the content of the SLA. One of the participants emphasised that the intensity of strictness and detailing of an SLA should be determined by the criticality of the service. According to the participant,

> *"…if it is a business-critical service, the organisation must request for better assurances and establish [a] stricter agreement around that, the criticality of the service will determine the kind of agreement you put together with the service provider." (MaPart4).*

The relationship between degree of strictness of SLAs and service criticality is emphasised by Stephanie *et al.* (2017), in which organisations that want to outsource a web service are recommended to develop an SLA that commensurate the criticality of the web service (such as the severity of the data that goes on to the website) to be outsourced.

- ***Penalties and rewards*** – Participants mentioned that organisations must ensure that penalties for defaulting and rewards for outperforming the signed agreement must be incorporated in the contract agreement. These penalties and rewards would help reduce the likelihood of a risk occurring. This was explained by one of the participants who said that,

> *"…penalties are mechanisms that deter the service provider from continuing to provide a bad level of service because it is contracted that it will ultimately have an effect on them financially in the long run, should they continue to provide a bad level of service. …it is important to include incentives in the SLA as it will prompt the service provider to deliver a good service" (OpPart3)*

Incorporating rewards and penalties in the contract agreement as mitigating measure corresponds with what was explained in the study of Osei-Bryson *et al.* (2006), where it was suggested that in order to reduce the likelihood of contract violation, organisations should develop incentive-driven contracts. According to Jin *et al.* (2002), incentive contracts foregrounds the rewards and penalties for adhering or defaulting to signed agreement. These rewards and penalties would compel the service provider to comply accordingly. Stephanie *et al.* (2017) indicated that the rewards and penalties for failing to comply with the signed SLA should be agreed and signed upfront and effected if the service provider fails to comply as agreed.

- ***Risk resolution strategy*** – is the set plan for resolving a risk event. From the interviews, participants suggested that organisations must establish risk resolution strategy during contract negotiation, as it helps to reduce the impact of ITSP's risk on the organisation. Participants of this study identified two types of risk resolution strategies, which are escalation plan and negotiation.

  On escalation plan, one of the participants indicated that as part of the contract agreement, the outsourcing organisation and the service provider must agree on the channel and mode of incident escalation. He explained that,

  > *"…service failure is expected at some point. So, the mode and medium of escalation should be agreed upon and stated in the contract in order to reduce the impact of the risk when it occurs." (ExPart1).*

  The need for establishing escalation plans were also emphasised in the study by Philip *et al.* (2004) and Aris *et al.* (2008). In these studies, it was indicated that an ITO contract must include a dispute resolution plan that must stipulate the escalation procedures and the responsibility of the organisation and service provider during incident recovery. Hence, should a risk event occurs, the impact of the risk will be reduced because the organisations will be following an already established procedures in the management of such risk event occurrence.

  Participants recommended that organisations should be open to negotiation if a risk event is encountered. In a study by Philip *et al.* (2004), it is indicated that one of the methods of mitigating contract management risk is to ensure that the organisations develop a negotiation plan to respond to risk incidents proactively and manage the situation amicably. Stephanie *et al.* (2017) indicated that organisations must include transition or exit plans in the ITO contract that would allow them to negotiate resolution plans should a risk event occurs. Also, the existence of a transition or exit plan would allow the outsourcing organisation to employee the staff of the ITSP that were involved in the service, and buy some of the software and hardware that were used for the service.

- ***Risk education and awareness*** **–** Some of the participants of this study noted that it is essential that the ITSP's employees be educated about potential risks. It is also important that organisations create awareness of the controls that are in place to manage risks. One of the participants explained that,

  > *"…risk education and awareness help reduce the likelihood of risk occurrence because everyone within the business will be clued up on the necessary steps to take in the event of a risk occurrence" (OpPart6).*

  According to ISACA (2017), risk education and awareness is a powerful tool for ensuring an effective risk management culture. The effective communication of organisational risks, controls and escalation procedures would enhance the risk culture in the organisation; hence, reducing the probability of risk occurrence.

5.3.5.3 Mitigating controls to address risks of Information Technology Outsourcing

This section presents the mitigating controls organisations could implement to manage the four common types of ITO risks that were identified in this study. Table 5-4 presents these risks and their corresponding mitigating controls. Most of these controls have already been discussed in sections 5.4.5.1 and 5.4.5.2.

Table 5-4: Mitigating controls to address the four common risks of ITO

ITO risks	Mitigating controls/ Description
Operational	• **Delegation of in-house staff –** organisations must delegate in-house staff to lead and manage the outsource team. • **Resource mapping –** organisations must map appropriate resources to outsourced IT service
Business continuity	• **Establish in-house capabilities –** organisation must establish alternative in-house capabilities where critical business processes can be done.

	• **Develop secondary site –** If the primary site is at the service provider's vicinity, organisations must develop a secondary site elsewhere.
Data privacy	• **Implement E2EE measures –** organisations must implement E2EE of communication channel and databases. • **Implement least privilege policy –** organisations should implement least privilege policy using user access control tools. • **Establish data breach penalties –** organisations must establish and incorporate data breach penalties in the contract.
Compliance	• **Denial uncompliant service provider business –** organisations should not compromise compliance for any reason; it is either the service provider stays compliant or no contract. • **Establish contractual agreement –** organisations must bind the service provider by contractual obligation. • **Establish assurance policies –** organisations must establish and incorporate assurance policies in the contract, which would allow them conduct regular checks on the service provider**.**

5.3.6 Additional themes that emerged from the analysis of interviews

From the analysis of the interviews, two additional themes emerged. These themes are not related to the primary objective of this study; however, they are significant to the main objective of the study. These themes are presented below.

5.3.6.1 Constituting a Risk Committee

From the analysis of the interviews, many of the participants emphasised that organisations must set up a Risk Committee that will be responsible for managing ITO risks. The Committee should, according to a participant,

> *"…be in charge of identifying, assessing and establishing management controls of potential ITO risks in the organisation." (ExPart1)*

As explained by participants, the role of the Committee will be to establish adequate plans, and to execute and monitor the series of activities required to effectively identify, assess and treat ITSP's risks. In a study on risk management of ITO, Syed *et al.* (2007) indicated that in the management of the risks of ITO, it is important to constitute a Risk Committee that will be responsible for the identification, assessment and treatment of risks.

Another point raised regarding constituting a Risk Committee is the composition of the Committee. Participants of this study indicated that it is important for the Risk Committee to be multidisciplinary. Similarly, in the Deloitte (2014c) Risk Committee resource guide, it is emphasised that the Risk Committee within an organisation should comprise of experienced staff members from different departments such as finance, operations, business improvement, and internal auditors. This is because the effective management of ITO risks require adequate experience and expertise to be able to identify possible risks, vulnerabilities and threats associated with the IT service to be outsourced. The experience and expertise of Risk Committee members is also highlighted in standards such as the Risk Management Standards (NIST, 2002) and organisational charters (IBC, 2015), where it is stated that Risk Committee members must have substantial level of experience and expertise in the principles and practices of risk management.

5.3.6.2 Assurance policies

From the interviews, the assurance policies theme emerged as a means of ensuring an effective and sustainable ITO risk management. As illustrated in Figure 5-10, three sub-themes emerged from this theme.

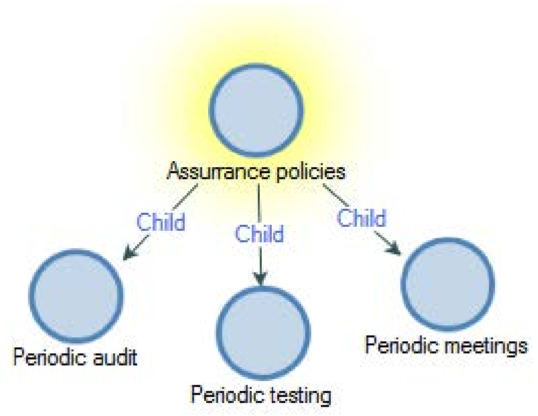


Figure 5-10: Assurance policies theme

Participants mentioned that risk changes over time, and this is often as a result of the changes in the business activities, processes and structures. Hence, tolerable risks could become intolerable over time. Participants indicated that organisations must identify residual risks of the ITSP by measuring the effectiveness of the risk response strategy implemented to address the current risks of the ITSP. Similarly, ISACA (2017) recommended that organisations must identify residual risks and continue to monitor the tolerance level of the risks on regular basis because of the changing nature of risk.

From the findings of this study, participants indicated that organisations must incorporate assurance policies into the outsourcing contract. These policies involve processes that would allow for the continuous monitoring of residual risks and identification of potentially new risks. As identified by the participants of this study, some of these processes are presented below.

- ***Periodic audit*** – many of the participants of this study indicated that organisations must ensure that they have the right to audit the ITSP on a periodic basis. This will grant the organisation access to check if ITSPs are complying with the contract terms and SLA; and to check the effectiveness of their controls on a periodic basis. In a study on third-party risk management, Vasant *et al.* (2017) emphasised that the Risk Committee must ensure that the right to audit, the audit scope, the audit process and frequency of audit are negotiated with the service provider and documented in the SLA. ISACA (2017) noted that it is essential to plan and conduct periodic IS audit. This is because periodic IS audit helps to identify potential risks, provide an objective review of the effectiveness and appropriateness of current controls, and generates necessary information required to update the service provider's risk profile.

- ***Periodic testing*** – some of the participants indicated that organisations must establish a plan that would allow for the periodic testing of controls and contingency plans. One of the participants of this study explained that,

  > *"Organisations must make sure that the contingency measures that are put in place are tested on a regular basis to make sure that they are continuously effective." (OpPart1)*

  Periodic testing is recommended as good practices in the Health Insurance Portability and Accountability Act (HIPAA) standard. This Standard, requires organisations to implement procedures for periodic testing and reviewing of contingency systems or plans in order to ensure the availability of user's health information when disaster strikes (Hash *et al.*, 2005).

- ***Periodic meetings*** – many of the participants indicated that Risk Committees must make provision for periodic meetings. The meeting could be daily, weekly or monthly depending on the criticality of the service. The agenda and purpose of this meeting, according to one of the participants should be to

  > *"…review the performance of the service provider. The reviews should then be used as a justification to either continue with the ITSP, renegotiate the contract term or move on to another service provider." (OpPart6)*

  The need to make provision for regular meetings was also identified in the study of Case (2011), where Risk Committees are recommended to conduct regular SLA performance management meetings. According to Case (2011), at these meetings, the service performance should be assessed against the key performance indicators (KPI) as specified in the SLA, with the objective of identifying areas of the SLA that are not met, or that may require improvement and revision.

