The Role of Information Technology Governance Frameworks on Cloud Computing Risks

by

TANDEKA DUNYISIWE MSIMANGA

A minor dissertation submitted in fulfilment for the Degree
of
Master's in Commerce
in
Computer Auditing

at the
College of Business and Economics
UNIVERSITY OF JOHANNESBURG

Supervisor: Rozanne Smith
Co-Supervisor: Pranisha Rama

2021

DECLARATION

I certify that the *minor dissertation* submitted by me for the degree *Master's of Commerce (Computer Auditing)* at the University of Johannesburg is my independent work and has not been submitted by me for a degree at another university.

TANDEKA DUNYISIWE MSIMANGA

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to Rozanne Smith and Pranisha Rama, my research supervisors, for their patience, guidance, enthusiastic encouragement, and valuable and constructive suggestions throughout this study. There were many times where I had reached the 'crossroads' and each time, you were both there to steer me towards the right path. Your willingness to offer me so much of your time and generously so has been very much appreciated. Thank you so much Rozanne and Pranisha.

I would also like to thank my family for their unwavering support and encouragement throughout my study. Your love and prayers carried me throughout this journey and the completion of this research study.

Finally, I would like to give a special thanks to Amani. The light that shined in the last leg of this study. This one is for you.

ABSTRACT

The study evaluated cloud computing risks against IT governance frameworks. The research has become relevant because of the increasing reliance on cloud computing as a mechanism of data storage. Cloud computing is an IT service that is offered to clients on a contract basis by a third party that owns the infrastructure. Thus, organisations must consider the risks and mitigating controls to address these risks. Cloud computing risks, such as security risk, privacy risk, data integrity risk, availability and network capacity, data segregation and multitenancy risk, access controls, governance and data location risk are very common to organisations. Consequently, organisations must fully understand the impact of these risks and the mitigating controls provided by IT governance frameworks. An empirical study and a literature review were conducted to address the research problem and objective. An analysis was conducted on cloud computing risks in the context of IT Governance frameworks. The study found that IT Governance Frameworks play a vital role in mitigating cloud computing risks and organisations can place reliance on them when adopting the cloud.

Key Words

Client Organisation

Cloud Computing

Cloud Service Provider

Cloud Computing Risk

Information Technology Governance

LIST OF ABBREVIATIONS

CIO	Chief Information Officer
CSP	Cloud Service Provider
COBIT	Controls Objectives for Information and Related Technologies
DOS	Denial of Service
DNS	Domain Name Server
DHCP	Dynamic Host Configuration Protocol
HTTP/S	Hypertext Transfer Protocol/Secure
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IaaS	Infrastructure as a Service
IODSA	Institute of Directors in Southern Africa
ISO/IEC 27002	International Organisation for Standardisation and International Electrotechnical Commission (27002:13)
IP	Internet Protocol
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
PC	Personal Computer
PaaS	Platform as a Service
POPI	Protection of Personal Information
SLA	Service level agreement
SaaS	Software as a Service
SOA	Service-Oriented architecture
URL	Uniform Resource Locator
VM	Virtual Machine
VSwitch	Virtual Switch
XML	External Entity

Table of Contents

Contents

CHAPTER 1: INTRODUCTION AND STUDY LAYOUT

1.1 INTRODUCTION

In an ever-changing environment of information technology (hereafter, IT), the modern world is at liberty to share information, solve problems and process information at a much rapid pace, thus decreasing the space and time between people, nations and continents by allowing accessibility of information at one's fingertips. IT can be viewed as the complete scope of jobs that are associated with computer systems, internet and technology in business (Garrisona, Wakefield & Kimc, 2015).

Mitchell (2017) describes IT as a study, design, development, implementation, guide or management of computer-based record systems, particularly software program applications and computer hardware. It deals with the use of electronic computers and computer software to convert, store, protect, process, transmit and retrieve data securely (Mitchell, 2017). Whilst this may ease the operating system of an organisation, the evolution of IT poses new risks to organisations (Rama, 2016).

In a world where technology is constantly growing, the risks associated with the transformation of IT continuously change. There are three major types of IT risks, namely known knowns, known unknowns and unknown unknowns (Grimes, 2013). Organisations' daily operations include the transfer of information over the internet, financial transactions related to the business as well as sensitive personnel and client information (Adjei, 2015). More emphasis must be placed on ensuring that the organisation is not vulnerable to cyber-attacks and that this information is securely protected. It should be the organisation's priority to identify the risks they could face in the IT environment and formulate their risk appetite, risk tolerance and factors strategies to mitigate the risks from threatening the organisation's daily operations (Rama, 2016).

Technology continues to increase in strategic importance and in the complexity of its nature. Many companies therefore created a department whose main responsibility pertained to the oversight of IT related activities that are in line with the organisation's objectives. This brought about the creation of IT departments whose main objective is to ensure that there are no threats posed to the organisation in information security, computer technology support and business computer network and database administration (Mitchell, 2017). Buchy (2016) describes IT security as the method of implementing measures and systems designed to securely protect and safeguard information through utilising various forms of technology. He further explains that the data which organisations attempt to protect can either be electronic or on paper.

Most organisations' daily operations involve many computer networking activities closely related to IT and these include cloud computing services (Mitchell, 2017). Kuyoro, Ibikunle and Awodele (2011) define cloud computing as an IT service that is offered to clients on a contract basis by a third party that owns the infrastructure. Due to the overload in data and large amounts of power needed to process data, cloud computing is a cost-effective method that allows scalability, resilience, flexibility and efficiency. However, as cloud computing is an IT service, there are still security concerns related to it. Cloud computing security refers to the safety of the cloud concerning the running of applications, storing of data and the processing of transactions (Kuyoro et al., 2011).

In embracing the emergence of cloud computing as the best method to improve and enhance IT infrastructures in organisations, management should always be cognizant of the risks associated with cloud computing to avoid any future problems (Viswanathan & Senguttuvan, 2017). Every organisation uses services delivered from the cloud, whether it knows it or not (Ernst & Young, 2014). However, the biggest challenge which cloud service providers face relates to data security. Clients are worried about the privacy and security of their data, where it is located and the access controls in place. Handing over full control of physical access to their data poses many questions, such as whether these cloud service providers will ensure data does not

leak or fall into the wrong hands, or whether these cloud service providers have any disaster recovery plans in place (Chunming, Nguyen & Martin, 2013). In addition to this, clients are worried whether cloud service providers would notify them timeously in the event of any breaches, as this is a vital part of ensuring security and privacy of data (Dobrygowski & Bohmayr, 2017). Other challenges faced with cloud computing include the location of infrastructure, multi-tenancy, authentication and trust of acquired information, system monitoring, logs, cloud standards, compatibility, financial, operational and vendor risks, loss of ownership, contractual breaches and the disclosure and notification of the event and availability (Chunming et al., 2013). These cloud computing challenges will be discussed in the literature review on cloud computing risks in Chapter 3.

When considering the location of the cloud service provider, clients need to be vigilant of the laws and regulations of the cloud service providers' country, as this may affect the client in cases where disputes emerge. In addition, the fact that there are multiple users on the cloud means that cloud service providers need to protect all the different stakeholders and ensure that strict access controls are in place to avoid unauthorised access or modification of data (Chunming et al., 2013).

To ensure there is correct, secure and trustworthy adaptation of cloud computing services, clients need to take precaution when selecting potential cloud computing service providers. According to the Cloud Standards Customer Council (hereafter, CSCC) (2015), a client should be aware of the regulatory environment of the cloud service provider. The client must make sure that all their data and applications stored by the service provider comply to the relevant laws and legislation that govern the client's industry and determine if these policies are in line with the organisation's objectives. This should be included and clearly stated in both the client and service provider's Service Level Agreement (hereafter, SLA) (Paquet, 2013).

Cloud computing risks and benefits are also widely based on the cloud deployment and cloud service models that the client decides to use (Information Systems Audit and Control Association (hereafter, ISACA), 2011). CSCC (2015) lists the cloud deployment models as public, private, hybrid and community, while the cloud service models consist of software as a service (hereafter, SaaS), infrastructure as a service (hereafter, IaaS) and platform as a service (hereafter, PaaS).

In terms of SaaS, the responsibility related to security lies entirely on the cloud service provider, as the infrastructure and software belongs to the cloud service provider. On the other hand, with IaaS, the cloud service provider supplies the client with all the resources needed to run the cloud service and it is entirely the responsibility of the client to ensure there is security when running the cloud computing service (CSCC, 2015). The cloud deployment methods and cloud service models need to be addressed in the SLA and these will be addressed further in Chapter 3.

1.2 BACKGROUND TO RESEARCH PROBLEM

Cloud computing has been a growing trend since the year 1950. Organisations have since moved from utilising a single computer, using terminals, to an increased number of computer systems enabled by the invention of virtual machines. This improved the efficiency and effectiveness of communication within the business environment and the increased use and production of virtualised private network connections (Zissis & Lekkars, 2010). Cloud computing has therefore eliminated the use of isolated data connections and has allowed companies to share internet connections from one physical structure. Considering the large amount of data companies must store, cloud computing offers a quick build and the efficient management of applications at a reduced cost (Aldossary & Allen, 2016). There is also an added benefit in reducing IT costs by cutting down on power, carbon footprint and consolidating servers (Slaheddine, 2012). With security being a concern for most organisations, the need to leverage the low-cost advantages of cloud computing security solutions, without

compromising corporate or customer information, is vital (Kuyoro, Ibikunle & Awodele, 2011).

One of the benefits of using cloud computing is the correct implementation of the service, something achieved by following guidelines or Frameworks which allow sound governance in the use of cloud computing services (Akande & Van Belle, 2014). This can be achieved by acquiring knowledge on IT Governance Frameworks available. These would then assist the organisation to effectively handle or manage cloud computing risks.

The challenge that most organisations have in adopting cloud computing services stem from not having enough knowledge on how to govern the cloud within the business environment (Van Ketwich, 2012). Such knowledge assists organisations in adopting cloud computing in a more regulated environment, which allows transparency, integrity and data security in cloud computing (Institute of Directors Southern Africa (hereafter, IoDSA), 2016). ISACA (2011) also gives some guidance on IT Control Objectives for Cloud Computing and addresses how organisations may successfully adopt cloud computing.

Ramgovind, Eloff and Smith (2010) note the need to address the governance of cloud computing and the drawing up of necessary Frameworks to ensure that organisations can effortlessly adopt cloud computing. The users of cloud computing services need to be in a position where they can trust their service providers to react quickly and be always available. This gives their clients assurance that their data is secure and protected and that the regulatory Framework enforces transparency and respect for data integrity (Ramgovind et al., 2010).

The following IT Governance Frameworks may assist organisations in the implementation of cloud computing services and reduce cloud computing risks. These include ISACA regulated Frameworks, Controls Objectives for Information and Related Technologies (hereafter, COBIT), Framework on Security and Privacy

Controls for Information Systems and Organisations by the National Institute of Standards Technology (hereafter, NIST), International Standard ISO/IEC 27002 and Protection of Personal Information Act (hereafter, POPI). IT Governance Frameworks that are most profoundly used as reference in addressing IT Governance related issues were selected for the study. Globally, the ISO/IEC 27000 series, COBIT and NIST are the most used governance Frameworks in addressing various risks related to IT for any given industry (Wild, 2018). Wild (2018) also refers to industry best practice standards related to the handling of personal information such as credit card information, medical information and privacy laws. This motivated the choice of the selected POPI Act that addresses confidentiality and privacy of personal information.

ISACA (2011) states that organisations can only optimise the use of cloud computing services if they have a sound management and strategy plan that can effectively direct the implementation of cloud computing services to the objectives of the organisation. This effectively forces the organisation to consider risk, security and compliance with IT related matters and the implementation of cloud computing services. The increased use and dependence on external IT service providers, with the aim of ensuring that risks are minimised, and external IT services providers deliver value added services that support the objectives of the organisation, is analysed by COBIT (2018).

According to NIST (2020), the Framework's aim is to assist organisations in identifying, assessing, responding and managing IT risks intrinsically and extrinsically. This means that cloud service providers and the organisation using the services from the cloud service provider can use this Framework to minimise risks associated with cloud computing during its implementation and its use. These include the privacy of data, which entails customer information, employee and organisational data.

The POPI Act applies to all organisations that process personal information (Republic of South Africa Protection of Personal Information Act: 2013). In implementing the use of cloud computing services, organisations need to be cautious of the data they store on the cloud. Welz (2016) describes personal information as employee and customer details (ID numbers, email addresses, bank account details, and medical records

etcetera). Both the organisation and cloud computing service providers need to be wary of the risks around privacy and ensure that data is not breached and is limited to a certain level of authority within the organisation. Organisations must also consider the cloud service model they choose to deploy, and the risks associated with the model and avoid infringing on the protection and privacy of personal information (Welz, 2016).

The International Standard ISO/IEC 27002 (2013) is a useful guide in assisting organisations to develop controls around information security and privacy risks associated with the use of cloud computing services offered by third party service providers. It highlights the potential costs and losses related to the failure of addressing risks related to IT and its ability to successfully implement and run cloud computing services. Further discussion on IT Governance Frameworks will be addressed in Chapter 4 (IT Governance Frameworks) of the study.

1.3 RESEARCH PROBLEM

As discussed above, the challenge that organisations have with adopting cloud computing, relate to data security, privacy, access controls, availability and governance of the cloud. Governance of the cloud is a set of guidelines or controls used to manage critical data stored on the cloud (Gunadham & Kuacharoen, 2016). The intention is to protect the client organisation's data against potential cloud computing risks during the time it is hosted on the server of the cloud service provider. The cloud service provider may be located within the Republic of South Africa or anywhere else in the world, which poses its own risks, as laws and regulations differ around the globe (Yimam & Fernandez, 2016). Being an IT related system, the cloud would be best governed by the industry's best practice Frameworks related to IT. It is; therefore, not clear what role IT Governance Frameworks play in addressing the challenges and risks associated with cloud computing. Thus, the stated research problem is "the role IT Governance Frameworks play in addressing cloud computing risks".

1.4 RESEARCH OBJECTIVES

The aim of this study is to understand:

1. The risks faced in implementing cloud computing applications by organisations,
2. The IT Governance Frameworks available to assist in mitigating the cloud computing risks; and
3. Which IT Governance Framework can best be applied by organisations in managing and improving their cloud applications whilst mitigating these risks?

To achieve the above objectives, a literature review will be conducted. Chapter 3 will focus on cloud computing risks and Chapter 4 on IT Governance Frameworks. Chapter 5 will discuss the empirical study and the findings in terms of how the cloud computing risks are addressed by the different Frameworks selected for this study.

The study will focus on the transformation of cloud computing and its adaption during the periods of 2012 to 2020 in order to extract meaningful characteristics in its improvement in cloud computing risks. From this timeframe, risks associated with the implementation of cloud computing applications and the IT Governance Framework which can assist in reducing cloud computing risks will be identified.

1.5 CONTRIBUTION OF THE STUDY

The Limited Scope Dissertation will enhance knowledge of the application of IT Governance Frameworks to cloud computing applications risks. The researcher aims to use the IT Governance Frameworks to address cloud computing risks and add to the existing literature. The motivation behind this stems from the challenge organisations have in governing information in the cloud (Deacutis, 2015).

1.6 ETHICAL CONSIDERATIONS

Information used in this study was collected from databases at the University of Johannesburg's online library. Research publications, journals, academic articles, textbooks and credible internet sources were obtained. Credit for the research is given

to various authors, web pages and organisations that had the necessary information the researcher needed to conduct the study. The researcher was also cleared by the School of Accountancy Research Ethics Committee and it was established that the study was of minimal risk since the researcher only used publicly available data. The researcher used the Harvard referencing technique of the University of Johannesburg for all referencing.

1.7 LIMITATIONS TO THE STUDY

Due to the limits placed on the length of the Limited Scope Dissertation, the researcher had to limit the number of Frameworks to ISO/IEC 27002, COBIT, NIST and the POPI Act. Only a few Frameworks give guidelines based solely on cloud computing and since cloud computing is an IT running application, the IT Governance Frameworks are deemed reliable tools in addressing these risks.

1.8 STUDY LAYOUT/OUTLINE

Chapter 1: Introduction

In this Chapter, the background information of the study is discussed, including the problem statement, the research objectives and the contribution of the study.

Chapter 2: Research Methodology

This Chapter explains how the researcher extracts information pertaining to the study and the ethical considerations to be adhered to.

Chapter 3: Cloud Computing Risks

Cloud computing risks are discussed at length, explaining how these risks affect organisations in adopting cloud computing applications.