5.3.7 Main objective

To propose an IT service provider risk management framework to help organisations effectively manage IT Service Provider's risks.

In order to achieve the main research objective of this study, a second cycle coding (Axial coding) was done. The themes that emerged from the first cycle coding were conceptualised and grouped according to their relationship to one another. Conceptualising the themes from the first cycle coding resulted in the emergence of five main themes of this study. Figure 5-11 shows the network of the main themes and sub-themes generated from the second cycle coding.

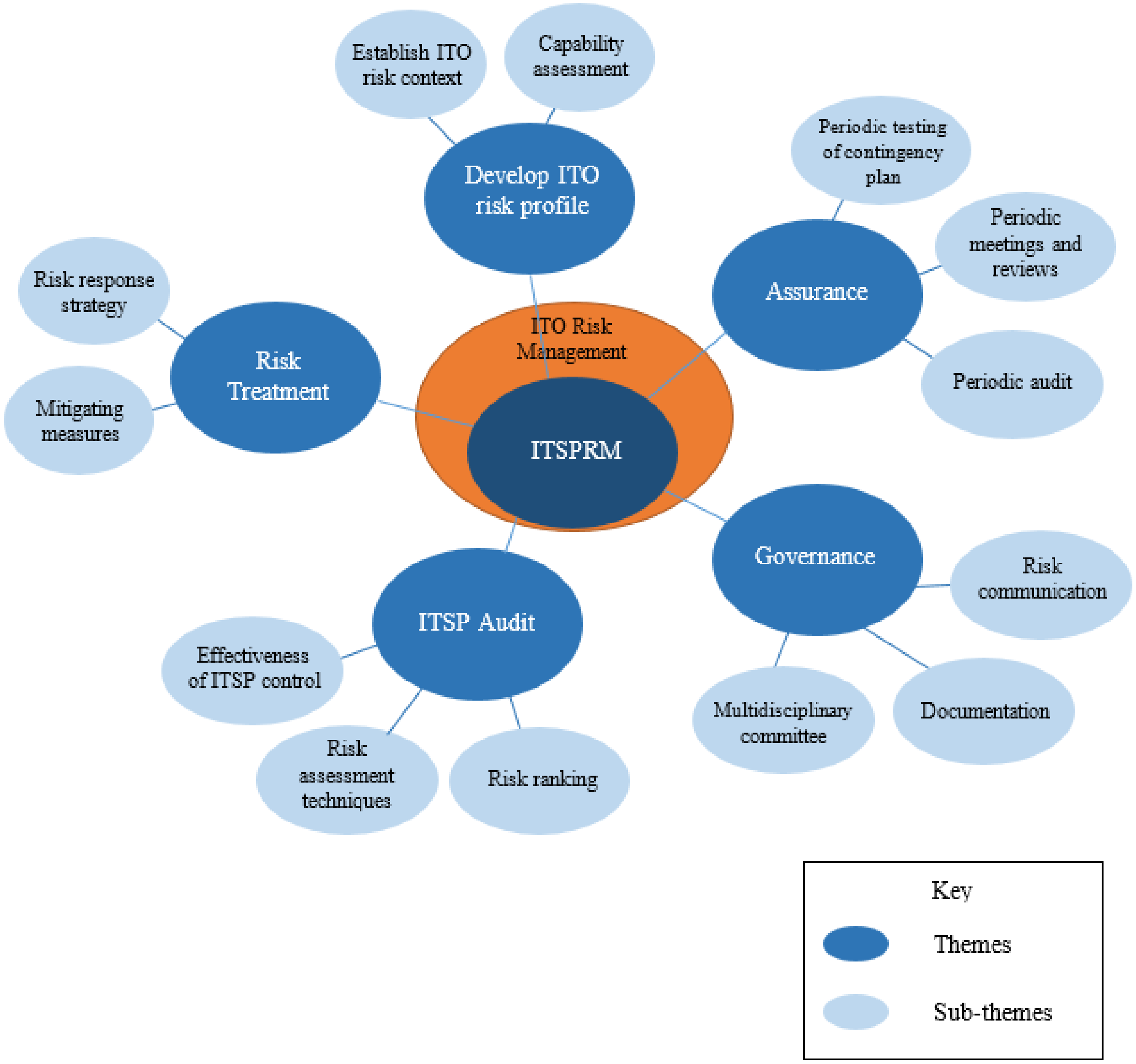


Figure 5-11: Themes and sub-themes from the findings of this study

Table 5-5: Relationship between the sub-themes generated in the second cycle coding and the first cycle coding

Themes	Sub-themes	Relation with themes generated in first cycle coding
Develop ITO risk profile	Develop ITO risk context Capability Assessment	Sub-themes emanated from the identification of risks theme in the first cycle coding
ITSP Audit	Effectiveness of ITSP control Risk assessment techniques Risk ranking	Sub-themes emanated from the assessment of risks theme in the first cycle coding
Risk treatment	Risk response strategy Mitigating Measures	Sub-themes emanated from the treatment of risks theme in the first cycle coding
Assurance	Period testing of contingency plan Periodic meetings and reviews Periodic audit	Sub-themes emanated from the additional themes that emerged from the analysis of interviews in the first cycle coding
Governance	Multidisciplinary committee Risk communication Documentation	Multidisciplinary committee emanated from the additional themes that emerged from the analysis of interviews; risk communication was conceptualised from the movement of risks from one theme to the other; and documentation is conceptualised from the development of risk documents such as the risk register and RACM in the first cycle coding. The Risk communication and Documentation sub-themes are integrated into other phases of the developed ITSPRM framework as enhancer of the risk processes.

Based on the main themes and sub-themes from the findings of this study (illustrated in Figure 5-11) a governance framework for ITSP risk management was developed. The framework, as illustrated in Figure 5-12 is a process flow of activities and tools organisations need in order to establish an effective ITSP's risk management. As noted by ISACA (2017, p. 3) risk governance aids appropriate risk management practices, adopting this framework would help organisations effectively manage ITSP's risks.

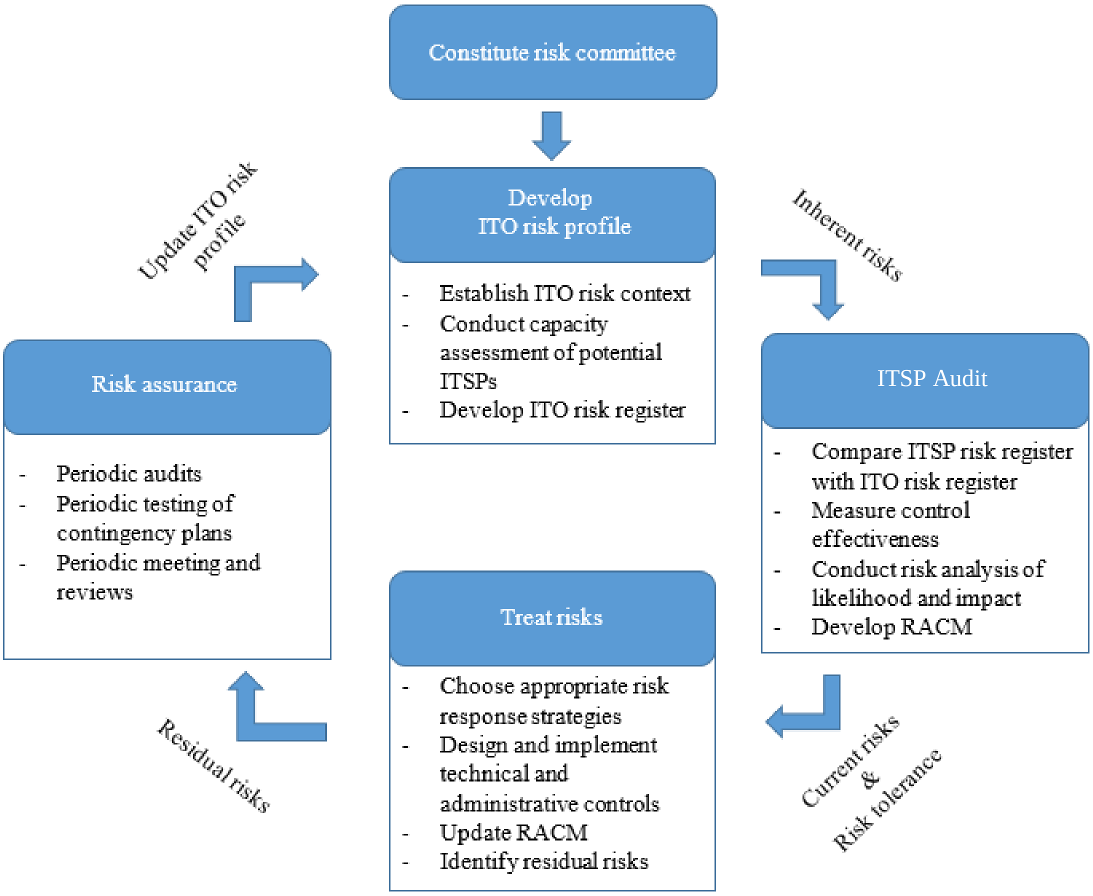

Constitute risk committee
Develop ITO risk profile
- Establish ITO risk context
- Conduct capacity assessment of potential ITSPs
- Develop ITO risk register
Inherent risks
ITSP Audit
- Compare ITSP risk register with ITO risk register
- Measure control effectiveness
- Conduct risk analysis of likelihood and impact
- Develop RACM
Current risks & Risk tolerance
Treat risks
- Choose appropriate risk response strategies
- Design and implement technical and administrative controls
- Update RACM
- Identify residual risks
Residual risks
Risk assurance
- Periodic audits
- Periodic testing of contingency plans
- Periodic meeting and reviews
Update ITO risk profile

Figure 5-12: Proposed governance framework for ITSP risk management

5.3.7.1 Discussion of proposed framework's components

The findings of this study showed that the risk management process is cyclic and sequential. The framework developed in this study is based on the relationship of the main themes that were generated from the findings of this study. The main themes of this study represent the components of the governance framework for ITSPRM, which consist of governance, development of an ITO risk profile, auditing the ITSP, treat risks and risk assurance policies, as illustrated in Figure 5-12. The sub-themes of the Governance theme, which include constituting a Risk Committee, documentation, and communication, are integrated into the holistic model to manage ITO risks effectively, specifically the risks of the ITSP. The components of the framework and their relationship with one another are discussed below.

Constitute a Risk Committee – the findings of this study showed that organisations must set up a Risk Committee who will be responsible for the risk management of ITO risks. The Committee must be multidisciplinary. Some of the responsibilities of the Risk Committee will be to ensure that appropriate risk management approaches, methods and tools are used to identify, assess and treat ITSP's risks. Ensure the integration of risk management practices and ITO practices.

Develop ITO risk profile – The findings of this study showed that at the initial stage of an ITO initiative, organisations must develop a risk profile of the initiative. This risk profile would present the risk exposure of outsourcing the proposed IT service to an ITSP. From the findings of this study, to develop ITO risk profile, Risk Committees must establish ITO risk context, conduct capacity assessment of potential ITSPs and develop ITO risk register. The process of developing an ITO risk profile would allow the Risk Committee to identify inherent risks of the ITSP; select the low-risk potential ITSP; and establish the assessment criteria, parameters and scope for an IT audit exercise.

ITSP audit – From the findings of this study, it was established that the next step after developing a risk profile is to audit the selected ITSP. This is the process of examining the appropriateness and effectiveness of the ITSP's control in managing inherent risks. From the findings of this study, to audit the ITSP, Risk Committees must compare the ITSP risk register with the ITO risk register, measure control effectiveness, conduct analysis on likelihood and impact of risk, and develop a RACM. The audit process would allow the Risk Committee to identify the current risks of the ITSP in the order of severity. The outcome of the audit process would then guide the Risk Committee on risk response strategies to adopt in addressing the current risks of the ITSP.

Treat risk – It was understood from the findings of this study that the next step after auditing the ITSP is to treat the current risks of the ITSP. This stage requires that the Risk Committee is familiar with the risk tolerance and appetite of the organisation. This is because the process of treating risks involves adopting and implementing appropriate risk response strategies to manage the current risks of the ITSP based on the tolerance and appetite of the organisation. The risk response strategies applicable are risk acceptance, mitigation, transference and avoidance. Considering that, risks cannot be totally eliminated and that risk changes, Risk Committees must identify residual risks, which must be monitored continuously.

Risk assurance – from the findings of this study, it was understood that risks change due to changes in the business. It is necessary that after treating risks, Risk Committees must make provision for continual monitoring of risks. As such, Risk Committees must incorporate assurance policies in the ITO contract. These policies should include processes such as periodic audit, periodic testing of contingency plans, and periodic meetings and reviews, as identified in this study. These processes would allow Risk Committees to check the compliant status of the ITSP, check that residual risks are still tolerable, and identify potentially new risks on a regular basis. The Risk Committee through regular meetings and reviews are then expected to update the ITO risk profile.

5.4 Conclusion

This chapter presented the findings of this study at the same time how the research objectives were achieved. The objectives of this study were highlighted and the findings relating to each of them were presented. Addressing the primary objectives of this study shows that organisations identify ITSP's risks through information gathering and capability analysis. The identified risks are assessed by examining control effectiveness and evaluating the probability of occurrence and impact of risks using techniques such as maturity assessment and BIA. The assessed risks are treated by adopting risk response strategies based on the assessment outcome and organisation tolerance/ appetite. The findings of the study also show that appropriate governance of the risk management activities facilitates effective identification, assessment and treatment of ITSP's risks.

This chapter also presented the findings on the impacts of the four common ITO risks and the controls to mitigate these risks. The findings show that the four common ITO risks are severe enough to cause reputational damage and loss in revenue to outsourcing organisations. However, mitigating controls such as contract obligation, contingency plans, risk resolution plans and E2EE could be used to attenuate the probability of occurrence and impact of ITSP's risks. Lastly, based on the findings on the primary objectives of this study, a governance Framework for managing the risks of ITSPs was developed and presented. The Framework was developed to facilitate the effective management of ITSP's risks. Hence, adopting this Framework would guide organisations on the procedures and tools to effectively manage the risk of ITSP throughout the contract period of ITO engagement.

CHAPTER 6: CONCLUSION

6.1 Introduction

The preceding chapter presented the findings of the study in relation to the research objectives. This chapter is the concluding chapter of this study. A summary of the dissertation, which highlights major steps taken in achieving the objectives of this study, is presented. Followed by the conclusion of this dissertation. The chapter further presents the recommendations and suggestions on further research for researchers and practitioners.

6.2 Summary of dissertation

This study explored how large organisations manage the risks of ITO, specifically the risks of ITSP. The main objective of the study was to propose a framework for managing the risks of ITSPs. However, in order to achieve this objective, the primary objectives that were achieved are:

1. To explore how large organisations identify IT Service Provider's risks.
2. To understand how large organisations assess IT Service Provider's risks.
    a. To highlight the impacts of the four common IT Service Providers' risks on large organisations.
3. To understand how large organisations treat IT Service Provider's risks.
    a. To explore the mitigating controls large organisations, have in place to manage IT service provider's risks and highlight the controls to attenuate the four common risks of ITO.

This dissertation comprises of six chapters including this chapter. A highlight of each chapter is presented below.

Chapter one – in this chapter, it was established that ITO is a common practice in organisations today. This is because organisations want to reduce cost and use external expertise to achieve internal objectives. Furthermore, it was revealed that ITO comes with risks, which could lead to unsatisfactory engagement. The operational risk, business continuity risk, information privacy risk and compliance risk of ITSPs were identified as the common risks of ITO. This chapter was concluded on the note that organisations need an ITSPRM framework to ensure that the risks associated with ITSPs are effectively identified, assessed and treated.

Chapter two – this chapter presented the literature on ITO. This included a review on the background of outsourcing, definitions of ITO, IT functions organisations outsource, types of ITO arrangements, ITO lifecycle, drivers of ITO, ITO success factors and challenges of ITO. The chapter further explored the risks associated with different types of ITO arrangements. The chapter concluded that irrespective of the type and form of ITO arrangement organisations may engage in, there are always risks involved. Hence, establishing the importance of managing ITO and the risks involved in ITO.

Chapter three – in this chapter, the review of the literature on risks, ITO risks and risk management practices were presented. It was established that just like every other business endeavours there are risks involved in outsourcing IT. It was identified that ITO risks stem from the client, contract agreement, and the ITSP. However, the ITSP's risks are the most common and severe risks of ITO. The chapter further elaborated on the four common risks of the ITSP, which are identified to be the operational risk, information privacy risk, business continuity risk and compliance risks of the service provider (Deloitte, 2012; Vasant *et al.,* 2017). The chapter concluded that risks are unavoidable and cannot be totally eliminated, however, using a risk management approach to ITO would help organisations achieve their outsourcing objectives.

Chapter four – this chapter presented the methods and approaches used in achieving the objectives of this study. The researcher's worldview, research methodology and design, sampling technique and analysis method were presented in the chapter. The chapter presented the reasons for selecting the research method and approach used in this study. In brief, the exploratory case study design, qualitative method, interviews, purposive and snowball sampling, and thematic analysis were employed in this study. The chapter concluded with the ethical issues considered during the course of this study.

Chapter five – in this chapter, the research framework, participants' demographics, and findings and discussion of this study were presented. From this chapter, it was deduced that there is no one size fit all approach to identifying, assessing and treating ITSP's risks. Organisations must set up a multidisciplinary committee that will be in charge of planning and executing appropriate methods, approaches and tools to effectively manage ITSPs' risks. Table 6-1 presents the summary of the methods and tools identified in this study, that are helpful in identifying, assessing and treating the risks of ITSPs.

Table 6-1: Summary of the methods and tools for managing the risks of ITSPs

Input	Process	Output
Identification of ITSP's risks		
IT service to be outsourced	Establish ITO risk context through requirements/specification gathering. Methods: Brainstorming and Roundtable discussion	The scope of the risk management process. List of risk criteria and parameters.
Risk criteria and parameters Potential ITSPs proposal	Capability assessment Methods: self-assessment, desktop review and on-site inspection	Risks, threats, and vulnerabilities of each ITSPs
Risks, threats, and vulnerabilities of each ITSPs	Grading of ITSP according to degree of risk exposure Method: ITSP ranking	Selection of lowest risk ITSP, risk ranking and degree of assessment to conduct
Assessment of ITSP's risks		
Selected ITSP	Contrast ITSP's risk register with inherent risks	Basis of risk assessment and list of established controls
Established controls	Measure effectiveness of controls Method: Control testing	Identify current risks of ITSP
Current risks of ITSP	Quantitative, qualitative or semi-quantitative analysis of the probability of occurrence and impact of current risks of ITSP on the organisation. Methods: Maturity assessment and BIA	Severity and likelihood values of the current risks of ITSP
Severity and likelihood values of the current risks of ITSP	Risk ranking Tool: RACM	List of risks in the order of severity and likelihood of

		occurrence and recommended risk response
Treatment of ITSP's risks		
List of risks in the order of severity and likelihood of occurrence, and risk tolerance and appetite of organisation	Adopt and implement risk strategy to manage risks to a tolerable level Controls: Technical and administrative mitigating controls	Treated risks and residual risks
Risk Assurance		
Residual risks	Periodic audit, testing, and reviews and meetings	Potential new risks and update risk profile

In this chapter, the impacts of the four common ITO risks on organisations were identified. These included a drop in revenue and productivity, failure or delay in service delivery, litigation, reputational damage, and regulatory fines. Furthermore, the mitigating controls for managing the impact or likelihood of the four common risks of ITO were identified. These included the delegation of in-house staff to lead and manage the outsourcing team, development of secondary sites, E2EE of communication and database, implementation of least privilege policy, and use of incentive contract method. Lastly, based on the findings of this study, a proposed governance framework for managing ITSP's risks was developed and presented. The Framework could help organisations establish a sustainable ITSPRM practices and culture.