Chapter 4: IT Governance Frameworks

This Chapter discusses mitigating controls recommended by the selected IT Governance Frameworks on the cloud computing risks identified in Chapter 3.

Chapter 5: Empirical Study and Research Findings

This Chapter maps the cloud computing risks against the selected IT Governance Frameworks and recommend which IT Governance Framework best addresses the cloud computing risks.

Chapter 6: Conclusion

In this Chapter, conclusions are drawn from the literature review and recommendations for areas of improvement are given.

1.9 CONCLUSION

Chapter 1 provided background information on cloud computing applications. Cloud computing was defined to illuminate where cloud computing, as a service, emanated from and definitions of cloud computing risks and benefits were discussed. Further discussions on challenges faced on the cloud were explained and it was evident from the literature that the risks associated with cloud computing are a concern for most organisations seeking the adoption of cloud computing. The research explores issues that affect organisations in the implementation of cloud computing services and the risks associated with cloud computing. IT Governance Frameworks are used to address cloud computing risks that can assist organisations to easily adapt cloud computing services. The following chapter describes the research design and methodology adopted in the study.

CHAPTER TWO: RESEARCH DESIGN AND RESEARCH METHODOLOGY

2.1 INTRODUCTION

This Chapter discusses the research methodology used to examine “the role of IT Governance Frameworks in addressing cloud computing risks”. In Chapter 1, cloud computing risks that affect organisations in the implementation of cloud applications, as well as IT Governance Frameworks that would address the cloud computing risks, were identified and briefly explained. The objective of the study is to provide a sound understanding of how these IT Governance Frameworks will address or improve an organisations’ cloud applications by mitigating risks. This Chapter outlines the research design and methodology used in the research.

2.2 RESEARCH DESIGN

Research design is a technique followed to address the research problem and achieve the research objectives resulting from it (Ling Lin, 2019). It speaks to the strategies and techniques for gathering and assessing information while providing suitable recommendations for the study on cloud computing risks and IT Governance Frameworks (Rajasekar, Philominathan, & Chinnathambi, 2013).

Rajasekar et al. (2013) describes a research design in three approaches, that is, a qualitative research approach, quantitative research approach and mixed methods research approach. The mixed method research approach is a combination of both qualitative and quantitative research approaches. To answer the research problem, a qualitative research approach is used.

The qualitative research approach is subject to the views, behaviours and analysis of attitudes (Johnson, Adkins & Chauvin, 2020). The results can give some indication on why, how and when something occurs. Its nature is the collection and analysis of primarily non-numerical data in the form of secondary data. Secondary data can either be in the form of published or unpublished data. To obtain published data, databases from the University of Johannesburg online library are used to obtain research

publications, journals, academic articles, textbooks and internet sources related to the problem. The goal is to collect data that is relevant for addressing the research problem and research objectives (Bryman & Bell, 2014).

The research objectives are addressed through a literature review in Chapters 3 and 4, and an empirical study in Chapter 5. The empirical study analyses how the different Frameworks selected for this study address the various cloud computing risks identified in the literature review. Secondary data is used in the literature review and empirical study. The goal of the study is to understand the cloud computing risks faced by organisations when implementing cloud computing applications. In addition, the researcher aims to determine the extent to which organisations can use IT Governance Frameworks to manage and improve their cloud applications by mitigating the risks identified. Therefore, the overall design takes an exploratory approach also known as formulative research studies. An exploratory design is defined as the design performed where there are few studies to depend on to predict a result (Mamaile, 2018).

The results of exploratory research are not usually useful for decision making, but they can provide significant insight into a given situation. The fundamental value of these studies is the ability to develop a research problem in a field of study. This study provides a chance to consider various outcomes and results from the research problem and research objectives. This includes:

- Understanding the general principles, background and concerns;
- Providing a detailed depiction of the condition being established;
- Developing new ideas and assumptions; and
- Evaluating whether further studies are achievable in future (Mamaile, 2018).

This allows flexibility in the study because the research problem, extensively described at first, is changed into one with more detailed meaning in exploratory studies (Creswell, 2003). A qualitative exploratory design is used in the sense that available literature on cloud computing risks and IT Governance Frameworks is reviewed. An understanding of how the IT Governance Frameworks can provide mitigating controls

against cloud computing risks and an evaluation of which IT Governance Framework provides the best controls in mitigating these risks are also conducted.

Examples of the exploratory research includes studies of concerning literature and experience studies. The study of concerning literature happens to be the most basic and productive technique for detailing the research problem. Theories expressed by earlier authors can be investigated and their usefulness assessed for further research. Such studies are also used to make recommendations and generate new speculations. The research therefore reviews and expand on work previously done by others using an exploratory research study of concerning literature (Creswell, 2003).

2.3 RESEARCH METHODOLOGY

Research methodology is a method or system used to identify, select, process and examine data on a topic. It is the process of discovering answers to logical and social issues through goals and deliberate investigations and studying how research can be carried out (Rajasekar et al., 2013). In describing the research methodology, the researcher must follow the following steps:

Step 1: Define the research problem

When conducting research, a research topic must first be defined (Langos, 2014). In this study, the importance of IT Governance Frameworks was recognised since cloud computing applications are closely related to IT. The research problem relates to the role of IT Governance Frameworks in addressing cloud computing risk to establish whether these IT Governance Frameworks truly address cloud computing problems. The research topic was formulated to understand how best cloud computing could be adopted and implemented by organisations fully informed on how best to mitigate risks.

Step 2: Review literature

A literature review will be carried out in Chapters 3 and 4. The purpose of the literature review is to inform readers about the cloud computing risks faced by organisations

when implementing this service and the role that IT Governance Frameworks play in managing and improving their cloud applications by mitigating these risks. The discussion in these Chapters is carried out by using secondary data.

Step 3: Prepare the research design

The research design adopted in this research is explained in section 2.2.

Step 4: Collect data

This section specifies the methodology used for the collection of data which, in this study, was secondary data. Data is observational proof deliberately gathered as per the requirements and techniques of the study. Secondary data is initially gathered for an alternate purpose and reused to address another research question (Mamaile, 2018).

Population

A population is a collection of items under consideration in a research field (Majid, 2018). One of the research objectives in this study is to understand how organisations can use IT Governance Frameworks in mitigating cloud computing risks. For the purposes of this study, the population consists of all the IT Governance Frameworks in the IT industry. Some of these Frameworks include ISO/IEC27001, ISO/IEC27002, ISO/IEC38500, COBIT, NIST, POPI Act and Information Technology Infrastructure Library (hereafter, ITIL).

Sample

A sample is a portion that represents the whole population (Taherdoost, 2016). In selecting the sample, the non-probability sampling method was used. In this sampling method, personal judgement is used to select elements that are a representation of the population (Rajasekar et al., 2013). In this study, the sample consisted of the ISACA regulated Frameworks COBIT, NIST, ISO/IEC 27002 and the POPI Act. ISO/IEC 27001/ISO 27002, NIST Framework and COBIT are among the 23 Top

Cybersecurity Frameworks (Mutune, 2020). These IT Governance Frameworks are commonly used by organisations to address third party service delivery and quality of service, which is essential in the successful implementation of the cloud. They also address the risks related with cloud computing and recommend procedures to address these risks (Nyandongo & Mxobo, 2018).

The POPI Act addresses the lawful processing of personal information and privacy regulations. These IT Governance Frameworks facilitate the implementation of cloud computing in a way that pursues principles of good governance in organisations (Solms & Willet, 2016).

Step 5: Reliability and Validity of Data

Validity

Validity is the degree to which data gathering methods and the research findings correspond to what they claimed to address (Saunders & Lewis, 2018). All data collected will address cloud computing risks and utilise the IT Governance Frameworks listed in Chapter 1. The most significant cloud computing risks will be addressed.

Validity was achieved using ISO/IEC 27002, COBIT, NIST and the POPI Act Frameworks to ensure different perspectives were represented in addressing cloud computing risks. The researcher also used existing literature to reduce research bias when addressing cloud computing risks.

Reliability

Reliability is the degree to which data gathering methods and investigation techniques result in reliable findings (Heale & Twycross, 2015). The collection of data was limited to the periods 2012-2020. This was to ensure data collected was relevant to the study. Data was collected from reliable online sources including the University of

Johannesburg online library, professional associations and organisations with expertise in cloud computing and IT Governance.

Step 6: Analyse the data

The analysis of data follows a qualitative approach. During this process, the IT Governance Frameworks listed above are analysed. The analysis is done to establish whether the cloud computing risks identified are addressed by these IT Governance Frameworks. To determine whether cloud computing risks are indeed addressed by the IT Governance Frameworks, the precise extent to which they address each cloud computing risk is analysed. This analysis is carried out in Chapter 5 of the study.

Step 7: Interpret the data

During this process, the results of the study are interpreted. From the analysis, the researcher will determine which IT Governance Framework best addresses the cloud computing risks. The interpretation of data will determine if:

- The IT Governance Frameworks selected address none of the cloud computing risks.
- The IT Governance Frameworks selected address some of the cloud computing risks.
- The IT Governance Frameworks selected address all the cloud computing risks.

From the interpretation of data, it can be determined which of the four selected IT Governance Frameworks is adequate for use by organisations in implementing cloud computing applications. This will assist organisations to mitigate risks.

2.4 CONCLUSION

The purpose of this chapter was to describe the research design and methodology used in addressing the research problem and research objectives. The IT Governance Frameworks that would address cloud computing risks were identified. Cloud

computing risk and IT Governance Frameworks are described in detail in Chapter 3 and 4.

CHAPTER 3: CLOUD COMPUTING RISKS

3.1 INTRODUCTION

In this chapter, a literature review on the cloud computing risks that organisations are likely to face is conducted. The review begins by introducing a background on cloud computing, by defining what cloud computing is and its growing popularity in the world. The review then describes the cloud deployment services and cloud service models offered. This informs the reader on the products offered by cloud computing service providers and the options organisations can choose from. The review will end by discussing the risks related to cloud deployment services, the cloud service models, and the myriad of cloud computing risks.

3.2 CLOUD COMPUTING

Cloud computing is a computing model, supplied by a third party on a contract basis, which enables one to access an IT service over a network at any given time (Solms & Willet, 2016). The term cloud computing has created a great deal of enthusiasm with many organisations worldwide embracing the different services it has to offer (Caldarelli, Ferri & Maffe, 2016). It is therefore imperative that the senior management of any organisation with IT systems stay abreast with the ever-evolving IT opportunities and benefits such as cloud computing (Von Solms & Viljoen, 2012). Cloud computing is an advanced technology system made up of four cloud deployment models and three cloud services models (Hussein & Khalid, 2016).

3.2.1 CLOUD DEPLOYMENT MODELS AND CLOUD SERVICE MODELS

Cloud computing is classified by its location. There are mainly four cloud deployment models, namely the Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud (Jakimoski, 2016). These models cater for various organisational needs depending on the objectives of the organisation. Manivannan and Zeadally (2016) define the Public Cloud as infrastructure held by the cloud service provider and the Private Cloud as infrastructure designed solely for an organisation's specific needs which cannot be shared. The Hybrid Cloud is the combination of both the public and private cloud

services while Community Cloud is a combination of organisations of the same industry or needs that share the same cloud infrastructure (Schneider & Sunyaev, 2016).

These four cloud deployment models are run on either one of the following cloud service models, namely IaaS, PaaS and SaaS (MacDonald, 2017). IaaS provides the infrastructure and storage space needed to provide the cloud service. PaaS offers the environment for the client to develop or accommodate cloud services. SaaS generally focuses on individual buyers or business organisations (Adjei, 2015).

The combination of the cloud deployment model and cloud service model provides organisations with the capacity to access computing resources in a flexible environment, without the budgetary cost of a conventional IT environment (Schneider & Sunyaev, 2016). When selecting a cloud deployment and cloud service model, it would therefore be imperative for the organisation to be aware of the risks associated with the cloud deployment and cloud service model selected. A portion of these risks (depending on the model selected) are the responsibility of cloud service providers while some risks are the responsibility of the organisation purchasing the cloud model (Morsy, Grundy & Müller, 2016).

3.3 CLOUD COMPUTING RISKS

As much as cloud computing has many benefits to offer, such as cost-effective rates, reduced IT costs and increased technological flexibility, there are several risks that cannot be ignored and should be addressed thoroughly to avoid any significant losses to the organisation (Changchit & Chuchuen, 2016). For organisations to maximise on the benefits offered by cloud computing, they must confirm that the use of cloud computing offers efficient, effective, secure and compliant services that add value to the organisation (Solms & Willet, 2016).

Below is an explanation of the risks associated with cloud computing, and how these risks affect the cloud deployment and service models mentioned in section 3.2.1 above. These cloud computing risks should be mitigated for the organisation to

maximise the benefits cloud computing offers. Below, the researcher discusses cloud computing risks associated with the cloud service models and cloud deployment models before addressing the security, privacy, data location, availability, access control, network capacity, integrity, data segregation, consumer and governance cloud computing risks.

3.3.1 CLOUD DEPLOYMENT AND CLOUD SERVICES RISKS

For an organisation to fully prepare its environment against the potential loss of data, it must fully understand the risks around the cloud models it selects. Below, the risks associated with cloud service models and cloud deployment models are discussed.

3.3.1.1 INFRASTRUCTURE AS A SERVICE (IAAS) MODEL

In instances where the organisation chooses to adopt IaaS, it must fully understand that the risks associated with the cloud service model are its responsibility. The organisation's IT security team would have to ensure that the IaaS is not vulnerable to attacks, viruses or malware that may compromise the security or privacy of data stored. The security controls it would have naturally applied on its traditional physical servers would have to be applied to the IaaS model. The level of security control should be based on the objectives of the organisation, its needs and risk appetite. The IT security team should also have security controls to mitigate the risk of severe threats when operating on- and offline (Morsy et al., 2016).

3.3.1.2 PLATFORM AS A SERVICE (PAAS) MODEL

Where an organisation selects the PaaS model, the security risks are shared between the cloud service provider and the client organisation (also referred to as cloud consumer for the purposes of this literature review). The PaaS model is built on a Service Oriented Architecture (hereafter, SOA) model (Morsy et al., 2016). This essentially means that both the cloud service provider and client organisation will have to implement controls to mitigate the following security risks in the SOA domain:

- Denial of Service (DOS) attacks:
  “DOS is a digital attack where the culprit attempts to make a machine or system asset inaccessible to its proposed clients by incidentally or inconclusively disturbing administrations of the host associated with the web" (Hussein & Khalid, 2016:53).
- Man-in-the-middle attacks:
  “Man-in-the-middle attacks is an attack where the aggressor subtly transfers and perhaps adjusts the correspondence between two parties who perceive they are legitimately speaking with one another" (Gangan, 2015:1).
- External Entity (XML-related) attacks:
  “Is an attack against an application that analyses XML input. This attack may prompt the divulgence of undisclosed information, denial of service, server-side request falsification, port examining from the point of view of the device where the analyser is found and other framework impacts" (Hussain, Fatima, Saeed, Raza & Shahzad, 2016:3).
- Replay attacks:
  “Is an attack that allows a cybercriminal to spy on secure network communication, interrupt it and then purposefully delays or redirects the receiver to perform an action the cybercriminal wants. The hacker achieves this by using a malignant element, which blocks the information and redirects it” (Binance Academy, 2019:1)
- Dictionary attacks:
  “Is an endeavour to increase unlawful access to a PC framework by utilising an exceptionally huge arrangement of words to create potential passwords" (Adam, 2017:17).
- Injection attacks and input validation related attacks:
  “Are attacks in which the objective is execution of subjective directions on the host working framework through a vulnerable application. These attacks are conceivable when an application passes risky client provided information (shapes, treats, HTTP headers) to a framework shell. In this attack, the hacker provides working framework directions which generally execute the benefits of the vulnerable application. These attacks are conceivable to a great extent because they lack information approval. This attack contrasts from code infusion, in that code infusion enables the hacker to include his own code that is then executed by

the application. The hacker expands the default usefulness of the application, which execute framework directions, without the need of the infusing code" (Manivannan & Zeadally, 2016:6).

3.3.1.3 SOFTWARE AS A SERVICE (SAAS) MODEL

In the SaaS model, the responsibility of ensuring there is security on the cloud and maintaining this security is a shared responsibility of the cloud service providers as the software service providers. The SaaS model is affected by the security risks within the IaaS and PaaS models as it is run on both platforms (Schneider & Sunyaev, 2016).