6.3 Conclusion

The main objective of this study was to develop an ITSPRM framework. The ISO 31000 risk management framework (ISO, 2009) was used to guide the course of the study. Using the main constructs of the Framework, three main research questions were formulated. The first research question was on how large organisations identify ITSP's risks. The second research question was on how large organisations assess ITSP's risks, and the impacts of the four common risks of ITO on large organisations. The last research question was based on how do large organisations treat ITSP's risks, and the mitigating controls to manage ITSP's risks. From the literature, different risk management methods, approaches and tools were identified, however, only few were relevant in management of the risks of ITSPs.

Using an exploratory and descriptive case study design, twelve risk experts from two large organisations in South Africa were interviewed. Interviews were transcribed and analysed using NVivo software. The findings showed that the management of ITSP's risks is a continuous endeavour that comprises of a series of identification, assessment, treatment and monitoring activities. From the findings, participants indicated that in order to effectively manage ITSP's risks, organisations must constitute a Risk Committee that will be in charge of identifying, assessing and treating risks. The Risk Committee must develop an ITO risk profile by establishing the context of the ITO initiative and assessing the capability of potential ITSPs in delivering the IT service as required. This would allow the Committee to determine the inherent risks of ITO. Likewise, allowing the Committee to establish the risk criteria and parameters that would be used to assess the selected ITSP.

From this study, it was found that the assessment of ITSP's risks comprises of series of analysis and evaluation activities. The appropriate analysis and evaluation activities to engage in must be determined by the Risk Committee based on established risk criteria and parameters. At the initial stage of the assessment, Risk Committees are advised to peruse the risk register of the ITSP to identify available controls that can be used by the ITSP to address inherent risks. The Committee must also test the available controls for effectiveness and appropriateness, which allows for the identification of current risks of ITSPs. The current risks should then be analysed, evaluated and ranked according to likelihood of occurrence and impact on the organisation using appropriate assessment techniques.

From the findings of this study, it was understood that treatment of ITSP's risk is the process of adopting and implementing appropriate risk response strategies to address the current risks of the ITSP. This study confirmed the four risk responses for addressing ITSP's risks as identified in other studies, which are acceptance, mitigation, transference and avoidance. It was discovered in this study that the ranking of risk and risk tolerance and appetite of the organisation should be an important factor in determining the choice of risk response strategy to adopt. This study further investigated the measures that are useful in managing ITSP's risks. Participants identified two categories of measures, which are the administrative and technical controls. The administrative controls identified include incentive contract and risk education and awareness, while the technical controls include E2EE, contingency planning, user access management tools, and network segmentation.

Based on the findings of this study, the main objective of this study was achieved. The study presented a proposed governance framework for ITSPRM. This framework will guide organisations on how to effectively manage the risks of ITSPs.

6.4 Recommendations

The findings from this study is beneficial to organisations willing to or already outsourcing IT. Based on the findings of this study, the following are the recommendations.

Although, the literature as well as this study has established that ITO could be hazardous to organisations. This study, however, conceives that organisations can benefit from ITO through effective management of ITSP's risks. Hence, this study suggests that:

- Organisations must incorporate an effective ITSPRM strategy as a necessary component of their overall ITO strategy;
- The risk management of ITO must be positioned as a core function in organisations because it is a strategic function that facilitates objective realisation;
- Organisations must invest in risk management capabilities (such as staff and tools) that will ensure the attainment of ITO objectives; and
- Organisations must take risk management approach to ITO and ensure that risks are identified, assessed and treated at the beginning of ITO initiatives (Aris *et al.*, 2008; Osei-Bryson *et al.*, 2006).

6.5 Future research

Considering the evolving nature of risks, researchers and practitioner should continuously explore ITO risks. Due to the scope of this study, the findings of this study are more relevant for managing ITSP's risks of ITO. Below are areas for further research:

- Researchers/practitioners should explore how organisations are managing the contract agreement risks and internal risks of ITO;
- Other studies should focus on how small and medium scale organisations and governments organisations are managing the risks of ITO; and
- Researchers should use the quantitative research approach to validate the proposed ITSPRM framework.

REFERENCES

Ackermann, T., Miede, A., Buxmann, P., & Steinmetz, R. (2011). *Taxonomy of technological IT outsourcing risks: support for risk identification and quantification.* Paper presented at the ECIS.

Alberts, C. J. (2006). Common Elements of risk: DTIC Document.

Alexander, C., & Marshall, M. I. (2006). The risk matrix: Illustrating the importance of risk management strategies. *Journal of Extension, 44*(2), 2T0T1.

Applegate, L., & Montealegre, R. (1991). Eastman Kokak Organization: managing information systems through strategic alliances. *Harvard Business Case, 9*, 192-030.

Aris, S. R. H. S., Arshad, N. H., & Mohamed, A. (2008). Conceptual framework on risk management in IT outsourcing projects. *management, 36*(37), 38.

Aron, R., Clemons, E. K., & Reddi, S. (2005). Just right outsourcing: understanding and managing risk. *Journal of Management Information Systems, 22*(2), 37-55.

Artunian, J. (2006). The seven deadly sins of outsourcing. *Computerworld, 40*(19), 56-58.

Aubert, B. A., Dussault, S., Patry, M., & Rivard, S. (1999). *Managing the risk of IT outsourcing.* Paper presented at the Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on.

Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. *ACM SIGMIS Database, 36*(4), 9-28.

Bachlechner, D., Thalmann, S., & Manhart, M. (2014). Auditing service providers: supporting auditors in cross-organizational settings. *Managerial Auditing Journal, 29*(4), 286-303.

Bahli, B., & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information technology, 18*(3), 211-221.

Bahli, B., & Rivard, S. (2005). Validating measures of information technology outsourcing risk factors. *Omega, 33*(2), 175-187.

Banham, R. (2009). ERM: Viewing Risk as Opportunity - Risk-based approaches to decision-making gain traction. *Managing risk.* Retrieved from: http://online.wsj.com/ad/article/managingrisk-opportunity

Barthelemy, J. (2001). The hidden costs of IT outsourcing. *MIT Sloan Management Review, 42*(3), 60.

Barthelemy, J. (2003). The seven deadly sins of outsourcing. *The Academy of Management Executive, 17*(2), 87-98.

Barthélemy, J., & Geyer, D. (2004). The determinants of total IT outsourcing: An empirical investigation of French and German firms. *Journal of Computer Information Systems, 44*(3), 91-97.

Basu, S., & Nikam, A. (2006). Offshore Outsourcing-How Safe is Your Data Abroad? Overview of Privacy, Data Protection and Security. *Global Jurist Topics, 6*(2).

Becky, M. (2017). The Security Benefits of Network Segmentation. Retrieved from https://www.sagedatasecurity.com/blog/the-security-benefits-of-network-segmentation

Benvenuto, N. A., & Brand, D. (2005). Outsourcing-a risk management perspective. *Information Systems Control Journal, 5*, 35.

Berg, B. (1998). Qualitative Research Methods for the Social Sciences Needham Heights: Viacom.

Berg, H. (2010). Risk management: procedures, methods and experiences. *Risk Management, 1*, 79-95.

Beulen, E., & Ribbers, P. (2002). *Managing complex IT outsourcing-partnerships.* Paper presented at the System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on.

BGFRS. (2013). Guidance on Managing Outsourcing Risks (pp. 12).

Bhattacherjee, A. (2012). Social science research: principles, methods, and practices.

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE software, 8*(1), 32-41.

Bourgeois, D. T. (2014). *Information Systems for Business and Beyond* Retrieved from http://bus206.pressbooks.com/

Bradley, A., Frederick, B., Jeanot, D., Dragon, T., Michael, L., & Cesar, M. (2012). Global Technology Audit Guide (GTAG®) 7 Information Technology Outsourcing 2nd Edition. *The Institute of Internal Auditors, June 2012*, 34.

Brandabur, R. E. (2013). IT Outsourcing-A Management-Marketing Decision. *International Journal of Computers Communications & Control, 8*(2), 184-195.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Burns, N., & Grove, S. K. (1997). The practice of nursing research: Conduct, critique & utilization (3rd ed.).

businessdictionary.com. (2018). expert.businessdictionary.com. Retrieved 21/03/2017, from http://www.businessdictionary.com/definition/expert.html

Campbell, S. (2005). Determining overall risk. *Journal of Risk Research, 8*(7-8), 569-581.

Case, G. (2011). Implementing service level management. *Pink Elephant*.

Catherine, W. (2004). Top three potential risks with outsourcing InformationSystems. *Information Systems Control Journal, 5*(2).

Chakrabarty, S. (2006). Making sense of the sourcing and shoring maze: various outsourcing and offshoring alternatives. *OUTSOURCING AND OFFSHORING IN THE 21ST CENTURY: A SOCIO ECONOMIC PERSPECTIVE, HS Kehal & VP Singh, eds*, 18-53.

Chandra, A. (2005). Ontology for MANET security threats. *Electronics and Telecommunication Engineering Departement*.

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative research. *SagePublications Ltd, London*.

Chauhan, P., Kumar, S., & Sharma, R. K. (2017). Investigating the influence of opportunistic behaviour risk factors on offshore outsourcing. *International Journal of Business Excellence, 12*(2), 249-274.

Cheng, Y. (2012). *Information security risk assessment model of IT outsourcing managed service.* Paper presented at the Management of e-Commerce and e-Government (ICMeCG), 2012 International Conference on.

Cherry, K. (2015, 7/10/2016). What Is a Sample? Retrieved 18/1/2016, 2016, from http://psychology.about.com/od/sindex/g/sample.htm

Choudhury, V. (1997). Strategic choices in the development of interorganizational information systems. *Information systems research, 8*(1), 1-24.

Clark Jr, T. D., Zmud, R. W., & McCray, G. E. (1995). The outsourcing of information services: transforming the nature of business in the information industry. *Journal of Information technology, 10*(4), 221-237.

Cohen, D., & Crabtree, B. (2006). Qualitative Research Guidelines Project. from http://www.qualres.org/HomeAudi-3700.html

Cohen, L., Manion, L., & Morrison, K. (2013). *Research methods in education*: Routledge.

Corbin, J., & Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory. *Thousand Oaks*.

David, C. C., & Amy, Y. C. (2009). Information systems outsourcing life cycle and risks analysis. *Computer Standards & Interfaces, 31*, 1036–1043.

Davis, P., & Knox, I. (2004). The Reasons Why Organisations Outsource Information Technology Systems. *Australian Institute of Project Management*.

De Bruin, T., Freeze, R., Kaulkarni, U., & Rosemann, M. (2005). Understanding the main phases of developing a maturity assessment model.

De Sá-Soares, F., Soares, D., & Arnaud, J. (2014). Towards a Theory of Information Systems Outsourcing Risk. *Procedia Technology, 16*, 623-637. doi: http://dx.doi.org/10.1016/j.protcy.2014.10.011

Deloitte. (2012). 4 IT Outsourcing Risks and How to Mitigate Them. *Deloitte CIO Journal*.

Deloitte. (2014a). Deloitte's 2014 Global Outsourcing and Insourcing Survey 2014 and beyond.

Deloitte. (2014b). Managing Outsourcing Risks at the Early Stages. *Risk and Compliance Journal*. Retrieved from: http://deloitte.wsj.com/riskandcompliance/2014/03/03/managing-early-stage-outsourcing-risks/

Deloitte. (2014c). Risk Committee Resource Guide.

Deloitte. (2016). Deloitte’s 2016 Global Outsourcing Survey.

Demaria, D. A. (2011). *Risk and risk management practices within Information system outsourcing.* (Masters in Informatics), Linnaeus University.

Dhar, S., & Balakrishnan, B. (2006). Risks, benefits, and challenges in global IT outsourcing: Perspectives and practices. *Journal of Global Information Management (JGIM), 14*(3), 59-89.

Dibbern, J., Goles, T., Hirschheim, R., & Jayatilaka, B. (2004). Information systems outsourcing: a survey and analysis of the literature. *SIGMIS Database, 35*(4), 6-102. doi: 10.1145/1035233.1035236

DiRomualdo, A., & Gurbaxani, V. (1998). Strategic intent for IT outsourcing. *MIT Sloan Management Review, 39*(4), 67.

Doran, B., & Steve, P. (2004). Is selective sourcing truly more satisfying? , from http://www.computerworld.com.au/article/118305/selective_sourcing_truly_more_satisfying_/

Eamonn, K., & Kelly, M. (2015). Supply chains and value webs. *Business Trends series*. Retrieved from: http://dupress.com/articles/supply-chains-to-value-webs-business-trends/

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2012). *Management research*: Sage.

Eileen, Y. (2014). Multi-sourcing offers benefits, but complex to manage. from http://www.zdnet.com/article/multi-sourcing-offers-benefits-but-complex-to-manage/

Erber, G., & Sayed-Ahmed, A. (2005). Offshore outsourcing. *Intereconomics, 40*(2), 100-112.

Erik, B., Peter, R., & Jan, R. (2006). Managing IT outsourcing. *Netherlands: Routledge*.

Erlandson, D. A. (1993). *Doing naturalistic inquiry: A guide to methods*: Sage.

Fan, Z.-P., Suo, W.-L., & Feng, B. (2012). Identifying risk factors of IT outsourcing using interdependent information: An extended DEMATEL method. *Expert Systems* *with Applications, 39*(3), 3832-3840. doi: http://dx.doi.org/10.1016/j.eswa.2011.09.092

Gabor, M. (2017). Why you really should control your IT provider. from https://www.balabit.com/blog/really-control-provider/

Gallivan, M. J., & Oh, W. (1999). *Analyzing IT outsourcing relationships as alliances among multiple clients and vendors.* Paper presented at the Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on.

Gartner, I. (2014). Forecast Analysis: IT Outsourcing, Worldwide, 4Q13 Update. *IT Outsourcing Worldwide*.

Gary, S., Alice, G., & Alexis, F. (2002). Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology Special Publication, 800-30*, 54.

Gellings, C. (2007). *Outsourcing relationships: the contract as IT governance tool.* Paper presented at the System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Gilley, K. M., & Rasheed, A. (2000). Making more by doing less: an analysis of outsourcing and its effects on firm performance. *Journal of management, 26*(4), 763-790.

Globalization101. (2012). Technology and Globalization.

Gonzales, A., Dorwin, D., Gupta, D., Kalyan, K., & Schimler, S. (2004). Outsourcing: past, present and future. *Unpublished paper*.

Gonzalez, R., Gasco, J., & Llopis, J. (2009). Information systems outsourcing reasons and risks: an empirical study. *International Journal of Human and Social Sciences, 4*(3), 181-192.

Gonzalez, R., Gasco, J., & Llopis, J. (2010). Information systems outsourcing reasons and risks: a new assessment. *Industrial Management & Data Systems, 110*(2), 284-303.

Gottschalk, P., & Solli-Sæther, H. (2005). Critical success factors from IT outsourcing theories: an empirical study. *Industrial Management & Data Systems, 105*(6), 685-702.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of qualitative research, 2*(163-194), 105.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods, 18*(1), 59-82.

Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling, 58*(5), 1189-1205. doi: https://doi.org/10.1016/j.mcm.2013.02.006

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study.

Handfield, R. (2008). A brief history of outsourcing. *Supply Chain Resource Cooperative-Supply Chain Management; May 2006; available at http://scm. ncsu. edu/public/facts/facs060531. html; Last accessed: 9 June 2007: http://atschool. eduweb. co. uk/kingworc/departments/geography/asglossarycw. ht m*.

Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. (2005). *An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule*: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Hätönen, J., & Eriksson, T. (2009). 30+ years of research and practice of outsourcing – Exploring the past and anticipating the future. *Journal of International*

Management, 15(2), 142-155. doi: http://dx.doi.org/10.1016/j.intman.2008.07.002

Hirschheim, R., & Dibbern, J. (2002). Information systems outsourcing in the new economy—an introduction *Information Systems Outsourcing* (pp. 3-23): Springer.

Hirschheim, R., & Lacity, M. (1997). Information Systems Outsoucing and Insourcing: Lessons and Experiences. *PACIS 1997 Proceedings*, 3.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: a literature review. *International Journal of Production Research, 53*(16), 5031-5069.

Hodosi, G., Kaye, R., & Rusu, L. (2015). IT Outsourcing Success Factors: A Study of Large and Medium. *Modern Techniques for Successful IT Project Management*, 183.

IBC. (2015). Risk Committee Charter.

Iqbal, Z., & Dad, A. M. (2013). Outsourcing: A Review of Trends, Winners & Losers and Future Directions. *International Journal of Business and Social Science, 4*(8).

IRM. (2002). The risk management standard.

ISACA. (2017). *Certified in Risk and Information Systems Control - Review manual*.

ISO, I. (2009). 31000: 2009 Risk management–Principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*.

Jackson, T., Iloranta, K., & McKenzie, S. (2001). Profits or perils? The bottom line on outsourcing. *Strategy+ Business*.

Jimmy Gandhi, S., Gorod, A., & Sauser, B. (2012). Prioritization of outsourcing risks from a systemic perspective. *Strategic Outsourcing: An International Journal, 5*(1), 39-71.

Jin, L.-j., Machiraju, V., & Sahai, A. (2002). Analysis on service level agreement of web services. *HP June*, 19.

Johnston, K., Abader, T., Brey, S., & Stander, A. (2009). Understanding the outsourcing decision in South Africa with regard to ICT. *South African Journal of Business Management, 40*(4).

Jonathan, W. (2017). British Airways Flights And IT Failure: Cue Furious Debate Around Outsourcing. Retrieved 11/06/2017, 2017, from https://www.forbes.com/sites/jwebb/2017/05/29/british-airways-flights-and-it-failure-cue-furious-debate-around-outsourcing/#5862832f7839

Kakabadse, A., & Kakabadse, N. (2002). Trends in outsourcing:: Contrasting USA and Europe. *European Management Journal, 20*(2), 189-198.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: a new framework.

Kayesa. (2016). Business Impact (Severity) Levels: Definition & Examples. Retrieved 04/10/2017, from https://helpdesk.kaseya.com/hc/en-gb/articles/229023048-Business-Impact-Severity-levels-Definition-Examples

Kerlinger, F. (1970). *Foundations of Behavioural Research*. United States of America: Holt, Rinehart and Winston: Inc.

King III. (2009). *King Report on Governance for South Africa*: Institute of Directors, Southern Africa.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management, 14*(1), 53-68.

Kliem, R. (2004). Managing the risks of offshore IT development projects. *Information Systems Management, 21*(3), 22-27.

KPMG. (2012). South African Sourcing Pulse Survey.

Kumar, S. (2016). Outsourcing versus insourcing, trust innovation to the experts. Retrieved 3/9/2016, from http://www.itnewsafrica.com/2016/02/outsourcing-versus-insourcing-trust-innovation-to-the-experts/

Kvale, S. (1996). InterViews London: Sage.

Lacey, A., & Luff, D. (2001). *Qualitative data analysis*: Trent Focus Sheffield.

Lacity, M. C., Khan, S. A., & Willcocks, L. P. (2009). A review of the IT outsourcing literature: Insights for practice. *The Journal of Strategic Information Systems, 18*(3), 130-146.

Lacity, M. C., Willcocks, L. P., & Feeny, D. F. (1996). The value of selective IT sourcing. *MIT Sloan Management Review, 37*(3), 13.

Laurie, W. (2004). *Risk Management* Retrieved from http://agile.csc.ncsu.edu/SEMaterials/RiskManagement.pdf

Lavrakas, P. J. (2008). Encyclopedia of Survey Research Methods. *Vol. 2, pp. 1072*.

Leavy, B. (2001). Supply strategy-what to outsource and where. *Irish marketing review, 14*(2), 46.

Lee, J.-N., Heng, C. S., & Lee, J. (2009). Multi-vendor outsourcing: Relational structures and organizational learning from a social relation perspective. *ICIS 2009 Proceedings*, 71.

Li, Y., & Liao, X. (2007). Decision support for risk analysis on dynamic alliance. *Decision Support Systems, 42*(4), 2043-2059.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*: SAGE Publications.

Loh, L., & Venkatraman, N. (1992). Diffusion of information technology outsourcing: influence sources and the Kodak effect. *Information systems research, 3*(4), 334-358.

Lonsdale, C., & Cox, A. (1997). Outsourcing: risks and rewards. *Supply Management, 2*(14), 32-34.

Lonsdale, C., & Cox, A. (2000). The historical development of outsourcing: the latest fad? *Industrial Management & Data Systems, 100*(9), 444-450.