Karajeh, Maqableh and Masa'deh (2016) state that the risks associated with the SaaS model include data location, integrity, data segregation, access, confidentiality, backups and network security. Network applications on the cloud must be scanned and ratified for vulnerabilities. There must be continuous monitoring of all vulnerabilities and attacks reported and these should be maintained in the National Vulnerability Database (NVD). Storing this data enables cloud and software service provider access to automation of vulnerability management, security measurement and compliance. The NVD also includes databases of security checklist references, security related software flaws, misconfigurations, product names and impact metrics. Network application firewalls should be in place to alleviate any security vulnerabilities detected. The service providers must also ensure there is no misconfiguration on the network application especially where there is multi-tenancy, as this may create security loops (Hussain et al., 2016).

3.3.1.4 COMMUNITY OR PUBLIC CLOUD DEPLOYMENT MODEL

Where an organisation decides to adopt the community or public cloud deployment model, there is a risk that the different clients on the network could be vulnerable to the exploitation of the following:

- Domain Name System servers (hereafter, DNS):

"Which is the web's framework that changes alphabetic names into numeric IP addresses. For instance, when a Web address (URL) is composed into a program, DNS servers return the IP address of the Web server related with that name" (Iqbal, Kiah, Anuar, Daghighi, Wahab & Khan, 2016:15).

- Dynamic Host Configuration Protocol (hereafter, DHCP):
  "Which is a convention for appointing dynamic IP addresses to tools on a system. With dynamic addressing, a tool can have an alternate IP address each time it associates with the system. In certain frameworks, the tool's IP address can even change while it is connected" (Patil & Kulkarni, 2017:1).
- Internet Protocol (hereafter, IP) vulnerabilities:
  "Is an advanced media transport Framework that keeps running over standard IP systems" (Tsou & Lusher, 2015:1).
- Virtual Switch (hereafter, vSwitch) software:
  "Is a product application that permits correspondence between virtual machines. A vSwitch accomplishes something other than forward information parcels, it wisely coordinates the correspondence on a system by checking information bundles before moving them to a goal" (Ibrahim, Harris & Grundy, 2010:1).
- Which would result in a network based Virtual Machine (hereafter, VM) attack:
  "Is a product PC that, like a physical PC, runs a working framework and applications. The virtual machine involves a lot of particular and arrangement records and is supported by the physical assets of a host" (Ibrahim et al., 2010:2).

In both the community and public cloud deployment models, the security and responsibility of the VM boundaries is the responsibility of the cloud service provider (Khan & Al-Yasiri, 2016). The cloud service providers would need to be conscious of the risks associated with VM templates that may have information of the previous owners and could be easily exploited by the new consumers and passed off as their own (Jones, Irani, Sivarajah & Love, 2017). It would also be noteworthy to mention that there is reduced ability to alter the public cloud system to suit the organisation fully, as control lies with the cloud service provider (Jones et al., 2017).

3.3.1.5 PRIVATE CLOUD DEPLOYMENT MODEL

Organisations that select the private cloud are at an added advantage. Private cloud means the infrastructure is designed solely for that organisation's specific needs and cannot be shared. This, on its own, aids to better security and privacy of data. The organisation's environment is handled by the employees (Goyal, 2015). This however does not necessarily mean that the private cloud is not prone to the same security risks as that on the public cloud. The risks are, however, slightly lower (Goyal, 2015).

Trust is a significant factor for any organisation when handing over the direct control of data to the cloud service provider (Shaikha & Sasikumarb, 2015). Organisations must get comfortable with the idea of not being in full control of their IT resources and entrusting this control to the cloud service provider. Strong security controls are imperative for any cloud model to so that information is not breached or stolen by tenants sharing the same cloud model (Sehgal, Bhatt & Acken, 2019). Selecting the right or best cloud service provider guarantees the client quality security controls and protection of data (Hussain et al., 2016).

3.3.2 SECURITY RISK

In preventing a system from being susceptible to cyber-attacks or risks, the cloud service provider guarantees the protection of physical access and location of the cloud infrastructure, systems and data, while the client organisation puts in place controls for logical access to the network, operating systems and the databases (Farrag & Nasr, 2017). It is important that the client organisation implements strong security controls to mitigate the risk of poor access management, data leaks, data loss, DOS attacks, malware and misconfigured cloud storage that could leave the organisation vulnerable to cyber-attacks. This can be guaranteed by having a cloud security system that has multi-factor authentication, data at rest encryption, firewalls and consistently monitors access (Hussain et al., 2016).

The client organisation must also be cognisant of security risks related to human error, which emanate from phishing emails or downloads of unapproved software and poor password protection controls. This is usually a result of lack of security user training awareness programs that keep the client's employees informed and alert to the ways of protecting the organisation's systems and data (Sehgal et al., 2019).

3.3.3 PRIVACY RISK

Privacy and confidentiality refer to restrictions of who is authorised to access information on the cloud. Confidential information, if breached, can easily be manipulated or used as ransomware against an organisation. It is important for the cloud consumer, before entering into a contract with the cloud service provider, to read the terms and conditions to avoid the risk of unknowingly agreeing to have their information shared with other parties (Mukherjee, Matam, Shu, Maglaras, Ferrag, Choudhury & Kumar, 2017).

Farrag and Nasr (2017) explain two cloud structures that cloud consumers can select to best suit the needs of their organisations and reduce privacy risks. These two cloud structures are the Domestic and Trans-border cloud structure. In the Domestic Cloud structure, the cloud infrastructure is physically located in the cloud consumer's premises. This reduces privacy risks as the cloud consumer is aware of where the data is located and collected; and the users with authorisation to access the data. In the Trans border cloud structure, the data is transferred across borders. In this structure, the privacy risks are much higher as the cloud consumer is nowhere close to where the data is located and has no visual capacity to investigate whether the data is stored correctly and safely. There is also the underlying risk of unauthorised access to data. International laws and governing structures of where the data is located may also pose privacy risks, especially in countries where there are no laws related to privacy and protection of data (Karajeh et al., 2016).

3.3.4 DATA LOCATION

Cloud service providers are not all situated in one location but are rather dispersed all through the globe. As information is stored in numerous physical areas, there is a risk of inaccessibility of data by the cloud consumer (Hussein & Khalid, 2016). This could prevent the organisation from the ability to monitor or keep track of movement of data within the cloud and the data centre where it is stored (Mukherjee et al., 2017).

3.3.5 AVAILABILITY

Availability is key in building trust with consumers and essentially means the ability of the consumers to retrieve their information at any given time. Cloud services should continue operating regardless of the differences in location for both the cloud consumer and cloud service provider. The cloud service provider should therefore ensure it does not over-burden its systems and there are no periods of downtime where cloud consumers are unable to retrieve their data due to the systems crashing or failing (Chandran & Angepat, 2012).

System crashes result in periods of unavailability which could lead to the undesired reputational risks for the cloud service provider and loss of consumer confidence (Manivannan & Zeadally, 2016). The absence of client confidence can also be escalated with lack of transparency from the cloud service provider in the event of a breach or system failure. Cyber-attacks and natural disasters also pose substantial risks to the functionality of a system. Viruses, malware, DOS, floods, earthquakes and fire could disrupt service delivery for hours on end, depending on the severity of the attack or disaster. It is important that the cloud service provider has a disaster recovery plan to minimise partial or complete loss of data which could result in financial loss or the complete shutdown of the cloud consumer's business. It is important that the cloud continue operating even in the event of a disaster or cyber-attack (Manivannan & Zeadally, 2016).

3.3.6 ACCESS CONTROL

Access to the data on the cloud should be restricted to authorised personnel of the organisation only. Continuous monitoring of access and logs of the cloud should be reviewed by the senior management of the organisation frequently (Mukherjee et al., 2017). The cloud service provider should provide these logs to cloud consumers, especially on the Public and Community Cloud deployment models that are not run by the cloud consumer themselves. The cloud consumer should be permitted to have these logs audited for cyber security reviews to minimise and identify vulnerabilities (Kumar, Raj & Jelcianac, 2017).

3.3.7 NETWORK CAPACITY

Iqbal et al. (2016) states that when planning and implementing cloud computing services, adaptability and versatility ought to be viewed as significant before implementing the cloud system. Servers crash because of high volume movement of information between systems that are not set up to hold such high volumes. Cloud system failures can be a signal of poor network assessment of the computing system. To avoid this risk, cloud consumers should be wary of the amount of storage they have available on the cloud. Failure to do so could put them at risk of having their data storage capacity limited without their knowledge (Chandran & Angepat, 2012). Poor performance is also common with new systems due to incorrect volume expectations. Sharing internal and external servers may present new risks because of the time required for information to move to external systems (Farrag & Nasr, 2017).

3.3.8 INTEGRITY IN CLOUD COMPUTING

Part of data security on the cloud is knowing that data cannot be altered by unauthorised personnel. Investor confidence is built when consumers know that their information is safe and secure and that strong security controls are in place (Karajeh et al., 2016). In cloud computing, information legitimacy, quality and security influence the systems activities and results produced. For a cloud service provider to ensure there is integrity on the cloud, they must adhere to change management, systems and

incident management agreed on in the SLAs. Adherence must be conducted with practicality, transparency, precision, approval and completeness (Velumadhava & Selvamanib, 2015).

3.3.9 DATA SEGREGATION

Data segregation is not effectively implemented in all cloud settings. Cloud service providers sometimes fail to isolate data to the specific needs of the cloud consumer. Some cloud consumers do not encrypt their data due to the fear that encryption may result in complete loss of data (Iqbal et al., 2016). When servers are compromised, servers are closed at whatever point for data to be recovered. During data recovery there could be replication of data in various sites. This means data is not accessible during the recovery period for the cloud consumer. The recovery of data must be brisk and complete to prevent further risks of replicating data to the wrong cloud consumer (Kumar et al., 2017).

It is important that in cloud deployment models such as the Public Cloud, data segregation is fully implemented for the different cloud consumers. Data can easily be destroyed because of a cyber-attack that would be significant to the cloud consumers. To avert these attacks, cloud service providers need to encrypt cloud consumer data so that their information is not hacked (Velumadhava & Selvamanib, 2015).

3.3.10 CONSUMER RISK

Before selecting a cloud computing service, client organisations need to acquaint themselves with the product and assess whether the product speaks to the strategies and objectives of the organisation and the risks prone to the selection of that product. It is however not possible for the consumer to cover pretty much all risks pertaining to that product (Chandran & Angepat, 2012). Cloud service providers are governed by the contracts they draft, which do not involve any contribution from the client organisation. It is also highly likely that the cloud service provider may not include rights to changes in the terms and conditions of their contract with the cloud consumer.

To cover all the necessary bases and avoid consumer risks, the client organisation should thoroughly go through the Universal Terms of Service, Additional Terms, Program Policies, Privacy Policy and Copy Right Notices prior to signing the contract with the cloud service provider (Iqbal et al., 2016).

3.3.11 MULTI-TENANCY

Multi-tenancy is a software architecture pattern where a single application instance is simultaneously utilised by multiple users over the internet. Applications that leverage multi-tenancy allow multiple customers to access the same application server and database. This contrasts with applications that utilise single tenancy. Single tenancy is structured so that each customer gets their own server and database (Morsy et al., 2016). Most of these servers are hosted by the customers themselves, giving them complete control over the system. With multi-tenancy there is a strong need to secure these servers and databases to prevent privacy and confidentiality risks. The cloud service provider must ensure there is separation and inaccessibility among tenants during the transfer of data, storing and service delivery (Ibrahim et al., 2010).

3.3.12 LACK OF GOVERNANCE

As a result of the cloud computing risks mentioned above, Deacutis (2015) emphasises the need for cloud computing governance and oversight of policies and standards for all organisations that plan to adopt or have cloud computing applications in place. Poor cloud governance can result in cyber-attacks, financial losses and reputational risks. This places senior management jobs at risk for failing to protect the organisation's intellectual property (Ketwich, 2012). Deacutis (2015) suggests that a board with a strong Chief Information Officer (CIO) should formulate strong policies with regards to data security, custody of documents and deletion of data, response to a security breach and methods on how to address cloud computing risks. For the purposes of this literature review, IT Governance Frameworks that organisations can implement to mitigate the cloud computing risks as discussed above, and to facilitate secure implementation of cloud computing services, will be identified. In the section

below, the researcher will discuss the importance of SLA's and how a well drafted SLA can aid in the reduction of cloud computing risks in an organisation.

3.4 SERVICE LEVEL AGREEMENTS

When an organisation has selected its cloud service provider, cloud deployment and service model that suit the needs, objectives and design of its organisation, an SLA must be drawn up. The SLA must define the responsibilities, roles and expectations of both the cloud service provider and the organisation purchasing these services. The definition of responsibilities gives assurance, to both parties, on the availability and ability to retrieve information at any given time (Alali & Yeh, 2012).

It is the responsibility of the senior management of the organisation to know where their data will be stored and which data they would want to store on the cloud. All risks relating to security, protection of the data, its accessibility on the cloud and legal issues related to the location of the cloud service providers must be addressed prior to accepting their services (Morsy et al., 2016). Senior management must also assess the policies of the cloud service provider and how these policies affect its presence on the organisation's network. These policies should include restriction of websites that may not be fully safe and could bring viruses to the organisation's network to block threats to its electronic information (Adjei, 2015).

Communication from the cloud service provider, on any changes in the legislation, breach of data and security vulnerabilities, should be addressed in the SLA prior to accepting these services. Organisations should insist on monitoring the services they receive from the cloud service provider and verify whether these services are as per their agreement in the SLA. Monitoring should include the implementation of the cloud service and deployment model, any upgrades or any network changes or when vulnerabilities have been detected. The board must ensure they have access to vulnerability assessment reports that are run by the cloud service provider to ensure their information is protected (Chandran & Angepat, 2012).

3.5 CRITICAL LINK TO EMPIRICAL STUDY

Careful analysis of the various risks that affect the adoption of the cloud to an organisation's environment is vital to assessing whether the IT Governance Frameworks can address those risks. The important step of mapping the cloud computing risks to the IT Governance Frameworks will be addressed in the empirical study. Controls from the Frameworks will be addressed for the individual risks or grouped in cases where the risks and controls complement each other. The following are risks as a result of cloud computing and can be summarised as follows:

- Security risk;
- Privacy risk;
- Data integrity risk;
- Availability;
- Network capacity risk;
- Data segregation;
- Multitenancy risk;
- Access controls;
- Governance risk;
- Data location risk; and
- Consumer risk.

In Chapter 4 and 5 of the study, the researcher will group some of the risks listed above since they fall under one category when implementing mitigating controls. Below is a table of how the cloud computing risks will be addressed.

Cloud computing Risks
Security Risk
Privacy Risk
Data Integrity Risk

Availability and Network Capacity Risk
Data Segregation and Multitenancy Risk
Access Control Risk
Governance and Data Location Risk
Consumer Risk

It is also important that the client organisation understand which party is responsible for mitigating the risks listed above and to adequately prepare controls to address these risks. The table below gives a summary of the cloud service models and the parties responsible for implementing controls to mitigate these risks.

Cloud Service Model	**Responsible for mitigating risks**
IaaS	Client organisation
PaaS	Client organisation and cloud service provider
SaaS	Cloud service provider and software service provider.

3.6 CONCLUSION

The purpose of this Chapter was to address the risks of cloud computing, its deployment and its service models. The aim was to provide insights on the cloud computing risks that organisations need to be aware of prior to adopting the service. The choice of the deployment and service model are highly dependent on the size, objectives and risk appetite of the organisation. Regardless of their choice, it is important that thorough consideration of the risks above is understood, and the organisation does its research on the options of cloud service providers available. In the following Chapter, the researcher will address the cloud computing risks discussed above and how best to apply the IT Governance Frameworks to mitigate these risks.

CHAPTER 4: INFORMATION TECHNOLOGY GOVERNANCE FRAMEWORKS

4.1 INTRODUCTION

In this Chapter, a literature review on organisations' use of IT Governance Frameworks to address cloud computing risks is conducted. The review begins by introducing the reader to the objective behind selecting IT Governance Frameworks to address cloud computing risks and explains the qualities of each framework. The controls suggested by ISO/IEC 27002, COBIT, NIST and the POPI Act Frameworks, for mitigating security, privacy, availability, network capacity, access control, integrity, data segregation, multitenancy, data location, governance and consumer risk are then discussed.

4.2 BACKGROUND OF THE IT GOVERNANCE FRAMEWORKS

The adoption and implementation of cloud computing has undeniably evolved over the last few years (Aljumah & Ahanger, 2020). Its value-added benefits include scalability, resilience, flexibility and efficiency when processing data (Yimam & Fernandez, 2016). For an organisation to enjoy these benefits, the risks associated with cloud computing need to be averted when adopting the cloud. Since the emergence of cloud computing technology, little development has been made on Frameworks that focus on cloud computing (Al-Ruithe, Benkhelifa & Hameed, 2016).