Lynda, M. A., Robert, D. A., & Deborah, L. S. (2009). *Corporate Information Strategy and Management*.

MacInnis, P. (2003). Warped expectations lead to outsourcing failures. *Computing Canada, 29*(7), 1-2.

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research*: Sage publications.

McFarlan, F. W., & Nolan, R. L. (1995). How to manage an IT outsourcing alliance. *Sloan management review, 36*(2), 9.

Meyer, K., & Weinert, S. (2005). The evolution of IT outsourcing: From its origins to current and future trends. *Arbeitspapiere des Fachbereichs Wirtschafts-und Sozialwissenschaften der Bergischen Universität Wuppertal, 202*.

Mitchell, O. (2014). Lesson from Kodak's demise: Beware of outsourcing too much of your secret sauce. Retrieved 04/09/2016, from http://business.financialpost.com/executive/c-suite/lesson-from-kodaks-demise-beware-of-outsourcing-too-much-of-your-secret-sauce

Morehouse, R. (1994). *Beginning qualitative research: A philosophic and practical guide* (Vol. 6): Psychology Press.

Nampak. (2012). Integrated Annual Report 2012.

Neuman, L. W. (2002). Social research methods: Qualitative and quantitative approaches.

NIST. (2002). Risk Management Guide for Information Technology Systems *Recommendations of the National Institute of Standards and Technology*

NOVA. (2010). Northern Virginia Hazard Mitigation Plan Update *Chapter 5: Capability Assessment*

OFCCP. (2014). Federal Contract Compliance Manual.

OICV-IOSCO. (2014). Risk Identification and Assessment Methodologies for Securities Regulators: The Board of the International Organization of Securities Commissions.

Ongwattanasirikul, T., Malisuwan, S., & Madan, N. (2013). Risk analysis of it outsourcing case study on public companies in Thailand. *Journal of Economics, Business and Management, 1*(4), 365-370.

Optimus, I. (2016). Pros and Cons of Pure Onshore, Pure Offshore and Hybrid Model Outsourcing. from http://www.optimusinfo.com/pros-and-cons-of-pure-onshore-pure-offshore-and-hybrid-model-outsourcing/

Osei-Bryson, K.-M., & Ngwenyama, O. K. (2006). Managing risks in information systems outsourcing: An approach to analyzing outsourcing risks and structuring incentive contracts. *European Journal of Operational Research, 174*(1), 245-264.

Oshri, I. (2010). *Global Sourcing of Information Technology and Business Processes: 4th International Workshop, Global Sourcing 2010, Zermatt, Switzerland, March 22-25, 2010, Revised Selected Papers* (Vol. 55): Springer Science & Business Media.

Panthi, K., Ahmed, S. M., & Azhar, S. (2007). *Risk matrix as a guide to develop risk response strategies.* Paper presented at the Proceedings of 43 rd ASC National Annual Conference.

Patricia. (2014). Advantages and Disadvantages of Outsourcing. Retrieved 22/03/2016, from http://smartchurchmanagement.com/advantages-and-disadvantages-of-outsourcing/

Patterson, F. D., & Neailey, K. (2002). A risk register database system to aid the management of project risk. *International Journal of Project Management, 20*(5), 365-374.

Patton, M. Q. (1980). Qualitative evaluation methods. Beverly Hills: cA: Sage.

Patton, M. Q. (1987). *How to use qualitative methods in evaluation*: Sage.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*: SAGE Publications, inc.

Patton, M. Q. (2001). *Qualitative Research & Evaluation Methods*: SAGE Publications.

Paul, A. (2004). Most outsourcing is still for losers. *Computerworld*.

Paul, K. (2011). Disaster recovery: Risk assessment and business impact analysis are key stages in disaster recovery planning, but where do they fit into the DR planning process? Retrieved 02/11/2016, from http://www.computerweekly.com/feature/Disaster-recovery-Risk-assessment-and-business-impact-analysis

Paul, S. (2011). Using Brainstorming Techniques To Identify Project Risk. Retrieved 01/01/2018, from https://mushcado.wordpress.com/2011/01/11/using-brainstorming-techniques-to-identify-project-risk/

PCISSC. (2016). Information Supplement: Third-Party Security Assurance *PCI Data Security Standard (PCI DSS).*

Pengilly, W. R. (2007). *Determining the level and extent of information technology outsourcing services in the South African higher education environment.* UNIVERSITY OF JOHANNESBURG.

Philip, O. K., & Scott, V. (2004). Managing the Risks of Outsourcing: A survey of current practices and their effectiveness (pp. 17).

PMBOK3. (2004). *A guide to the project management body of knowledge.* Paper presented at the Project Management Institute.

Power, M. (2009). The risk management of nothing. *Accounting, organizations and society, 34*(6), 849-855.

Prado, E. P. V. (2011). Risk analysis in information technology and communication outsourcing. *JISTEM-Journal of Information Systems and Technology Management, 8*(3), 605-618.

Prince 2. (2017). Risk. from http://prince2.wiki/Risk

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis, 30*(6), 881-886.

PWC. (2015). Risk Management: IT Vendor Management and Outsourcing.

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2013). RESEARCH METHODOLOGY.

Ramachandran, V., & Gopal, A. (2010). Managers' judgments of performance in IT services outsourcing. *Journal of Management Information Systems, 26*(4), 181-218.

Ramanujan, S., & Jane, S. (2006). A legal perspective on outsourcing and offshoring. *Journal of American Academy of business, 8*(2), 51-58.

Ramsaran, C. (2004). “Outsourcing Obstacle”. *Bank System and Technology, 41*(6), 38.

Rana, P. (2013). Importance of Information Technology in Manufacturing Sector: A Review. *3*(9), 432-435.

Ravi, S. (2010). The benefits and risks of outsourcing. Retrieved 05/12/2016, from http://www.lexology.com/library/detail.aspx?g=e698d613-af77-4e34-b84e-940e14e94ce4

Richard, M. (2009). How to mitigate operational, compliance risk of outsourcing services. Retrieved from: http://searchcompliance.techtarget.com/tip/How-to-mitigate-operational-compliance-risk-of-outsourcing-services

Richie, H. (2015). Risk Analysis: The Most Important Risk Management Stage. Retrieved 24/10/2016, 2016, from https://goo.gl/amRF2i

Ritchie, M. (2015). Outsourcing's booming business. Retrieved 3/2/2016, 2015, from http://www.iso.org/iso/news.htm?refid=Ref1922

Robert, J. S. (2014). Greatest Compliance Risks Surrounding Third-Party Outsourcing. Retrieved 06/11/2016, from http://corporatecomplianceinsights.com/greatest-compliance-risks-surrounding-third-party-outsourcing/

Robinson, M., Kalakota, R., & Sharma, S. (2005). *Global outsourcing: executing an onshore, nearshore or offshore strategy*: Mivar Press.

Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers* (Vol. 2): Blackwell Oxford.

Saldaña, J. (2015). *The coding manual for qualitative researchers*: Sage.

Samantra, C., Datta, S., & Mahapatra, S. S. (2014). Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective. *Expert Systems with Applications, 41*(8), 4010-4022. doi: http://dx.doi.org/10.1016/j.eswa.2013.12.024

Saunders, M. N., Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research methods for business students, 5/e*: Pearson Education India.

Schaaf, J. (2004). Offshoring: Globalisation wave reaches services sector. *Deutsche Bank Research. E-conomics, 45*.

Sharma, R., & Yetton, P. (1996). Interorganizational cooperation to develop information systems. *ICIS 1996 Proceedings*, 9.

Shawn, M. (2013). What Is an Inspection Checklist? *The Checker Blog.* from http://www.thechecker.net/stories/blog/bid/312464/What-Is-an-Inspection-Checklist

Slovic, P. (1999). Are trivial risks the greatest risks of all? *Journal of Risk Research, 2*(4), 281-288.

Smith, M. A., Mitra, S., & Narasimhan, S. (1998). Information systems outsourcing: a study of pre-event firm characteristics. *Journal of Management Information Systems, 15*(2), 61-93.

Spikin, I. C. (2013). Risk Management theory: the integrated perspective and its application in the public sector. *Estado, Gobierno y Gestión Pública*(21), pp. 89/126.

Statista. (2015). Global market size of outsourced services from 2000 to 2015 (in billion U.S. dollars). Retrieved 3/2/2016, from http://www.statista.com/statistics/189788/global-outsourcing-market-size/

Stephanie, O., Lynn, G., & Lauren, G., Paul. (2017). What is an SLA? Definition, best practices and FAQs. Retrieved 01/01/2018, from https://www.cio.com/article/2438284/outsourcing/outsourcing-sla-definitions-and-solutions.html

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research techniques*: Sage publications.

Sue, C. (2012). Service Level Agreement in Outsourcing Contracts. *Outsourcing.* Retrieved 01/01/2018, from http://www.slaw.ca/2012/04/04/service-level-agreement-in-outsourcing-contracts/

Surak, J. G., & Wilson, S. (2007). *The certified HACCP auditor handbook*: ASQ Quality Press.

Syed, S. R. H., Arshad, N. H. H., & Mohamed, A. (2007). Critical Review of Risk Management in IT Outsourcing.

Tayauova, G. (2012). Advantages and disadvantages of outsourcing: analysis of outsourcing practices of Kazakhstan banks. *Procedia-Social and Behavioral Sciences, 41*, 188-195.

Thanapol, O., Settapong, M., & Navneet, M. (2013). Risk Analysis of IT Outsourcing Case Study on Public Companies in Thailand. *Journal of Economics, Business and Management, 1*(4).

Tho, I. (2012). *Managing the Risks of IT Outsourcing*: Taylor & Francis.

Tjoa, S., Jakoubi, S., & Quirchmayr, G. (2008). *Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology.* Paper presented at the Availability, Reliability and Security, 2008. ARES 08. Third International Conference on.

Tomlin, B. (2006). On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science, 52*(5), 639-657.

Tompkins, J. A., Simonson, S. W., Upchurch, B. E., & Tompkins, B. W. (2005). *Logistics and manufacturing outsourcing: harness your core competencies*: Tompkins Press.

Vasant, R., & Samir, S. (2017). The Practical Aspect: Third-party Risk Managaement. *ISACA Journal, 2*.

Vaughan, E. (1997). Risk Management. New York: John Willey and Sons: Inc.