IoDSA (2016) observes that technology governance and security have become a matter of significant importance. This means that the successful adoption and implementation of the cloud is reliant on some form of governance to mitigate the risks an organisation is exposed to. As previously mentioned in the study, "governance of the cloud is a set of guidelines or controls used to manage critical data stored on the cloud" (Gunadham & Kuacharoen, 2016). Organisations subcontracting elements of their IT to third parties face a high level of risk, which needs to be managed. The success of adequate security controls and ideal risk treatment generally depend on global standards or principles. Reliance on IT Governance Frameworks in this regard is paramount to a clear strategy in mitigating cloud computing risks (Rebollo, Mellado, Fernandez-Medina & Mouratidis, 2014).

Over the last decade, a couple of IT Governance Frameworks have been developed, with the intention to give great practice to IT pioneers to create, implement, monitor, and consistently improve IT Governance and controls (Mohlameane & Ruxwana, 2016). Reference to these Frameworks can assist organisations to solve the governance issues related to cloud computing (Bounagui, Mezrioui & Hafiddi, 2019). The commonly used IT Governance Frameworks include COBIT, ISO/IEC 27001/2, and NIST (Silva, Silveira, Dornales & Ferreira, 2019). In this study, these frameworks are used to assess how organisations can manage and improve the implementation of cloud computing applications. The POPI Act of South Africa, that came into effect on the 1st of July 2020 (Michalsons, 2020), will also be used as a reference in terms of the controls that should be implemented to protect personal information on the cloud (Al-hashimi, Othman, Sulaiman & Zaidan, 2018).

Although these Frameworks were not designed solely for cloud computing, they can be used to respond to cloud computing risks (Bounaguia et al., 2019). Organisations can therefore use a blend of the above-mentioned frameworks or select one. Below, the qualities of each of the IT Governance Frameworks, that is, ISO/IEC 27002, COBIT, NIST and the POPI Act, are described in relation to how they can aid in minimising cloud computing risks.

4.3 IT GOVERNANCE FRAMEWORKS

IT Governance is a process used to monitor and control key information efficiency decisions so that sound delivery is made to value stakeholders in the business environment (Motii & Semma, 2017). IT Governance has an impact on all the IT decisions made within an organisation and boils down to how an organisation chooses to run its operation under set policies and standards (Alloussi, Fetjah & Chaichaa, 2016). IT Governance should therefore see to the procurement and implementation of IT resources, including systems, networks and processes, in accordance with the organisation's policies and procedures. It is imperative for the systems to be well maintained and controlled so that they can add value to the organisation in a way that supports its objectives (Enslin, 2012).

To address the cloud computing risks, the ISO/IEC 27002 Framework, which is designed to address information security controls of third-party related services and can be applied to any IT industry, was selected. This Framework is used to address these significant cloud computing risks (Tariq & Santarcangelo, 2016).

The COBIT Framework addresses the expectations and conditions of services that need to be delivered by the organisation's stakeholders in line with its objectives. COBIT addresses governance topics and elements that address areas such as cybersecurity, cloud computing, Small Medium-Sized Enterpises (hereafter, SME), privacy and digital transformations (Mutune, 2020). The COBIT 2019 Framework (2018) thus provides the governing body of the organisation with direction through prioritisation, decision-making and the monitoring of service delivery tasks agreed upon by the organisation and service provider. It is then management's responsibility to plan, build, run and monitor these activities and ensure the cloud service provider does not deviate from the guidance and objectives set by the governing body in their attempt to insulate the organisation from cloud computing risks (Faizi & Rahman, 2019).

The NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) offers a well organised and adaptable procedure for overseeing data security and privacy risk. It incorporates exercises that equip organisations to execute the cloud computing system at appropriate risk management levels and allows for continuous monitoring. The POPI Act of South Africa (2013), on the other hand, is designed to provide organisations with a clear understanding of their responsibility in lawfully processing the personal information of data subjects (both natural and juristic persons). This aids in reducing the risk of theft, discrimination and fraudulent use of personal information (Skolmen & Gerber, 2015).

Governance of the cloud regulates cloud service providers and services rendered, facilitates and allows transparent communication between the cloud service provider and the client organisation, while providing return on investment and mitigating cloud computing risks. Without cloud governance, the risks of using any of the cloud models would be high. This would minimise the opportunities and benefits it has to offer (ISACA, 2014).

IoDSA (2016) encourages the board to govern all technology and information in a manner that achieves the organisation's objectives and improves operational efficiency. This will guarantee integrity, responsibility, accountability, trust and transparency of services to be delivered (Jakimoski, 2016). Mitigating cloud computing risks on the cloud is a continuous process carried out across all cloud delivery models. This includes cases where the cloud service provider outsources their services to a third party, which further complicates security controls in place, business continuity and legal requirements (Tariq & Santarcangelo, 2016).

This Chapter will explore literature on the IT Governance Frameworks mentioned above and how these Frameworks address cloud computing risks. The aim is to ensure that the implementation of cloud computing services in an organisation are governed according to industry best practices. Mitigating controls of each IT Governance Framework, aiming to address the cloud computing risks, are therefore discussed below.

4.4 MITIGATING CONTROLS RECOMMENDED BY ISO/IEC 27002

4.4.1 SECURITY MITIGATING CONTROLS

Security risk, associated with the cloud, and areas that require special attention in averting this risk, were discussed in Chapter 3. These areas covered network and connectivity security, endpoint security (for laptops, tablets, mobile phones and other wireless devices) and access control (i.e. user identity, logical access, physical access to IT assets and sensitive documents) (Enslin, 2012).

During migration to the cloud, there is the risk of breach and interception of client data, since this process utilises public networks, such as the internet. Security on the cloud is therefore a vital component during and after the implementation stages (Schluga, Bauer, Bicaku & Maksuti, 2018). It is therefore imperative that organisations are aware of the best practice controls for securing information on the cloud.

In the process of mitigating security risk, the client organisation must define a security policy that covers its expectations around security controls for the organisation and any third-party service providers it chooses to engage with (Alloussi et al., 2016). The security policy should address controls around data segregation, physical and environmental security, data transfer, security against malware, management of vulnerabilities and encryption. Candiwan and Priyadi (2016) also advises the client organisation to gain an understanding of the security controls defined by the cloud service provider, to evaluate the adequacy and effectiveness of these controls in meeting the client's organisational objectives around combating cloud computing risks within their environment. The implementation of security controls to the cloud environment by either the cloud service provider, client organisation or both, should be continuously monitored and updated when necessary or as risks evolve (Odun-Ayo, Mistra, Abayomi-Alli & Ajayi, 2017).

Security controls can include the use of firewalls and intrusion detection/prevention systems, technological controls such as authentication, encryption tools and network connection controls (Ali, Shrestha, Chatfield & Murray, 2020). Schluga et al. (2018) propose the installation of firewall software against cyber-attacks or vulnerabilities on the cloud. Firewalls are web security systems that observe and regulate inbound and outbound web traffic constructed on programmed security guidelines. A firewall naturally creates a barricade between a reliable network and an untrusted network, such as the internet. This places security controls on both the entry and exit points of the network (Kalaiprasath, Elankavi & Udayakumar, 2017).

Firewalls facilitate functions such as virtual machine isolations. Virtualisation permits the sharing of equivalent physical assets among a few clients. On the account of cloud computing where assets, for example, computing, storage and networking, might be remotely leased in a virtualised structure under precise SLAs, it would be exceptionally attractive that the exhibition of the virtualised assets be as steady and predictable as could reasonably be expected. This minimises interferences among virtual assets (Mukherjee, 2019).

Another layer of security would be to add intrusion detection/prevention systems on virtual machines (Tariq & Santarcangelo, 2016). This will keep the cloud service provider ahead of possible cyber-attacks and up to date with security updates needed for the cloud service software. Outdated software operations pose weaknesses on the network and minimise the strength and effectiveness of encryption controls on the cloud. Gunadham and Kuacharoen (2016) recommend adopting intrusion detection tools which aid privacy, integrity and protection of data transmitted on the cloud.

Examples of these intrusion detection/prevention tools include the following:

a) **Server-side Encryption-** This tool can be purchased from a third-party cloud software service provider. The tool is used to encrypt data at its endpoint by the application or service that receives it (Ramachandra, Iftikar & Khan, 2017);
b) **New Technology File System (hereafter, NTFS)-** It is a built-in encryption tool. NTFS is a file system used for storing and recovering data on a hard drive (Ramachandra, et.al, 2017);
c) **Hypertext Transfer Protocol Secure (HTTPS)-** It warrants that the user is authorised and authenticated to access and read the data on the cloud (Huang, Zhang & Xin, 2018);
d) **Secure Socket Layer (SSL)-** It is an encryption link between a web server and browser (Borgolte, Fiebig, Hao, Kruegel & Vigna 2018); and
e) **Transport Layer Security (TLS)**- It is a “protocol that provides communication security between the client and server applications that communicate with each other over the internet” (Gunadham & Kuacharoen, 2016).

The use of encryption methods and antivirus software can be utilised as controls against security risk on the cloud. An antivirus software will protect the cloud network from malware through detection or preventing the malware from penetrating the network. It also restricts the use of unapproved software, which may increase the risk of the client's data being exposed to vulnerabilities (Odun-Ayo et al., 2017). ISO/IEC 27002 (2013) also encourages the continuous monitoring of the network by obtaining tools that perform network vulnerability scans. Vulnerability scans can detect malware on the network and identify outdated software that may need to be replaced or patched up to maintain effective security controls. This additionally guarantees that all data scanned, prior to being saved on the cloud, is secure and will not pose a threat to the overall security of data stored on the cloud (Omar, 2017). Lastly, it is the responsibility of both the client organisation and cloud service provider to provide security awareness, education and training to its employees on risks regarding security on the cloud (Brandis, Dzombeta, Colomo-Palacios & Stantchev, 2019).

4.4.2 PRIVACY CONTROLS

Privacy controls refer to the regulatory, specialised and physical safeguards utilised by organisations to secure and guarantee the best possible treatment of personally identifiable information and prevent events that pose a risk to privacy (Grama, 2016). To successfully protect the privacy of personal data on the cloud, the client organisation needs to avoid non-compliance to privacy laws, standards or guidelines (Arafat, 2018).

Formal policies and procedures, addressing controls to be implemented to safeguard the transfer of data through all types of communication services and its storage on the cloud, must be defined, The controls to safeguard the privacy of data should block interference, replication, alteration, misrouting and deletion (Madi, 2018). Privacy or non-disclosure agreements defining the client organisation's needs, in terms of protection of personally identifiable information, must be documented and communicated to the cloud service provider. This agreement must address all privacy concerns for the stipulated duration of the contract between both parties and

procedures to be followed if the contract is dissolved (Kurniawan & Riadi, 2018). This should detail the rights of ownership over the data on the cloud, how the data is destroyed, and the steps taken in the event of a breach in contract and where data privacy is affected.

It is the client organisation's responsibility to fully understand the policies and laws the cloud service provider adheres to, and the controls they have in place. Where there is a difference in location between the two parties, the client organisation should obtain a clear understanding of the laws and legislations governing that country in terms of privacy and protection of personally identifiable information and its effects on their organisation as a whole (Mohlameane & Roxwana, 2016). This will give better insight on how the cloud service provider stores and disposes data and whether it provides enough security controls in terms of data privacy.

Storage and disposal of data should be in line with the client organisation's policies, procedures and code of ethics. Therefore, this should guide the client organisation in the selection process of a cloud service provider, which should be in line with their business objectives and stakeholder interests. This too will largely influence the logical and physical safeguards put in place by the cloud service provider to ensure that privacy for the client's data is prioritised correctly (Simpson, 2016).

To avoid the breach of data privacy, the transfer or deletion of sensitive data on the cloud must be authorised by the client organisation (Mohlameane & Ruxwana, 2016). Records of any transfers, deletions and alterations must be kept for audit trail purposes and sent to the client organisation by the cloud service provider. All data must be encrypted before it is deleted or destroyed to ensure that it cannot be recovered by unauthorised persons (Choudhury, Gupta, Pradhan, Kumar & Rathore, 2017).

4.4.3 DATA INTEGRITY CONTROLS

Velumadhara and Selvamani (2015) define data integrity as the means of ensuring data is not altered. Data integrity controls are necessary to protect data from unauthorised deletion, modification, fabrication or manipulation. This step is crucial due to the interoperability across devices and systems when using cloud services. To prevent the loss of data integrity, data must be attributable to the person(s) and or system that generated it, to guarantee accountability of actions performed on the cloud (Grama, 2016). All electronic data should be permanently recorded and stored at the time it is generated, with clear time/date stamps, so that the sequence of events can be easily followed (Motii & Semma, 2017). These logs must be available for review and retrieval upon the request of the client organisation. ISO/IEC 27002 (2013) recommends the proper maintenance of original data and replicas. Replicas, including backup/archive copies, must be verified as accurate and true to protect the content and connotations of the original source (Ramachandra, Iftikar & Khan, 2017).

To enhance data integrity controls, Vumo, Spillner and Kopsell (2019) recommend the use of cryptographic methods. Cryptographic controls facilitate data integrity and restrictions against the installation of unauthorised software, as these can bring unknown vulnerabilities that could alter the integrity of data. Any security updates installed to the cloud systems must be tested to safeguard the integrity of data.

4.4.4 AVAILABILITY AND NETWORK CAPACITY CONTROLS

In today's computing age, each day can bring a host of challenges to do with the location of data, who has access to it, its availability and how the high volumes of data generated on an hourly or daily basis are managed (Mohammad, Amir & Mehdi, 2018). With availability and network capacity, the client organisation needs to select a cloud service provider with reliable and sound cloud infrastructure. Simple inconsistencies of limited internet bandwidth, service unavailability and lack of support do not convince investors to procure services from some cloud service providers. Therefore, assessing

network connectivity and network capacity are vital to the maximisation of benefits by the client organisation (Candiwan & Priyadi, 2016).

ISO/IEC 27002 recommends that network capacity requirements for the client organisation be determined prior to accepting services from a cloud service provider (Adendorff & Smuts, 2019). Both parties need to determine the criticality of the client organisation's data system. Included in the terms and conditions of the SLA between the two parties should be the continuous monitoring of the system to improve efficiency and availability. The cloud service provider should manage network capacity by eliminating outdated data to free up disk space; clearing applications, systems and databases, that are not in use, in the cloud environment and restricting bandwidth for applications that are not critical to the environment (Motii & Semma, 2017).

4.4.5 DATA SEGREGATION AND MULTITENANCY CONTROLS

Data segregation is the classification or grouping of data on a server (Bansidhar, Bineet & Kritika, 2017) while multitenancy is the cloud service providers ability to host multiple tenants on its servers (Madi, 2018). The responsibility of data segregation of the multiple tenants on the cloud, lies with the cloud service provider. Data segregation allows the cloud service provider to run data in a controlled and secure manner, whilst actively complying with client requirements (Nasseri & Duncan, 2016). This helps limit the risk of data leakage, sharing, breach or the spread of any malware amongst the multiple clients on its cloud servers. Cloud service providers should aim to ensure that their client's data is not misplaced, and privacy is not infringed in any way (Jackson, 2017).

According to Retselisitsoe (2016), cloud service providers can achieve this by segregating their tenants' data in terms of sensitivity and criticality to guarantee security in terms of data privacy, integrity and accessibility on its cloud servers. Data segregation should be based on the client organisation's requirements for data limitations and sharing, and the legal requirements that should be met (Nasseri &

Duncan, 2016). To safeguard against loss of data or a data breach, the cloud service provider must encrypt all client data on their cloud servers. This must be included in the client organisation's policy and SLA with the cloud service provider to warrant compliance with ISO/IEC 27002 and industry best practices (Madi, 2018). Encrypting data should be used concurrently with user authentication and access controls for all users with access to the cloud server. This guarantees that the multiple client organisations sharing the same pool of cloud resources have data security enforced, giving assurance that privacy, reliability and validation controls are enforced on their data (Odun-Ayo et al., 2017).

4.4.6. ACCESS CONTROLS

When addressing access controls, ISO/IEC 27002 (2013) recommends that the cloud service provider and client organisation must have strict controls on users who have access rights on the cloud servers, networks and system administration. These rights must be defined and allocated based on the user's role and responsibilities. To achieve this there must be monitoring of access through record keeping (Candiwan & Priyadi, 2016). Security parameters to the cloud servers must be defined and protected to ensure security of sensitive and critical data stored.

The cloud service provider has the responsibility to ensure that the facilities where the data is stored are manned and properly secured, such that no unauthorised persons can enter the facilities, and there is no environmental contamination of assets that can occur. A formal process of registering users on the network must be implemented for transparency and audit trail purposes (Yimam & Fernandez, 2016).

4.4.7 GOVERNANCE AND DATA LOCATION CONTROLS

When addressing the governance and data location risks, both the client organisation and cloud service provider must ensure that they comply with applicable laws and regulations around the cloud and industry best practice on information and technology.

The two parties may not share the same geographical location or be in one country; therefore, the client organisation should consider the statutory differences and legal compliance pressures they may face from this (Brandis et al., 2019).

ISO/IEC 27002 (2013) requires the client organisation to evaluate the legal implications of the laws and legislations where the cloud service provider is located and carefully consider the ethical processing of data in that location. This decision will have an impact on the client organisation's stakeholders and its business objectives (Mukherjee, 2019).

4.4.8 CONSUMER RISK CONTROLS

In Chapter 3 we noted that consumer risk involves client organisations getting into contracts where the terms and conditions may not necessarily allow them to easily change from one cloud service provider to another. This is a common problem which results from the client's lack of involvement during the process of drafting the contract with the cloud service provider (Mohlameane & Roxwana, 2016).

To avoid this, ISO/IEC 27002 (2013) recommends that the client organisation include conditions of service, access rights to the client's data and rights to have the cloud service providers processes and procedures audited. The myriad of controls that are agreed upon by both parties in the SLA should be used as a benchmark for either continuing with the enlisted cloud service provider or terminating the contract all together. This keeps both parties honest and ensures service obligations are met and, therefore, allows the client organisation to speedily change cloud service providers (Motii & Semma, 2017). Refer to Chapter 5 on the Empirical Study and Research findings on cloud computing risks and the controls defined in ISO/IEC 27002 Framework.

Summative comment

The following cloud computing controls were identified to address the cloud computing risks:

- Define policies that address security, privacy and access controls.
- Implement security tools such as firewalls, intrusion detection/prevention systems, encryption and vulnerability scans.
- Ensure that there is compliance of laws and regulations and industry best practice on security, privacy of data and the client organisation and cloud service provider's location.
- Define roles and responsibilities of those who grant and revoke logical and physical access to the cloud environment.
- Consider continuous monitoring and review of network security controls on the cloud.
- Ensure there is user awareness training on security and privacy of data for both the client organisation and cloud service provider.

Below the researcher will discuss the mitigating controls recommended by COBIT 2019 Framework, to address cloud computing risks.

4.5 MITIGATING CONTROLS RECOMMENDED BY COBIT

4.5.1 SECURITY CONTROLS

Security risk of the cloud is a shared responsibility of the client organisation and cloud service provider. The two are required to secure controls around infrastructure, applications and data storage (Maduka, Aghili & Butakov, 2017). The cloud service provider should have controls in place to authenticate users on the cloud, prevent data leaks, secure applications, operating systems and databases, as well as have physical safeguards for the physical environment of the cloud servers (Samer, 2019). The client organisation has the responsibility of training its employees on how to securely use

the cloud application and any IT related devices to minimise human error that could potentially minimise the effect of security controls put in place (Khan & Gouvia, 2017).

To mitigate security risk on the cloud, Setiyawan (2019) states that an organisation should have a data security management system that provides a standard, formal and continuous approach to data security, thus enabling a secure environment, for the cloud, that is aligned to the organisations objectives. Roles and responsibilities should be established and communicated to both the client organisation and cloud service provider. Awareness training programs must be established to educate all employees and responsible parties on how to ensure security on the cloud is not compromised (Soubra & Tanriover, 2017).

The COBIT 2019 Framework (2018) is also known to adopt preventive, detective and corrective measures to manage security on the cloud. Maduka et al. (2017) propose the installation of malicious software defence tools. This will ensure only authorised software devices are connected to the network and will minimise risks that may come with rogue and unprotected devices. A malicious software defence tool also facilitates monitoring of all activities on the network and becomes the first line of defence in detecting and preventing any cyber-attacks, malware or viruses. All registered devices should have password authentication enabled before connecting to the network to limit unauthorised personnel from accessing the client organisation's data.

Soubra and Tanriover (2017) add that network filtering tools, such as firewalls and intrusion detection software, mitigate the security risk of unwanted access to the cloud. This ensures that endpoints such as the servers, workstations, mobile devices and network programming are protected (Ramachandra et.al., 2017). This control can be enhanced by ensuring the latest security updates, patches and antivirus controls are in place across the cloud environment to protect information systems and technology from malware (i.e. viruses, worms, spyware and spam) (Mukherjee, 2019). COBIT 2019 Framework (2018) also encourages frequent reviews of security controls on the

cloud by utilising a selection of supported technologies and services such as vulnerability assessment scanners, to identify security vulnerabilities on the cloud.

4.5.2 PRIVACY CONTROLS

Privacy controls on the cloud are essential to the protection of the organisation's data. When selecting a cloud service provider, it is important for the client organisation to clearly define its expected service obligations related to privacy of information on the cloud (Suess, 2019). These service obligations should detail collection, use, disclosure, management of personal data, data confidentiality and the sale or sharing of the client organisation's data to other organisations. The SLA should emphasise compliance to industry regulations on protection of data (Ukidve, Mantha & Tadvalkar, 2019).

According to the COBIT 2019 Framework (2018), the client organisation must also consider appointing a Privacy Officer. A Privacy Officer is an executive responsible for managing risks related to data privacy legislation and regulations. He/she will manage the implementation of controls relating to data privacy. It is however a joint responsibility for both the client organisation and cloud service provider to create a culture of data security and privacy awareness throughout their organisations. This can be achieved by providing training and constant awareness on privacy risk, as well as the employee's individual commitment to applying these controls to mitigate the risk (Suess, 2019).

4.5.3 DATA INTEGRITY CONTROLS

Data integrity controls are set to ensure that only authorised individuals have access and the ability to create, change and delete data (Gerber, 2015). By assigning these controls to authorised personnel only, the confidentiality of data is inherently protected. This ultimately ensures that data remains complete, accurate and valid, thus protecting the very principles of data integrity (Khan & Gouvia, 2017).

To mitigate data integrity risk, the client organisation must establish an integrated strategy for the organisation to uphold a certain level of data quality (such as complexity, integrity, accuracy, completeness, validity, traceability and timeliness) that is aligned to its organisational objectives (Vumo, Spillner & Kopsell, 2019). There should be a tracking process for any inaccurate data transactions made on the system to ensure they do not interfere with the dispensation of valid transactions. The integrity of the data can be assessed by verifying any information within or outside the organisation, for the validity of its source and the integrity of its content. COBIT once again emphasises that employees, from the client organisation and cloud service provider, be trained on the importance of data integrity controls (Omar, 2017).

4.5.4 AVAILABILITY AND NETWORK CAPACITY CONTROLS

Availability of cloud computing services refers to the ability to access data stored on the cloud at any given time. Network capacity is the cloud's ability to handle volumes of data at any given time. The two components should function at optimum levels for the client organisation to continue with its day to day business activities. This is guaranteed by having systems and infrastructure such as network load balancers, in place, that meet network performance and capacity requirements to process requests promptly and guarantee the availability of cloud services (Ukidve et al., 2019).

To implement this control, the client organisation must assess its budget towards procuring the right amount of capacity (future and present) on the cloud to make sure that its needs, in terms of availability and performance, are prioritised. Choosing the right cloud service provider warrants the consistency of these requirements for the duration of the contract. The client organisation should also have the flexibility to change values in capacity based on any changes in network capacity requirements and business objectives (Vani & Priya, 2015).

The availability of cloud services by the cloud service provider is also vital and may be attained avoiding periods of downtime due to servers crashing (Vani & Priya, 2015). To mitigate the risk of availability and network capacity constraints, there should be controls in place addressing business continuity and disaster recovery. These must be developed and followed by both parties to ensure that critical systems remain available and operational in the event of a disaster (COBIT 2019 Framework, 2018). The Business Continuity Plan (hereafter, BCP) and Disaster Recovery Plan (hereafter, DRP) must be frequently tested and updated where necessary by both the client organisation and cloud service provider (ISACA, 2014). This will help assess the strength of controls in maintaining availability, network performance and the network capacity on the cloud.

4.5.5 DATA SEGREGATION AND MULTITENANCY CONTROLS

Kusumawardhani and Masyithah (2017) observe that when data segregation is appropriately applied, sensitive or classified data assets are supervised with more prominent oversight than data assets that are viewed as public or allowed to be distributed freely. Where a cloud service provider has multiple tenants on the cloud, data must be managed adequately.

The cloud service provider should define the controls in place to safeguard and maintain confidentiality of its client's data kept on the cloud by correctly and securely segregating it from its multiple tenants. This can be achieved by categorising data as restricted, sensitive and unrestricted, thus further enhancing the sound management of data assets on the cloud service provider's servers (Al-Ruithe et al., 2016).

The cloud service provider must allocate roles and responsibilities to the management of critical data, data sharing, compliance of laws in terms of data privacy and the risk reduction for all its clients on the cloud. This can be achieved by restricting access of users according to defined roles and responsibilities (Simorjay, 2014). This will require implementing user authentication and authorisations controls. User authentication is the process of verifying who the user is, and authorisation is the process of allowing

the authenticated user access to the data that is either restricted, sensitive and unrestricted based on defined roles and responsibilities (Simorjay, 2014).

The client organisation must monitor the flow of its data and keep track of the data inventory in the duration of its contract with the cloud service provider. It is therefore important for the selection process of the cloud service provider to be performed diligently to assure data security on the cloud (Rashid & Chaturvedi, 2019).

4.5.6 ACCESS CONTROLS

Access controls must address both logical and physical controls. The cloud service provider must have measures in place for the safety of the cloud assets and data against natural elements and cyber-attacks (Onankunju, 2013). The environment must be set up with equipment and devices to monitor and control the cloud infrastructure and assets. This includes security in terms of the power supply and intrusion or the detection equipment, such as alarms and cameras, to monitor the environment. These must be implemented based on the organisation's policies and specifications on environmental safety standards and procedures (ISACA, 2014). The cloud service provider must manage physical access to cloud servers and other IT related assets by implementing appropriate restrictions to these facilities. Access to these facilities must be warranted, approved, recorded and observed to mitigate breach and the potential loss of sensitive and critical data or contamination of the environment. This process must be followed by all employees, cloud service providers, sub-contractors, guests or any third parties upon arrival to the cloud server facilities (COBIT 2019 Framework, 2018).

There should be controls in place to manage user identity and logical access by ensuring that all users have data access rights in accordance with the organisation's requirements. These rights must co-ordinate with the business units that manage their own access rights within the business processes. All users must have data access rights necessary for their specific roles within the organisation (Simorjay, 2014).

To guarantee logical security of access on the cloud, the cloud service provider could consider the use of Fine-grained Access Control (hereafter, FAC) which is an encryption tool that blocks cyber criminals from stealing/accessing data easily in a readable format. This tool can be complemented with Secure Data Sharing (hereafter, SDS) which promotes data accessibility at any given time in a protected form, whilst concurrently increasing the integrity of data on the cloud (Gunadham & Kuacharoen, 2016). Logical access controls tools are utilised for approval, authorisation and responsibility in the cloud environment. These elements enforce access controls for the various cloud models and data within (Collins, 2014).

4.5.7 GOVERNANCE AND DATA LOCATION CONTROLS

The client organisation ultimately has the responsibility to consistently comply with applicable laws around cloud applications and information and technology (Ahmad, Mukhneri, Mochamad & Karlena, 2017). The Privacy Officer should constantly stay up to date with any changes in local and global laws related to information and technology. He/she should be able to distinguish and evaluate all potential compliance requirements and their effect on cloud computing activities, such as data movement, data privacy and industry specific regulations (Andry & Hartono, 2017). An assessment should also be made of the effects any changes to laws and regulations will have on the cloud service provider's operations within the client organisation's environment.

4.5.8 CONSUMER RISK CONTROLS

In addressing consumer risk, finding the most reputable cloud service providers on the market, known for their excellence in cloud service delivery, is imperative (COBIT 2019 Framework, 2018). Once the client organisation has made their selection for a cloud service provider, both parties must engage and agree on the cloud deployment model as well as the cloud service model to be adopted. The cloud models selected must align with the client organisation's operational objectives and the SLA must address product and service expectations, while monitoring these services (Hussain et al., 2016). This will give the client organisation clarity on the cloud service provider's

delivery of the agreed upon services defined in the SLA, while reducing risks of non-compliance to the organisation's IT Governance policies and industry laws (Al-hashimi et.al, 2018).

It is the client organisation's responsibility to manage all contracts and validate their compliance to the organisation's policies, legal and regulatory requirements. This should include making certain that security, availability and privacy risks on the cloud are effectively and efficiently mitigated. This gives the client organisation reassurance, confidence and trust that its data is protected (Adendorff & Smuts, 2019). It is imperative that the client organisation has a clear understanding of the cloud service provider's terms and conditions within the SLA. This will allow the client organisation clarity on matters concerning obligations to third party audit reports and the right to change cloud service providers when necessary (Tiwari & Mehta, 2019).

Refer to Chapter 5 on the Empirical Study and Research findings on cloud computing risks and the controls defined in COBIT 2019 Framework.

Summative comment

The following cloud computing controls were identified by literature to address the cloud computing risks:

- Define a standard Data security management system that defines controls to secure the cloud.
- Conduct awareness training programs on security, privacy and data integrity on the cloud.
- Define roles and responsibilities for the client organisation and the cloud service provider in managing security, privacy, availability, integrity, network capacity, access control, data segregation, multitenancy, data location, governance and consumer controls for the cloud.
- Implement network filtering tools such as firewalls, intrusion detection software, vulnerability scanners and encryption tools.
- Appoint a Privacy officer.

- Comply with the client organisation's standard principles and best practice guidelines and laws.
- Develop a Business Continuity Plans and Disaster Recovery Plan.
- Monitor and restrict access to data on the cloud and the cloud facilities.

In the section below, the mitigating controls recommended by the NIST, to address cloud computing risks, are discussed.

4.6 MITIGATING CONTROLS SUGGESTED BY NIST

4.6.1 SECURITY AND PRIVACY CONTROLS

Adopting the cloud requires close cooperation between data security and data privacy controls. The NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) addresses the two components together. While data security and privacy controls have various targets, their objectives in mitigating risks often overlap and are mostly a shared responsibility between the client organisation and cloud service provider. The common goal for data security and privacy controls is safeguarding data and data systems from unapproved access, use, interruption and alteration. Therefore, there should be a commitment to ensure that the security and privacy posture of cloud systems and its users is managed on a regular basis by evaluating and constantly monitoring the controls on the cloud (Anand, Ryoo, Kim & Kim, 2016).

The cloud service provider must make use of tools that ensure reliability of software, firmware and data integrity on the cloud (Kalaiprasath et al., 2017). This can be achieved by running vulnerability scanning tools to monitor and detect any weaknesses on the cloud environment in a timely manner. The aim is to get an understanding of the vulnerability and its target areas on the cloud (Mukherjee, 2019). The scanned results must be investigated, and all vulnerabilities identified should be

fixed. Consideration should be made to have proactive system tools that detect, identify and prevent network based malicious codes and websites that may infiltrate the cloud environment.

Tariq, Tayyaba, Ashraf, Rasheed and Khan (2016) further recommend having a well-managed vulnerability management plan in place. The vulnerability management plan should address the controls required to prevent the installation of software that is not known or authorised by the organisation. To have control over software installed, the client organisation should classify acceptable and forbidden activities concerning software installation. Acceptable software installations include updates and security patches to present software and the downloading of new applications from app stores authorised by the client organisation.

The vulnerability management plan should define and detail the implementation of configuration settings for the cloud software deployed on the system and network with the most restrictive controls, in line with the client organisation's security controls. Configuration settings are restrictions applied to a system or application to maintain and enforce security controls on the cloud. Audit log settings should be enabled on the cloud to track any changes made. Strong configuration settings prevent cyber criminals from penetrating the client organisation's environment and stealing data (Griffin, 2016).