Vaxevanou, A., & Konstantopoulos, N. (2015). Models Referring to Outsourcing Theory. *Procedia - Social and Behavioral Sciences, 175*, 572-578. doi: http://dx.doi.org/10.1016/j.sbspro.2015.01.1239

Wijnia, Y., & Nikolic, I. (2007). *Assessing business continuity risks in IT.* Paper presented at the 2007 IEEE International Conference on Systems, Man and Cybernetics.

Willcocks, L. P., Lacity, M. C., & Kern, T. (1999). Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA. *The Journal of Strategic Information Systems, 8*(3), 285-314.

Willis, H. H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis, 27*(3), 597-606.

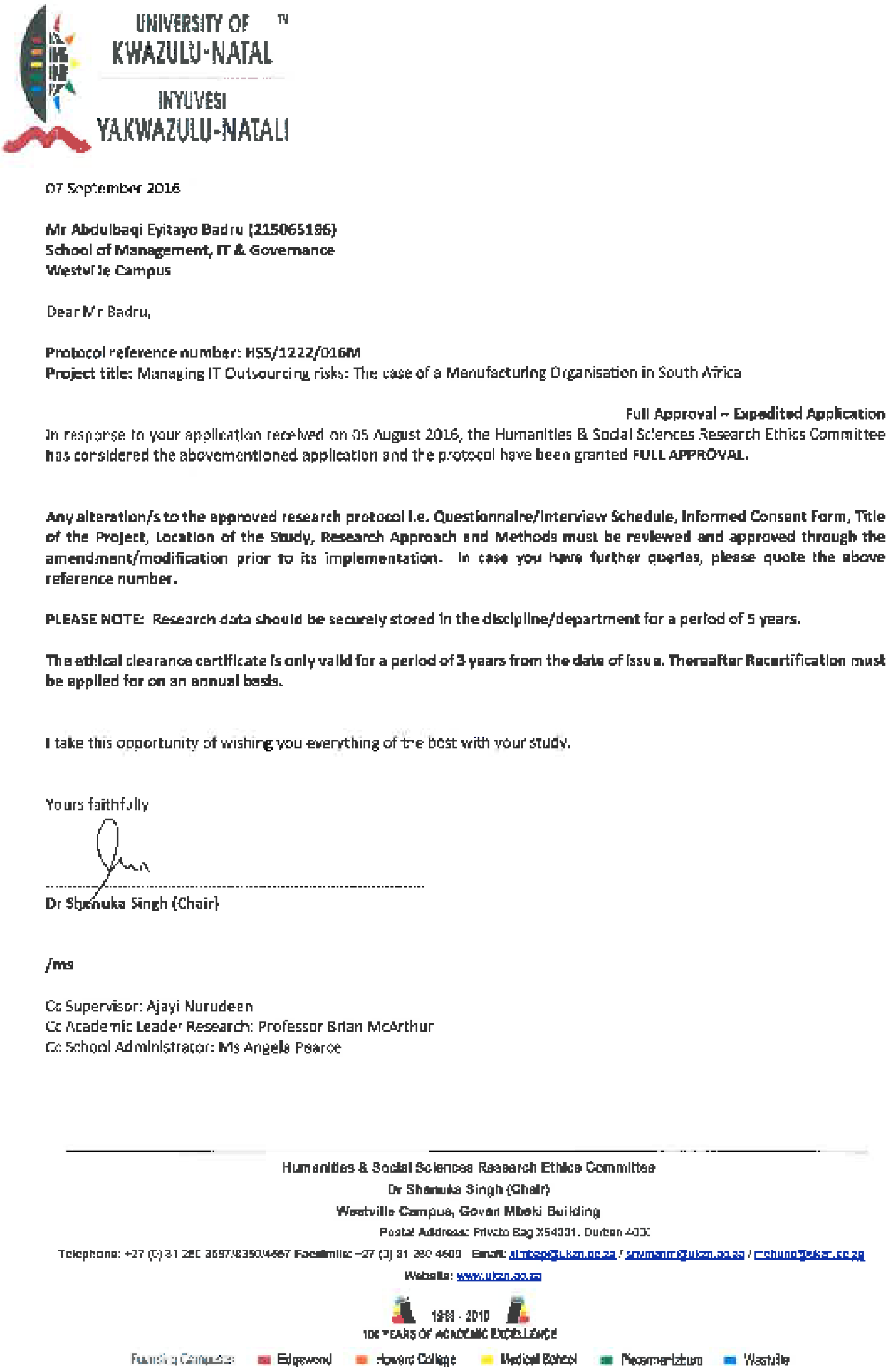
Yin, R. K. (1989). Case study research: Design and methods, Revised ed. *Applied Social Research Series, 5*.

Yin, R. K. (2003). Case study research design and methods third edition. *Applied social research methods series, 5*.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

APPENDICES

Appendix A – Ethical clearance



UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

07 September 2016

Mr Abdulbaqi Eyitayo Badru (215065196)
School of Management, IT & Governance
Westville Campus

Dear Mr Badru,

Protocol reference number: HSS/1222/016M
Project title: Managing IT Outsourcing risks: The case of a Manufacturing Organisation in South Africa

Full Approval – Expedited Application

In response to your application received on 05 August 2016, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol have been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Dr Shenuka Singh (Chair)

/ms

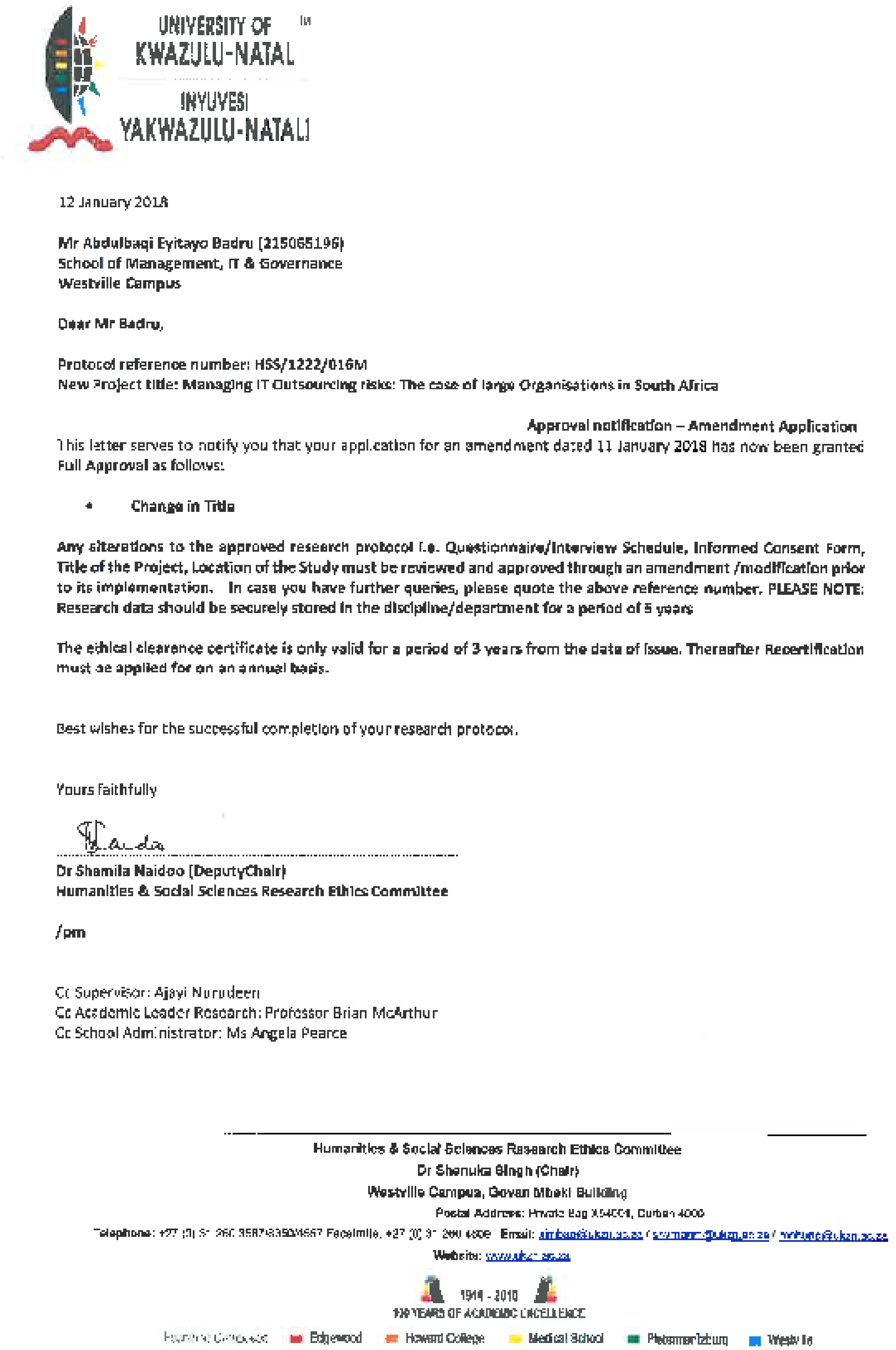
Cc Supervisor: Ajayi Nurudeen
Cc Academic Leader Research: Professor Brian McArthur
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 Facsimile: +27 (0) 31 260 4609 Email: ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: ■ Edgewood ■ Howard College ■ Medical School ■ Pietermaritzburg ■ Westville

Appendix B – New Ethical clearance



UNIVERSITY OF KWAZULU-NATAL

INYUVESI YAKWAZULU-NATALI

12 January 2018

Mr Abdulbaqi Eyitayo Badru (215065196)
School of Management, IT & Governance
Westville Campus

Dear Mr Badru,

Protocol reference number: HSS/1222/016M
New Project title: Managing IT Outsourcing risks: The case of large Organisations in South Africa

Approval notification – Amendment Application

This letter serves to notify you that your application for an amendment dated 11 January 2018 has now been granted Full Approval as follows:

- **Change in Title**

Any alterations to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study must be reviewed and approved through an amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

Best wishes for the successful completion of your research protocol.