To further cement security and privacy controls on the cloud, both the client organisation and cloud service provider should offer security and privacy awareness training based on roles and responsibilities assigned to cloud system users (Kumar, Tyagi & Nayeem, 2018). Users that would require role based training include cloud service providers, authorising officials; system security officers; privacy officers; systems engineers; system and software developers; system, network, and database administrators; personnel conducting configuration management activities; personnel performing verification and validation activities; auditors; personnel having access to system-level software; control assessors; personnel with contingency planning and

incident response duties; personnel with privacy management responsibilities; and personnel having access to personally identifiable information.

Privacy controls are useful for compliance with material privacy prerequisites and handling the risk to data or people related with the creation, collection, use, preparation, distribution or removal of personal information. At the point when a data system processes personal information, the organisation's data security controls and privacy controls have a mutual duty in handling the risk that may emerge from unapproved access or activity on the cloud (Ramachandra et al., 2017).

4.6.3 AVAILABILITY AND NETWORK CAPACITY CONTROLS

To address the risk of availability, Kumar, Raj and Jelcianac (2017) recommend that a contingency plan be defined and documented. Availability of data on the cloud is the responsibility of the cloud service provider. The contingency plan should address recovery controls, restoration priorities, roles and responsibilities in the event of a natural disaster or cyber-attack. Plans that are closely related to contingency plans include BCP, DRP, Crisis management plans and Cyber Incident Response plans. These plans will generally identify and define critical systems and data that require additional security controls to ensure they are readily available in the event of a threat or disaster (Ibrahim, Valli, McAteer & Chaudhry, 2018).

Wang (2016) recommends that a capacity plan be developed and defined to ensure that the required capacity for data processing, communications and cloud support are available during contingency operations. This is essential as vulnerabilities found on the network have different effects on the availability of communications, data processing and support services to ensure the organisation continues with its day to day activities. Adequate capacity is vital in maintaining availability on the cloud.

4.6.4 DATA INTEGRITY CONTROLS

Integrity of data is linked with how well privacy controls are held on the cloud. Controls put in place to mitigate security and privacy risks, in turn, address data integrity and availability risk. Information and records (data) should be managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information. This will cut across all networks within the organisation that transmit data, such as servers, laptops or computers, mobile devices and printers (Kumar et al., 2017).

Rizwana and Sasikumar (2015) recommend that all communication paths be securely protected to prevent interceptions that could lead to any adjustments of that data and disrupt data integrity. There should be strong access controls to the cloud environment, both logical and physical, to aid the protection of data integrity. The client organisation must assess the cloud service provider's controls with regards to confidentiality of data, to ensure integrity is not compromised. Encryption tools can be considered, to protect data on the cloud environment, as compensating controls to mitigate data integrity risk. Encryption protects the client organisation's data from manipulation by unauthorised persons, whether internal or external. Tariq et al., (2016) also recommends deploying integrity verification tools that can detected any unapproved modifications to software, firmware and data on the cloud.

4.6.5 DATA SEGREGATION AND MULTITENANCY CONTROLS

To mitigate the risks associated with data segregation and multitenancy controls, the cloud environment must be segregated according to the different clients hosted (Rashid & Chaturvedi, 2019). Segregating data of the different clients on the environment facilitates security and confidentiality on the cloud. This also allows the cloud service provider to cater to the different security and privacy requirements of its multiple clients and ascertain the criticality of the data stored. This facilitates the protection of the cloud service provider's network integrity, further incorporating

network segregation amongst the multiple tenants where appropriate (Ramachandra et al., 2017).

To prevent any risks related to multitenancy, Anand et al. (2016) recommends that the cloud service provider separate the network addresses for the multiple clients that connect to the cloud server. The separation of networks into subnetworks affords a suitable level of security for the multiple tenants and minimises breach and loss of data integrity, confidentiality and availability.

4.6.6 ACCESS CONTROLS

To mitigate the access control risk, Kumar et al. (2017) recommend a defined access control policy and procedure for all systems used within the organisation. This policy should detail management's commitment and procedures around giving logical or physical access to employees, contractors, auditors or third-party service providers and compliance with best practice standards on access controls. It is the cloud service provider's responsibility to secure the physical environment of the cloud. The cloud service provider needs to ensure that the physical environment is monitored to detect potential cybersecurity events **(**Wang, 2016)**.** Access to cloud resources and related cloud infrastructure should be limited to approved users. A list of authorised users to the cloud servers must be kept and reviewed by management to ensure access is revoked for all terminated employees.

Physical access to IT resources should be supervised and secured by the cloud service provider. All visitors to the cloud facilities must be accompanied by an authorised or approved staff member (Ibrahim et al., 2018). Where necessary, and depending on the client organisation's form of business, a security clearance may need to be performed for any intended visits to ensure the security of data within the facility. All physical access must be monitored using cameras and manual logs, which should be reviewed regularly for authorisation (Fajar, Christian & Girsang, 2018). Any monitoring of remote access must be supervised by a delegated IT/Cloud personnel.

The cloud service provider must ensure there is segregation of duties when allocating users access rights. Network integrity must be secured while incorporating network segregation where appropriate (Jakimoski, 2016).

In terms of logical access controls, Huang, Debnath, Iorga, Kumar and Xie, (2019) state that access should be assigned on a role or privilege basis, to prevent access to sensitive data or critical configuration settings, within the cloud, that can affect the operation of security controls on the cloud. Management should create user access identities and credentials for approved users and devices on the network. Sensitive or critical data on the cloud may include privilege access control lists, filtering guidelines for routers or firewalls, configuration settings that enforce security controls, such as system password settings and system audit settings, and encryption key data. Therefore, to enforce access controls for logical access, it is imperative that role-based access controls are enforced on users with access to the cloud system's backend features (Changchit & Chuchuen, 2016).

To enhance these controls, the client organisation can prevent access to the cloud environment by implementing the device lockout control after periods of inactivity by the user. This prevents unauthorised logical access to the client organisation systems and data whenever an employee stops working or is absent from their device. The device lock can be implemented at the operating system level or application level. Management should ensure they review and supervise user access rights and controls on the cloud (Morrow, 2019).

4.6.7 GOVERNANCE AND DATA LOCATION CONTROLS

Jamal (2019) point out that the client organisation must evaluate the cloud service provider's location and the laws that govern processing and storage of data. This process can be handled by a Data Governance Body, which can help guarantee that the organisation has clear policies in place to maintain the effectiveness of data security and privacy requirements. The policies and procedures should address data

governance on the cloud, including personally identifiable data and ensuring it is adequately managed as per the relevant laws and guidelines of the client organisation's industry. The Data Governance Body can comprise of a chief information officer, senior information security officer and a privacy officer (Rashid & Chaturvedi, 2019).

Users with access and the responsibility of securing the confidentiality of data on the cloud should be clearly defined. The client organisation must also investigate the security controls in place of the cloud service provider's location and evaluate the legal implications of the laws and legislations of that location (Huang et al., 2019). This includes the ethical use and processing of data and its impact on the organisation's stakeholders and objectives. Mukherjee (2019) notes that the client organisation must take responsibility of ensuring that they and the cloud service provider comply with applicable laws around cloud applications and information and technology as per the NIST Security and Privacy Controls for Information Systems and Organisations Framework (2020).

4.6.8 CONSUMER RISK CONTROLS

NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) requires that the service provider meets the best practise standards of security and privacy controls when selecting a cloud service provider. The risk of having a cloud service provider must meet the organisation's acceptable risk tolerance levels. The level of assurance and confidence in the cloud service providers may also be influenced by the level of control the client organisation has on influencing the cloud service providers' security and privacy controls. It may also be based on the cloud service provider's willingness to exert the best security controls in the cloud environment and follow the client organisation's security policies in place. A thorough evaluation, during the selection of the cloud service provider, is therefore recommended (Satya, Alo, Pranab & Bhabani, 2018). The potential cloud service provider's industry reputation and any former contractual relationships should also be assessed. A clear SLA that defines what service the provider is responsible for, the rights over data and how it is processed and stored, and the protection of the cloud

infrastructure must be in place. The SLA should define levels of control, expectations and obligations for both parties (Khan & Gouveia, 2018).

The cloud service provider is required to give a full description of the cloud service and the security and privacy controls configured. There must be continuous monitoring plans in place to ensure that the system operates adequately and securely (Satya et al., 2018). Chapter 5 discusses the NIST Framework on Security and Privacy Controls for Information Systems and Organisations.

Summative comment

The following cloud computing controls were identified to address the cloud computing risks:

- Make use of security encryption tools and vulnerability scanners.
- Develop and define a Vulnerability Management Plan to address controls to mitigate security and privacy risks.
- Provide security and privacy awareness training based on defined roles and responsibilities for the client organisation and cloud service provider.
- Define a contingency plan and an access control policy.
- Monitor physical and logical access to the cloud environment.
- Have a Data Governance body in place, that comprises of the Chief Information Officer, Senior Information Security Officer and the Privacy officer, which will manage controls in terms of compliance with laws and regulations and the assessment of third-party service providers.

In the section below, the mitigating controls recommended by the POPI Act to address cloud computing risks are discussed.

4.7 MITIGATING CONTROLS SUGGESTED BY POPI

4.7.1 SECURITY CONTROLS

The POPI Act (2013) refers to security safeguards under condition 7 subsection 19 (2) (a-d) and subsection (3). These safeguards can be applied to the cloud at implementation stage and during operation. The cloud service provider must protect the truthfulness and privacy of personal information under its control by taking suitable, sensible technical and structural measures to avoid damage or illegal destruction of personal information; and illegal access to the processing of personal information (Crawford, 2018). To achieve security over data, the cloud service provider should conduct a risk assessment of all possible risks that may be a threat to its environment and the data it hosts. It should determine the security controls to address these risks. These controls should be monitored frequently, to evaluate their effectiveness, and must be regularly updated where necessary (Adendorff & Smuts, 2019).

According to Jackson (2017), these controls could include tools such as malware protection software that regularly scan computers on the network to detect and prevent threats. Staff, for both the client organisation and the cloud service provider, must be trained to recognise common threats such as phishing emails and malware infection. They must also when and how to report any data security breaches. General compliance with the accepted information security standards in the given industry of the client organisation must be adhered to (Weintraub & Cohen, 2016).

4.7.2 PRIVACY CONTROLS

Privacy, which usually complements security, is also a vital component that needs to be carefully addressed prior to implementing a cloud model. This means that strict controls on confidentiality of data on the cloud must be in place (Gunawan, 2019). The POPI Act (2013) addresses the risk to personal data across all cloud models and the risk to an individual's privacy rights. It touches on the responsibility of both the cloud service provider and client organisation on the lawful processing of information (Jackson, 2017). This entails handling all personal data in their control with

confidentiality and not sharing this data without the approval of the client organisation, unless when mandated to do so by law. These expectations of the cloud service provider, by the client organisation, must be outlined from the onset and defined in the SLA. This includes obligations to inform the client organisation when or if ever there is a breach in the cloud environment. The client organisation must avoid storing sensitive information on the cloud and safeguards must be implemented for the data that is stored for historical and statistical purposes (Weintraub & Cohen, 2016).

4.7.3 DATA INTEGRITY CONTROLS

The POPI Act (2013) states that the responsible party must take the necessary steps to see that data is complete, accurate, true and updated when necessary. To govern data integrity throughout its journey, the client organisation must follow a software development lifecycle. These software development lifecycles are important for understanding the various governance procedures necessary to manage data integrity according to regulatory and security requirements (Chandiwala, 2016).

This method is an integral step in understanding where data is and how it is deployed. This knowledge can be used as a foundation to create sustainable practices. To complement this process, the client organisation must develop process maps for critical data. This is a crucial aspect of governing how data is used, by whom and where. By mapping these processes ideally before data is used, organisations have greater control over their data assets. These maps are fundamental for implementing proper measures for data integrity, as well as security and regulatory compliance (Kalaiprasath, Elankavi & Udayakumar, 2017).

4.7.4 GOVERNANCE AND DATA LOCATION CONTROLS

The POPI Act requires that the client organisation assess the legal implications of keeping data on trans-border cloud applications as these may affect their ability to access this data. The cloud service provider must establish and approve a data

contingency plan in case of a data security breach so that data is always available to the client (Jackson, 2017).

When an organisation chooses to adopt cloud computing, special attention must be paid to the location of the cloud service provider's facilities. The governance of information varies from country to country and, therefore, the impact of non-compliance of laws and regulations would need to be considered (Brandis et al., 2019). These laws have a huge impact on an organisation's decision to adopt cloud computing or its selection of a cloud service provider, considering some cloud service providers are located outside the borders of South Africa (Jackson, 2017).

It is in the best interests of any client organisation to avoid any breaches in customer privacy when it comes to the selection of a cloud service provider (Adendorff & Smuts, 2019). Reference can be made to the South African POPI Act (2013) that addresses conditions of legal protection and processing of personal information, restrictions on transmitting, storing, or processing of personal information outside of South Africa. Refer to Chapter 5 on the Empirical Study and Research findings on cloud computing risks and the controls defined in the POPI Act of South Africa.

Summative comment

The following cloud computing controls were identified to address the cloud computing risks:

- Conduct a risk assessment on the risks that could affect the cloud environment.
- Determine security controls to mitigate the risk.
- Implement and monitor these controls regularly.
- Make use of security tools to monitor the cloud environment.
- Train staff on the common threats that could leave the environment vulnerable.

- Consider the lawful processing of data and compliance of laws and regulations.

The researcher also noted that availability, network capacity, access control, data segregation, multitenancy, and consumer risk were not addressed by the Act.

4.8 CRITICAL LINK TO EMPIRICAL STUDY

This Chapter explored literature on the four selected IT Governance Frameworks and how these Frameworks would address security risk, privacy risk, data integrity risk, availability and network capacity risk, data segregation and multitenancy risk, access control risk, governance and data location risk and consumer risk. It was observed that most of these risks were addressed by ISO/IEC 27002, COBIT and NIST Framework, whilst POPI focused on security, privacy, data integrity, governance and data location risks. The aim was to establish whether organisations could rely on these frameworks when adopting the cloud.

In Chapter 5, the cloud computing risks listed above will be clearly mapped against the IT Governance Frameworks to evaluate whether controls or guidelines are provided to mitigate the cloud computing risks. This important aspect of mapping the IT Governance Framework and the cloud computing risk will be analysed as follows:

Risk	Framework	Control	Paragraph
Security	ISO/IEC 27002		
	COBIT 2019		
	NIST		
	POPI Act		

4.9 CONCLUSION

The objective of this Chapter was to address how organisations could use IT Governance Frameworks to manage and improve their cloud applications by mitigating the risks discussed in Chapter 3. IT Governance controls that can be found in various Frameworks were discussed. Based on the literature review, controls and recommendations can be obtained from a combination of all the IT Governance Frameworks selected by the researcher or a selection of one Framework that suits the organisation's needs. Professional judgement and preference must be applied by the client organisation. Most risks are addressed in the selected Frameworks, with some of the Frameworks affording more detail in the mitigation of risks. A comparison of the risks and how they can be aligned to the IT Governance Frameworks will be clearly mapped out in Chapter 5 of the empirical study. The purpose of the study is to address how IT Governance Frameworks can ease the adoption of cloud computing solutions, whilst mitigating its risks. As such, the IT Governance Frameworks will be analysed and mapped against the cloud computing risks, bridging this gap in Chapter 5.

CHAPTER 5: EMPIRICAL STUDY AND RESERCH FINDINGS

5.1 INTRODUCTION

The objective of this study is to examine the risks that organisations face when implementing cloud computing applications and identify the IT Governance Frameworks that can be applied by organisations to manage and improve their cloud applications whilst mitigating risks. Relevant literature on cloud computing risks organisations was reviewed in Chapter 3. Chapter 4 discussed the IT Governance Frameworks that can be implemented to mitigate the cloud computing risks. The literature in Chapters 3 and 4 provided the basis for the elements that are tested in the empirical study. This Chapter discusses the empirical study and research findings. The empirical study evaluates the extent to which the selected IT Governance Frameworks address cloud computing risks identified in the literature.

5.2 IT GOVERNANCE FRAMEWORKS LINKED TO CLOUD COMPUTING RISKS

In this Chapter, the cloud computing risks will be mapped against ISO/IEC 27002, COBIT 2019, NIST Framework on Security and Privacy Controls for Information Systems and Organisations, and the POPI Act. Each risk will be addressed individually or grouped (as demonstrated in Chapter 4).

Table 5.1 below contains the IT Governance Framework control requirements that are essential to addressing cloud computing risks. An analysis will be done to evaluate whether the chosen IT Governance Frameworks could help manage or mitigate the risks discussed in this study for any organisation adopting cloud computing. This will answer the research question on the role IT Governance Frameworks have on addressing cloud computing risks and whether reliance can be placed on these Frameworks. In Table 5.1 below, the first column lists the cloud computing risks that were discussed in Chapter 3. The second column contains the selected IT Governance Frameworks discussed in Chapter 4. The third column addresses the controls recommended by the IT Governance Framework to mitigate the cloud computing risk. The last column links to the research findings.

Table 5.1: IT Governance Framework control requirements

Risk	Framework	Control	Paragraph
Security Risk	ISO/IEC 27002	• Define a security policy that addresses security controls around the cloud for both the client organisation and the cloud service provider; • The policy should address data segregation, physical and environmental security, data transfer, security against malware, management of vulnerabilities and encryption; • Implement security tools such as firewalls, intrusion detection/prevention systems, encryption software and vulnerability scans, that will continuously monitor the cloud security controls and make updates when necessary; and • Provide security awareness education and training to its employees on risks regarding security on the cloud.	5.3.1
	COBIT 2019	• Define a standard Data security management system that outlines controls that should be in place to secure the cloud; • Define roles and responsibilities of the client organisation and cloud service provider in managing security, privacy, availability,	

		integrity, network capacity, access control, data segregation, multitenancy, data location, governance and consumer controls for the cloud; • Conduct security and privacy awareness training for all users on the cloud; • Implement network filtering tools such as firewalls, intrusion detection software and vulnerability scanners; • Ensure that the latest security updates, patches and antivirus controls are in place across the cloud environment to protect information systems and technology from malware; • Ensure that there are frequent reviews of the adequacy and effectiveness of the security controls and tools used to mitigate risks on the cloud; and • Ensure that password authentication is enabled for all registered devices connecting to the cloud network to mitigate the risk of a data breach.	
	NIST	• Develop and define a Vulnerability Management Plan to address controls to mitigate security and privacy risks; • Make use of security encryption tools and vulnerability scanners to monitor the cloud against any	

		vulnerabilities and remediate any threats; and • Provide security and privacy awareness based on defined roles and responsibilities for the client organisation and cloud service provider.	
	POPI Act	• The client organisation and cloud service provider must take the necessary steps to guarantee the security of data on the cloud by utilising security software tools that will monitor the environment and protect it from vulnerabilities; • The client organisation and cloud service provider must conduct a risk assessment on the risks that could potentially affect data on the cloud; and • Develop and implement security controls and monitor these controls regularly.	
Privacy Risk	ISO/IEC 27002	• Define a policy and procedure addressing controls to secure privacy on the cloud; • The policy should address rights of ownership of data, transfer, storage and disposal of data, confidentiality and non-disclosure agreements in terms of the protection of personally identifiable information;	5.3.2

		• Ensure there is compliance of the relevant laws and regulations regarding privacy of data, that also address the location of both the client organisation and cloud service provider; and • Implement encryption software tools to prevent access from unauthorised persons.	
	COBIT 2019	• Define the expected service obligations related to privacy of information on the cloud in the SLA regarding collection, use, disclosure, management of personal data, confidentiality and the sale or sharing of information; • Ensure there is compliance of industry regulations on the protection of confidentiality of data; and • Appoint a Privacy Officer who will manage privacy risks related to legislation and regulations, implementation of controls.	
	NIST	• Privacy controls with regards to compliance with material privacy prerequisites; and • Management of privacy risk in relation to data or people related with the creation, collection, use, preparing, distribution or removal of personal information.	

	POPI Act	• Define and agree on the lawful processing of data in compliance with laws and regulations with the cloud service provider; • Define expected service obligation with the cloud service provider, on managing data privacy, sharing of data without the consent and approval of the client organisation; and • Ensure that the cloud service provider agrees in writing to immediately informing the client organisation where there is a breach in data on the cloud.	
Data Integrity Risk	ISO/IEC 27002	• There should be an audit log of all activities carried out on the cloud to monitor their authenticity; • These audit logs should be reviewed regularly by management to verify that data is accurate and true, protecting the original content from its source; • Management should ensure data is backed up and the original data and any replicas are well maintained and secure from alteration; • Implement cryptographic software tools to protect the integrity of the data; and • Test any security updates installed to the cloud systems prior an update	5.3.3

		to ensure that there is no disruption to the integrity of data.	
	COBIT 2019	• There should be a tracking system for any inaccurate data transactions made on the system to ensure they do not interrupt with the dispensation of valid transactions; and • Train users on the importance of data integrity to uphold a certain level of data quality (such as accuracy, completeness, validity, traceability and timeliness) and the risks in negligence to maintain this level of data quality.	
	NIST	• Secure all communication to prevent interception that could lead to any adjustments of that data and the disruption of data integrity; • This can be made possible with the use of encryption tools and integrity verification tools that can detect any unapproved modifications to software, firmware and data on the cloud; • Implement strong access controls to the cloud environment, both logical and physical to aid the protection of data integrity; and • The client organisation must assess and obtain better insight to the cloud service providers controls with	

		regards to confidentiality of data, to ensure integrity is not compromised.	
	POPI Act	• Develop and follow a software development lifecycle to monitor the flow of data and digital footprints of when the data was processed and by whom.	
Availability and Network Capacity Risk	ISO/IEC 27002	• Evaluate and screen the potential cloud service provider based on their reputation to provide reliable and sound infrastructure; • The client organisation must determine what their network capacity requirements are and ensure this is agreed upon in the SLA with the cloud service provider; • Define the critical systems of the client organisation so that these are prioritised during any scheduled downtime periods or in the event of a disaster; • The client organisation should agree in writing, on the continuous monitoring of the system to improve efficiency and availability of the cloud service from the cloud service provider; and • The cloud service provider should manage the network capacity and ensure that there is no outdated data that is consuming disk space; unnecessary applications, systems	5.3.4

		and databases in the cloud environment that are not in use and potentially restrict bandwidth on the cloud.	
	COBIT 2019	• The client organisation must consider its budget towards procuring the right amount of capacity on the cloud to ensure its needs in terms of availability and performance are prioritised; • The SLA should allow terms of flexibility with regards to changing capacity requirements for data stored on the cloud; and • Define a BCP/DRP to address the relevant controls to be followed in the event of a disaster and ensure that systems continue to operate and minimise periods of downtime.	
	NIST	• Define a contingency plan that will detail the recovery controls, restoration priorities and role and responsibilities in the event of a natural disaster or cyber-attack; and • Define a capacity plan that addresses the capacity for data processing, communications and cloud support needed and that should be available for the client organisation during contingency operations.	

	POPI Act	• The cloud service provider must establish and approve a data contingency plan in case of a data security breach to ensure that data is always available to the client.	
Data Segregation and Multitenancy Risk	ISO/IEC 27002	• The cloud service provider must segregate data for all for the different clients on the cloud to limit accessibility from unauthorised users; • The cloud service provider must, together with the client organisation, define and agree on what or which data should be treated as sensitive and critical to guarantee security in terms of privacy, integrity and accessibility on its cloud environment; • The cloud service provider should use encryption software tools to secure all data for the multiple clients on the cloud; and • Enforce user authentication and access controls for all users with access to the cloud server.	5.3.5
	COBIT 2019	• The cloud service provider should define the controls in place to safeguard and maintain confidentiality of its client's data kept on the cloud by correctly and securely segregating it from its multiple tenants;	

		• Categorise the client's data as restricted, sensitive and unrestricted to enhance sound management of data assets on the cloud servers; • Restrict and define user access according to defined roles and responsibilities on the management of critical data, data sharing, compliance of laws in terms of data privacy and the risk reduction for all clients on the cloud; • Implement user authentication and authorisations controls to ensure only approved users have access to the cloud; and • Monitor the flow of all data and keep track of inventory in the duration of the contract with the cloud service provider.	
	NIST	• Segregate the cloud environment according to the different clients hosted to ensure the security and confidentiality of data; and • the cloud service provider must separate the network addresses for the multiple tenants connecting to the cloud server.	
	POPI Act	*None*	
Access Control Risks	ISO/IEC 27002	• Access rights for logical access and physical access to the cloud must be defined and allocated based on the user's role and responsibilities for	5.3.6

		both the client organisation and cloud service provider; and • Implement security measures such as monitoring of access through record keeping and defining security parameters to the cloud servers.	
	COBIT 2019	• The cloud environment must be set up with equipment and devices that will monitor physical access to the cloud facilities, e.g. alarms and cameras; • Implement controls around user identity and logical access by ensuring that all users have data access rights in accordance with the organisation's requirements; • Ensure users have data access rights necessary for their specific roles in the organisation; and • Implement an encryption software tool that blocks cyber criminals from stealing/accessing data easily in a readable format.	
	NIST	• Define an access control policy; • The policy should detail management's commitment and procedures around granting logical or physical access to internal and external stakeholders of the organisation; • Monitor physical and logical access to the cloud environment and ensure	

		that it is limited to authorised users only; • Maintain a list of authorised users that is reviewed and updated when necessary, e.g. when new employees are appointed or when employees leave the organisation; • Maintain a record of all assets and devices on the network and review for authorisation; • Physical access to IT resources should be supervised and secured by the cloud service provider; • All visitors to the cloud facilities must be accompanied by an authorised or approved staff member; • Perform security clearance where necessary for external parties that may need to visit the cloud premises; • All physical access must be monitored with the use of cameras and manual logs, which should be reviewed regularly for authorisation; • Remote access to the client organisation's cloud network must be monitored and supervised by a delegated IT/Cloud personnel; • Assign logical access on a role or privilege basis to prevent access to sensitive data or critical configuration settings within the cloud that can possibly affect the	

		operation of security controls on the cloud; and • Implement the device lockout security function on employee devices for periods of inactivity and mitigate unauthorised access to hackers.	
	POPI Act	*None*	
Governance and Data Location Risk	ISO/IEC 27002	• Both the client organisation and cloud service provider must consider compliance of applicable laws and regulations around the cloud, for the industry and geographical location of both parties.	5.3.7
	COBIT 2019	• The Privacy Officer should manage and make sure there is compliance with the relevant local or international laws governing the client organisation or the cloud service provider.	
	NIST	• Have a Data Governance body in place comprising the Chief Information Officer, Senior Information Security Officer and the Privacy officer, who will manage controls in terms of compliance of laws and regulations and the assessment of third-party service providers.	
	POPI Act	• Assess the legal implications of keeping data on trans-border cloud applications as this may affect the	

		client organisation's ability to access data; and • Consider compliance of laws internally and externally and their effect on the client organisation data,	
Consumer Risk	ISO/IEC 27002	• The client organisation must define, in the SLA with the cloud service provider, the following: ✓ The expected conditions of service; ✓ Access rights to the client's data; ✓ Rights to have the cloud service provider's processes, procedures and security controls audited; and ✓ Conditions that warrant the client organisation to cancel their contract with the cloud service provider, e.g. breach of contract agreement.	5.3.8
	COBIT 2019	• The client organisation must select the cloud deployment and cloud service model that will suit their organisation's operations and objectives. This is imperative especially in evaluating the security controls that may be affected by the different models and services and how they may impact the organisation at large; and	

		• The client organisation must manage all potential and existing contracts and validate their compliance to the organisation's policies, legal and regulatory requirements.	
	NIST	• Thoroughly evaluate all potential cloud service providers by assessing current or previous contractual agreements and industry reputations; • Clearly define service obligations and requirements in the SLA for the client organisation and cloud service provider; • The SLA should address rights over data, how it is processed and stored, and the protection of cloud infrastructure; • The cloud service provider is required to give a full description of the cloud service and security and privacy controls they will configure on the cloud to ensure security for the client organisations data; and • Ensure there are continuous monitoring plans in place to ensure that the system operates adequately and securely.	
	POPI Act	*None*	

5.3 RESEARCH FINDINGS

In this section, the researcher analysed the results in Table 5.1 of the cloud computing risks and IT Governance Frameworks. The analysis shows how the Frameworks address the cloud computing risks through the mitigating controls suggested by the Frameworks. This will indicate to the reader whether an organisation can place reliance on the selected Frameworks to mitigate the particular risk. The objective and findings of each cloud computing risk will be explained and discussed below.

5.3.1 SECURITY RISK

The objective was to determine whether organisations can use the IT Governance Frameworks to manage or mitigate security risk on the cloud. In the literature review, it was established that the security of the cloud was a huge component in the successful implementation of cloud applications. The various security risks that could hinder the cloud application's functionality, that is, malware and vulnerability related risks, were discussed. It was noted that if security is not adequately addressed, privacy of information, access controls, the cloud's assets, operating systems and databases could be largely affected (Mukherjee, 2019). Table 5.1 above illustrates the controls recommended by ISO/IEC 27002, COBIT 2019, NIST and the POPI Act in addressing security risk.

It was noted that all four frameworks addressed the issues related to malware and vulnerability risks on the cloud by recommending control measures, such as implementing security software tools and security policies to govern security controls on the cloud. The recommended security tools were firewalls, intrusion detection/prevention systems, encryption software and vulnerability scans. These would continuously monitor the effectiveness and adequacy of the cloud security controls and provide timely updates and patches when necessary.

The frameworks further recommended formally defining controls that should be implemented in mitigating security risk in the cloud. The following were noted:

- ISO/IEC 27002 (2013) recommends defining a security policy to govern the security controls and mitigate security risk on the cloud.
- COBIT 2019 Framework, (2018) recommends a data security management system that defines security controls on the cloud.
- The NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) addresses security risk by defining a vulnerability management plan to address controls to mitigate security and privacy risks; and
- The POPI Act recommends evaluating risks that could potentially affect the cloud and implement security controls to mitigate the risk.

Findings from Table 5.1 above showed that ISO/IEC 27002, COBIT 2019 and NIST recommended controls around providing security awareness education and training for employees to mitigate the risk of falling prey to threats and vulnerabilities that may place the cloud environment at risk. From the analysis above, all these control measures address security risk of malware and vulnerabilities on the cloud, with the COBIT 2019 Framework providing more security controls than ISO/IEC 27002, NIST and the POPI Act.

5.3.2 PRIVACY RISK

The objective was to derive whether organisations can use the IT Governance Frameworks below to manage or mitigate the risk of privacy on the cloud. The literature review discussed the privacy risks which were noticeably linked to data collection and storage, data location, unauthorised access to data and the laws governing data depending on where the cloud service provider is located. All these elements, if not carefully considered, can pose a risk to the client organisation's data privacy on the cloud (Bailey & Becker, 2014). Table 5.1 above illustrates the controls recommended by ISO/IEC 27002, COBIT 2019, NIST and the POPI Act in addressing privacy risk on the cloud.

It was noted that all four frameworks addressed the issues related to rights of ownership to data, transfer, storage and disposal of data, service obligations related

to privacy of information on the cloud, as well as compliance of the relevant laws and regulations regarding privacy of data. ISO/IEC 27002 (2013) further recommends that there should be a defined policy and procedure addressing control measures on privacy and protection of personally identifiable information on the cloud. This should be enhanced by the implementation of encryption software tools to prevent unauthorised access on the cloud.

COBIT 2019 Framework (2018) recommends appointing a Privacy Officer who will manage all risks related to privacy and manage or approve the implementation of controls to mitigate the risk. All these control measures address privacy risk linked to data collection and storage, data location, unauthorised access to data and the laws governing data depending on where the cloud service provider is located. Reliance can be placed on any of the four frameworks to address privacy risk.

5.3.3 DATA INTEGRITY RISK

The objective was to derive whether organisations can use the IT Governance Frameworks below to manage or mitigate the risk of data integrity on the cloud. In the literature review, data integrity risk, as the safety of information against any form of manipulation to represent its accuracy, completeness and integrity, was discussed. Table 5.1 above illustrates the controls recommended by ISO/IEC 27002, COBIT 2019, NIST and the POPI Act in addressing data integrity risk on the cloud.

In the findings, it was noted that ISO/IEC 27002 and COBIT 2019 addressed issues, such as enabling and reviewing audit logs to track activities carried out on the cloud, for authenticity to ensure data remains accurate. ISO/IEC 27002, (2013) also addressed recommended control measures on the backup and replication of information on the cloud to secure the original source from any alterations. Reference was also made to the use of cryptographic software tools and keeping security updates on the latest versions to protect the integrity of the data and avoid the disruption of its authenticity.

COBIT 2019 Framework recommended training of users on the importance of data integrity to uphold a certain level of data quality (such as accuracy, completeness, validity, traceability and timeliness) and the risks in negligence to maintain this level of data quality. NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) results refer to the use of security tools such as encryption tools and integrity verification tools that can detect any unapproved modifications to software, firmware and data on the cloud and secure communications on the cloud. Whilst the POPI Act (2013) addresses data integrity risk by developing a software development lifecycle to monitor the flow of data, digital footprints of when the data was processed and by whom are unavailable.