Yours faithfully

Dr Shamila Naidoo (DeputyChair)
Humanities & Social Sciences Research Ethics Committee

/pm

Cc Supervisor: Ajayi Nurudeen
Cc Academic Leader Research: Professor Brian McArthur
Cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: 🟥 Edgewood 🟧 Howard College 🟨 Medical School 🟩 Pietermaritzburg 🟦 Westville

Appendix C – Interview schedule

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

Managing IT Outsourcing Risks: The case of Large Organisations in South Africa

Interview Schedule

MCom Research Project

School of Information Systems & Technology

Faculty of Management Studies

University of KwaZulu-Natal

Researcher: Badru Abdulbaqi (0768216798)

Supervisor: Mr Ajayi Nurudeen (031-2606013)

Introduction

My name is Badru Abdulbaqi. I am a Masters student at the School of Information Systems & Technology, University of KwaZulu-Natal. I would like to ask you some questions that are related to your background, your job, and your experience. Particularly the experience you have gained in the course of managing the risks of outsourcing IT infrastructure in your organisation. This is to enable me to understand how the following IT outsourcing (ITO) risks - operational risks, information privacy risks, business continuity risks, and compliance risks can be managed with respect to outsourcing IT infrastructure in your organisation. This interview will help me gain insight into the impact of these risks on your organisation. It will also enable me to examine risk management practices employed in your organisation with the aim of proposing an effective ITO risk management framework which risk and information technology officers can adapt to their respective companies, thereby gaining the full benefit of outsourcing IT.

In the cause of this interview, the following keywords will be used: Information technology outsourcing, Risks, Risk factors and Risk management practices.

As used in the research, each can be briefly described as:

Information technology outsourcing: this is the contracting out of information technology function to a third-party organisation.

Risk: The state of uncertainty, threat or probability that an action or event will adversely or beneficially affect the ability to achieve desired objectives.

Risk factors: These are the elements or attributes that contribute to a risk event.

Risk management Practices: these are the tools, methods or techniques used to identify, assess and manage risks.

The interview should take about 50 minutes.

Job & Experience

Job & Job role

a) How long have you worked in this organisation?
b) What position do you hold in this organisation?
c) How long have you worked in your current position?
d) Could you please tell me what your main responsibilities are?

Experience in Information technology outsourcing & Risk management

a) Before joining this organisation, did you work within the:
   i. Information technology outsourcing unit of any organisation?
   ii. Risk management unit of any organisation?

b) Does your present job position/responsibility involve the:
   i. Management of information technology outsourcing contracts or projects?
   ii. Risk management of this organisation?

c) Have you had any training or certification in:
   i. Information technology outsourcing management?
   ii. Risk management?

Section A

The risks in this interview guide are based on your organisation's service providers.

Operational Risk

a. Risk Identification

i. How has your organisation been able to identify the risk of your service provider, possibly failing to deliver their services due to operational issues?

ii. Could you please explain the possible factors that may prevent your service provider from delivering their services due to operational issues?

b. Risk Assessment

i. How does your organisation assess the probability that the service provider could fail to deliver their services due to operational issues?

ii. Could you please explain what the impact would be on your organisation, if the service provider fails to deliver their services due to operational issues?

iii. How has your organisation prioritised the risk that could be caused if the service provider fails to deliver their services due to operational issues?

c. Risk Control

i. Could you please explain the risk management strategies your organisation has in place to address the risk of the service provider failing to function due to operational issues?

ii. How have you implemented these strategies towards reducing/eliminating the likelihood of the occurrence of the risk of the service provider failing to function due to operational issues?

iii. How have you implemented these strategies towards reducing/eliminating the impact of risk on your organisation if your service provider fails to function due to operational issues?

iv. How have these strategies functioned for your organisation?

Business Continuity Risk

a. Risk Identification

i. How has your organisation been able to identify the risk of your service provider, possibly going out of business?

ii. Could you please explain the possible factors that may result in your service provider going out of business?

b. Risk Assessment

i. How does your organisation assess the probability that the service provider could possibly go out of business?

ii. Could you please explain what the impact would be on your organisation if the service provider goes out of business?

iii. How has your organisation prioritised the risk that could be caused if the service provider going of business?

c. <u>Risk Control</u>

i. Could you please explain the risk management strategies your organisation has in place to address the risk of the service provider going out of business?

ii. How have you implemented these strategies towards reducing/eliminating the likelihood of the occurrence of the risk of the service provider going out of business?

iii. How have you implemented these strategies towards reducing/eliminating the impact of risk on your organisation if your service provider goes out of business?

iv. How have these strategies functioned for your organisation?

Information Privacy Risk

a. <u>Risk Identification</u>

i. How has your organisation been able to identify the risk of your service provider, intentionally or unintentionally disclosing your information to unauthorised users?

ii. Could you please explain the possible factors that may result in your service provider disclosing your information to unauthorised users?

b. <u>Risk Assessment</u>

i. How does your organisation assess the probability that the service provider could disclose your information to unauthorised user?

iv. Could you please explain what the impact would be on your organisation if the service provider discloses your information to unauthorised user?

ii. How has your organisation prioritised the risk that could be caused if the service provider discloses your information to unauthorised user?

c. <u>Risk Control</u>

i. Could you please explain the risk management strategies your organisation has in place to address the risk of the service provider disclosing your information to unauthorised users?

ii. How have you implemented these strategies towards reducing/eliminating the likelihood of the occurrence of the risk of the service provider disclosing your information to unauthorised users?

iii. How have you implemented these strategies towards reducing/eliminating the impact of risk on your organisation if your service provider discloses your information to unauthorised users?

iv. How have these strategies functioned for your organisation?

Compliance Risk

a. Risk Identification

i. How has your organisation been able to identify the risk of your service provider's noncompliance with regulations? Could you please identify some of these regulations?

ii. Could you please explain the possible factors that may result in your service provider not complying with these regulations?

b. Risk Assessment

i. How does your organisation assess the probability that the service provider could fail to comply to regulations?

ii. Could you please explain what the impact would be on your organisation if the service provider fails to comply with regulations?

iii. How has your organisation prioritised the risk that could be caused if the service provider fails to comply with regulations?

c. Risk Control

i. Could you please explain the risk management strategies your organisation has in place to address the risk of the service provider not complying with regulations?

ii. How have you implemented these strategies towards reducing/eliminating the likelihood of the occurrence of the risk of the service provider not complying with regulations?

iii. How have you implemented these strategies towards reducing/eliminating the impact of risk on your organisation if your service provider does not comply with regulations?

iv. How have these strategies functioned for your organisation?

Section B

Risk Management Practices

1. How has your organisation been able to sustain the risk management standard or practices with regards to ITO?
    a. Could you please explain the tools or methods used by your organisation for the risk management standard or practices?
    b. Could you please explain the role of stakeholders involved in establishing the risk management standard or practices?
2. Do you think your organisation’s risk management practices is functional? If yes, please tell me about the functionality of your risk management practices.
3. Could you please explain how your organisation has incorporated ITO risk management practices into the organisation corporate practices?

Appendix D – Information sheet

Managing IT Outsourcing Risks: The case of Large Organisations in South Africa

Information Sheet

Date: 18-11-2016

Greetings,

My name is Badru Abdulbaqi from the University of KwaZulu-Natal (School of Management, IT, and Governance). My contact number is 0768216798 and my email address is abdulbaqibadru@gmail.com. My research supervisor's contact number is 033 260 2013 and his email address is Ajayi@ukzn.ac.za.

You are being invited to consider participating in a study titled "**Managing IT Outsourcing Risks: The case of Large Organisation in South Africa"**.

The aims of this research are:

1. To explore how large organisations are managing the risks associated with IT outsourcing.
2. To explore the IT outsourcing risk management practices used by large organisations.
3. To propose IT outsourcing risk management framework for the effective management of IT outsourcing risks.

Through your participation, I hope to enable understand how the following IT outsourcing risks- operational risks, information security risks, business continuity risks, and compliance risks can be managed with respect to outsourcing IT infrastructure in your organisation. This interview will help me gain insight into the impact of these risks on your organisation. It will also enable me examine risk management practices employed in your organisation with the aim of proposing an effective ITO risk management framework which risk and information technology officers can adapt to their respective companies, thereby gaining the full benefit of outsourcing IT.

In the event of any problems or concerns/questions you may contact the Researcher at (provide contact details) or the UKZN Humanities & Social Sciences Research Ethics Committee, contact details as follows:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office,
Westville Campus Govan
Mbeki Building

Private Bag X 54001

Durban 4000 KwaZulu-Natal, SOUTH
AFRICA Tel: 27 31 2604557- Fax: 27 31
2604609

Email: HSSREC@ukzn.ac.za

Your participation in the study is voluntary and by participating, you are granting the Researcher permission to use your responses. You may refuse to participate or withdraw from the study at any time with no negative consequence. There will be no monetary gain from participating in the study. Your anonymity will be maintained by the Researcher and the School of Management,

I.T. & Governance and your responses will not be used for any purposes outside of this study. All data, both electronic and hard copy will be securely stored during the study and archived for 5 years. After this time, all data will be destroyed.

If you have any questions or concerns about participating in the study, please contact me or my research supervisor at the numbers listed above.

Please Note

- The interview will be for about 50minutes

Thank you for your willingness to participate!

Sincerely,

Badru Abdulbaqi Eyitayo

Appendix E – Consent to participate

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

Managing IT Outsourcing Risks: The case of Large Organisations in South Africa

Consent to Participate

I____have been informed about the study entitled "**Managing IT Outsourcing Risks: The case of large Organisations in South Africa"** by Badru Abdulbaqi Eyitayo.

I understand the purpose and procedures of the study.

I have been given an opportunity to ask questions about the study and have had answers to my satisfaction.

I declare that my participation in this study is entirely voluntary and that I may withdraw at any time without affecting any of the benefits that I usually am entitled to.

If I have any further questions/concerns or queries related to the study, I understand that I may contact the Researcher at 0768216798 or abdulbaqibadru@gmail.com.

If I have any questions or concerns about my rights as a study participant, or if I am concerned about an aspect of the study or the Researchers then I may contact:

HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS ADMINISTRATION

Research Office,
Westville Campus Govan
Mbeki Building
Private
Bag X
54001
Durban
4000
KwaZulu-Natal, SOUTH AFRICA
Tel: 27 31 2604557 - Fax: 27 31 2604609
Email: HSSREC@ukzn.ac.za

____________________ ____________________

Signature of Participant **Date**