From the analysis above, all these control measures address integrity risk linked to safety of information against any form of manipulation to represent its accuracy, completeness and integrity on the cloud. Reliance in mitigating data integrity risk can be placed on the NIST Framework as it provides more controls on data integrity in comparison to ISO/IEC 27002, COBIT 2019 and the POPI Act.

5.3.4 AVAILABILITY AND NETWORK CAPACITY RISK

The objective was to derive whether organisations can use the IT Governance Frameworks below to manage or mitigate availability and network capacity risk on the cloud. In the literature review in Chapter 4 it was established that availability and network capacity relied on each other for optimal service performance on the cloud. Where network capacity is not managed accordingly, availability of data may be adversely affected should the cloud server crash. Availability and network capacity risks that could hinder the cloud application's functionality were discussed in chapter three. Issues such as inadequate capacity requirements, poor network assessment of the cloud computing system and inability to access the cloud during periods of downtime resulting from maintenance, natural disaster or a cyber-attack were identified. It is therefore imperative that the client organisation and cloud service provider decide on continuity related matters and capacity on the cloud (Bounagui et al., 2019). Table 5.1 illustrates the controls recommended by ISO/IEC 27002, COBIT

2019, NIST and the POPI Act in addressing availability and network capacity risk on the cloud.

The control measures provided by the four frameworks are different, but they all address issues related to availability and network capacity risk uniquely. ISO/IEC 27002 (2013) addressed the importance of selecting a reliable and reputable cloud service provider with sound infrastructure, making clear arrangements on the network capacity requirements prior to procuring the cloud service and defining critical systems that should be prioritised during periods of downtime. COBIT 2019 Framework (2018) recommended that the client organisation should consider its budget when procuring the capacity they would need on the cloud, define a BCP/DRP to address the relevant controls to be followed in the event of a disaster and ensure that systems are prepared to handle continued operations in the event of a disaster.

NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) recommends defined contingency and capacity plans. These will address recovery controls, restoration priorities and role and responsibilities for data processing, communications and cloud support during contingency operations as control measures. The POPI Act (2013) recommends that the cloud service provider establish and approve a data contingency plan in case of a data security breach to ensure that data is always available to the client.

From the analysis in Table 5.1 and the discussion above, all these control measures address availability and network capacity risk such as inadequate capacity requirements, poor network assessment of the cloud computing system and inability to access the cloud during periods of downtime resulting from maintenance, natural disaster or a cyber-attack. Organisations can choose to place reliance on ISO/IEC 27002, COBIT 2019 or the NIST Framework for control measures addressing availability and network capacity risk.

5.3.5 ACCESS CONTROL RISK

The objective was to derive whether organisations can use appropriate IT Governance Frameworks to manage or mitigate access control risk on the cloud. In the literature review it was established that access to data on the cloud should be restricted. These restrictions should comprise of both logical and physical access controls. Table 5.1 illustrates the controls recommended by ISO/IEC 27002, COBIT 2019 and NIST to address access control risk on the cloud.

It was noted that ISO/IEC 27002, COBIT and NIST recommend control measures related to the allocation of access based on the user's role and responsibilities for both the client organisation and cloud service provider. The implementation of security measures, such as monitoring of access through record keeping and defining security parameters to the cloud servers, is also key. The COBIT 2019 Framework (2018) further recommends the use of an encryption software tool that blocks cyber criminals from obtaining logical access that may allow them to steal/access data easily in a readable format on the cloud. NIST Framework on Security and Privacy Controls for Information Systems and Organisations (2020) recommends that there be a defined access control policy and that security clearances be carried out where necessary for external parties that may need to visit the cloud premises.

The analysis in Table 5.1 and the preceding discussion demonstrate that the control measures provided by ISO/IEC 27002, COBIT and NIST address the access control risk for logical and physical access. However, NIST provides more details and controls measures that may provide more secure controls. As such, more reliance can be placed on the NIST Framework on Security and Privacy Controls for Information Systems and Organisations. Little detail is provided by the POPI Act for logical and physical access as the Act only places emphasis on information granted to authorised personnel only. Not much reliance or reference can be made from POPI to address access control risk.

5.3.6 DATA SEGREGATION AND MULTITENANCY RISK

The objective was to derive whether organisations can use the IT Governance Frameworks below to manage or mitigate data segregation and multitenancy risk on the cloud. In the literature review in Chapter 4, it was established that data segregation and multitenancy relied on each other for optimal service performance on the cloud. The public cloud has multiple clients on its servers, which concurrently means multiple segments of data unique to the different clients (Cayirci, Garaga, Oliveira & Roudier, 2016). It is therefore important, as highlighted in the literature review, that the multiple clients are protected from sharing data, breach or loss of data on the servers and data replication on various sites (which could be the wrong cloud tenant). Table 5.1 illustrates the controls recommended by ISO/IEC 27002, COBIT 2019, NIST and the POPI Act in addressing data segregation and multitenancy risk on the cloud.

ISO/IEC 27002, COBIT 2019 and NIST 2020 recommend the segregation of networks amongst the different clients, restrictions on access to the cloud platform to limit accessibility from unauthorised users; securely segregating data for the multiple tenants; categorising the client's data and data assets in terms of its sensitivity; making use of encryption software tools to secure all data for the multiple clients on the cloud; and enforcing user authentication and access controls for all users with access to the cloud server. COBIT 2019 Framework (2018) further recommends the monitoring of all data for the duration of the contract with the cloud service provider.

All the control measures address the data segregation and multitenancy risk. However, COBIT and ISO/IEC 27002 provide more details and controls measures in addressing the risk. As such more reliance can be placed on these two frameworks. POPI Act (2013) does not give any guidelines on data segregation and multitenancy risks.

5.3.7 GOVERNANCE AND DATA LOCATION RISK

The objective was to determine whether organisations can use the IT Governance Frameworks below to manage or mitigate governance and data location risk on the cloud. In the literature review in Chapter 4, it was established that governance and data location relied on each other for optimal service performance on the cloud. The governance and data location risks, related to inadequate laws and legislation governing the cloud and services offered by trans-border cloud service providers, that could hinder the cloud application's functionality were discussed. Table 5.1 illustrates the controls recommended by ISO/IEC 27002, COBIT 2019, NIST and the POPI Act for addressing governance and data location risk on the cloud.

All four frameworks referred to the consideration of compliance with applicable laws and regulations around the cloud for the client organisation and cloud service provider. COBIT 2019 Framework (2018) recommended the appointing of a Privacy Officer to manage compliance with the relevant local or international laws governing the client organisation or the cloud service provider. NIST (2020), on the other hand, recommended having a Data Governance body in place that would comprise the Chief Information Officer, Senior Information Security Officer and the Privacy officer, who would manage controls in terms of compliance with laws and regulations, and the assessment of third-party service providers.

Based on the literature review, governance of the cloud is mainly linked with the location of where the client organisation's data sits. Careful consideration and compliance of laws, regulations, as well as industry best practices must be followed (Al-Ruithe et al., 2016). The IT Governance Frameworks discuss compliance of legal regulatory requirements for data on the cloud. These include privacy regulations of the cloud service providers' country. Organisations within the Republic of South Africa, or businesses with financial interest within South Africa, must rely on the privacy laws recommended by the POPI Act (2013). The act provides guidelines on how a client organisation within the Republic must manage data stored outside the borders of South Africa. The first point of reference in terms of governance and data location

would be the POPI Act (2013). Further reliance can thus be made on ISO/IEC 27002, COBIT and NIST for guidance on industry's best practice.

5.3.8 CONSUMER RISK

The objective was to derive whether organisations can use the IT Governance Frameworks to manage or mitigate consumer risk on the cloud. Table 5.1 illustrates the controls recommended by ISO/IEC 27002, COBIT 2019 and NIST for addressing consumer risk on the cloud. Careful consideration of whom to select as the cloud service provider is vital to the successful adoption of cloud computing. It also has a major role on the safety of the client organisation's data and how the risks associated with the cloud can be managed (Adendorff & Smuts, 2019). Poor selection of the cloud service provider can result in poor service delivery and breach of data and possible financial losses (Cayirci et al., 2016).

ISO/IEC 27002, COBIT and NIST Frameworks provide adequate controls in managing consumer risk. All three have recommendations on managing relationships with the cloud service provider and terms and conditions that should be addressed in the SLA. Emphasis should be made on the compliance of laws and regulations for both parties. It is also important that performance evaluations are done to monitor the quality of service delivered. Therefore, it is imperative to ensure a thorough screening is done during the selection process.

The following controls were addressed by ISO/IEC 27002, COBIT 2019 and NIST frameworks; the expected conditions of service; access rights to the client's data; rights to have the cloud service providers processes, procedures and security controls audited; and conditions that warrant the client organisation to cancel their contract with the cloud service provider when there is a breach of contract agreement. From the analysis in Table 5.1 and the discussion above, it may be concluded that all the control measures address consumer risk. However, NIST and ISO/IEC 27002 provide more details and control measures that address the risk. Resultantly, more reliance can be placed on these two frameworks.

5.4 CONCLUSION

This Chapter established the extent to which the four IT Governance Frameworks address the cloud computing risks identified in the literature. The cloud computing risks were mapped to the IT Governance Frameworks. Findings on which Frameworks organisations could place reliance on when adopting the cloud to mitigate computing risks of security, privacy, integrity, availability and network capacity, data segregation and multitenancy, access controls, governance, data location and consumer risk were drawn.

In the analysis of IT Governance Frameworks, it was found that most of the cloud computing risks could be avoided if organisations applied the principles or controls suggested in the Frameworks. However, the selection of which IT Governance Framework to rely on should ultimately be based on the organisation's business objectives, industry and location. As discussed in the literature review, the successful implementation of the cloud is highly dependent on the security controls administered by the client organisation and the cloud service provider.

The COBIT 2019 Framework recommends more control measures for addressing security risk. It can be considered as the first choice in the selection of IT Governance Frameworks for the cloud. ISO/IEC 27002 and the NIST Framework on Security and Privacy Controls for Information Systems and Organisations also provides control measures that would be suitable to govern the cloud and would depending on the client organisation's business. Not much reliance can be placed on the POPI Act in addressing the listed cloud computing risks, but it should be relied on for the security, privacy and integrity of personally identifiable information, as well as the lawful processing of this information.

The results of mapping the cloud computing risks against the IT Governance Frameworks prove that IT Governance Frameworks have a significant role in

addressing cloud computing risks. Therefore, whilst there may not be a cloud computing governance framework specifically, organisations can safely rely on established IT Governance Frameworks to govern the cloud and manage the applications risks. Chapter 6, which follows, presents a summary and conclusion of the literature review and empirical study and the study objectives were achieved.

CHAPTER 6: CONCLUSION

6.1 INTRODUCTION

The primary objective of this study was to understand the risks faced in implementing cloud computing applications within organisations. The secondary objective was to evaluate how these risks could be mitigated using IT Governance Frameworks. The third objective was to establish which IT Governance Framework can best be applied by organisations in managing and improving their cloud applications while avoiding these risks. This chapter summarises the research findings in chapter 5 and the findings of the literature review in Chapter 3 and 4. Future areas of research are also identified.

6.2 DEDUCTIONS

6.2.1 LITERATURE REVIEW

The literature review described the cloud computing risks and the role IT Governance Frameworks had in managing and mitigating these risks. It indicated the importance of relying on IT Governance Frameworks for the successful implementation of the cloud in an organisation. The Frameworks provided controls and guidelines on the elements which organisations need to look out for to make sure that the cloud is secure and in compliance with industries laws and regulations.

The significant findings from the literature study are as follows:

- Security on the cloud is imperative for any cloud model to ensure that the client organisation's data is not breached.
- The laws governing the cloud service provider, and any weak security controls around access to confidential information, pose a threat to privacy on the cloud.
- Data hosted by the cloud service provider cannot be easily monitored and the efforts to track this data must be defined in the SLA.
- Lack of a business continuity plan and the evaluation of network capacity could affect the client organisation's ability to access its information at any given time.

- Security software tools are a vital component in protecting data from misuse by cyber criminals.
- Not restricting access to confidential information to the appropriate personnel can pose a risk to the integrity of the client organisation's data.
- It is important for the client organisation to go through the terms and conditions of any contract with the cloud service provider before agreeing to the SLA.
- The cloud service provider must ensure there is separation and inaccessibility among tenants during transfer of data, storage and service delivery, if the cloud deployment model is public.
- Roles and responsibilities between the client organisation and the cloud service provider must be clearly defined in the SLA.

6.2.2 ANALYSIS

The analysis found that:

- The cloud computing risks are largely addressed by ISO/IEC 27002, COBIT 2019 and the NIST Frameworks. The POPI Act only addresses control measures for security and privacy risk to a larger extent.
- Business continuity plans and Disaster recovery plans are vital to guarantee availability of data, and enough network capacity so that the servers do not crash.
- Much reliance in terms of mitigating the risk of governance and data location should be made to the POPI Act for organisations within the Republic of SA.
- Awareness training must be offered, to both the staff of the client organisation and the cloud service provider, on cloud computing risks.
- The analysis indicates that IT Governance Frameworks have a significant role in addressing cloud computing risks, as they all described controls to mitigate the risks.
- Organisations can place reliance on IT Governance Frameworks when implementing the cloud to their environment.

6.3 POSSIBLE AREAS FOR FUTURE RESEARCH

The following could be recommended as focus areas in the IT Governance Frameworks:

- Training of client organisations on how and why to effectively apply IT Governance Framework guidelines to cloud applications; and
- Emphasis on security awareness training for the safety of information on the cloud and a better understanding for the need for it.

6.4 CONCLUSION

The purpose of this study was to evaluate the role of IT Governance Frameworks in addressing cloud computing risks. The research described the various cloud computing risks that organisations were faced with when implementing the cloud. This posed the question of how well organisations could use IT Governance Frameworks to mitigate cloud computing risks. The gap identified in adopting the cloud was mainly that organisations could not refer to a cloud governance Framework that could provide guidance on mitigating its risks or, more so, govern it. However, because cloud computing falls under IT, the IT Governance Frameworks were chosen to bridge the gap in addressing cloud computing risks.

Based on the analysis in Chapter 5, there is a clear indication that the controls provided by the IT Governance Frameworks can be used by organisations when adopting the cloud. Professional judgement must be made in the selection of Frameworks to ensure the organisation's objectives are met. The selection process should be based on the client organisation's choice of cloud deployment or service models discussed in Chapter 3. In conclusion, sound and effective governance on the cloud can be achieved by applying the control measures recommended by the IT Governance Frameworks. This would provide added assurance for the organisation's executives and governing body that its data is protected, secure, available and governed on the cloud.

REFERENCE LIST

Adam, C. (2017). *Threats and Attacks* (Lecture notes). Ohio: University of Ohio State.

Adendorff, R. and Smuts, H. (2019). *Critical Success Factors for Cloud Computing Adoption in South Africa. Twenty-fifth Americas Conference on Information Systems,* Cancun, Mexico.

Adjei, J.K. (2015). Explaining the role of trust in computing services*. Emerald publishing group limited*, 17(1):54-67.

Ahmad, I., Mukhneri, M., Mochamad, W. and Karlena, I. (2017). Information Technology Governance Using COBIT 4.0 Domain Delivery Support and Monitoring Evaluation. *Journal of Theoretical and Applied Information Technology,* 95(2017): 1992- 8645.

Akande, A.O and Van Belle, J.P. (2014). *A Proposed Framework to Assess and Increase the Cloud Computing Readiness of Financial Institutions in South Africa. 5th International Conference- Confluence the Next Generation Information Technology Summit (Confluence),* 48:978-1-4799-4236-7/14*.* Available from: 10.1109/CONFLUENCE.2014.6949250.

Alali, F.A. & Yeh, C.L. (2012). Cloud Computing: Overview and Risk Analysis. *Journal of Information System,* 26(2):13-33

Aldossary, S. and Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: Issues and current solutions. *International Journal of Advanced Computer Science and Applications*, 7(4):485-498.

Al-hashimi, M., Othman, M., Sulaiman, H and Zaidan, A.A. (2018). Information Security Governance Frameworks in Cloud Computing an Overview. *Journal of Advanced Computer Science and Technology Research*, 8(2):67 – 81.

Ali, O. Shrestha, A. Chatfield, A and Murray, P. (2020). Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities. *Government Information Quarterly,* 37 (2020): 101419.

Aljumah, A. and Ahanger, T.A. (2020). Cyber Security Threats, Challenges and Defence Mechanisms in Cloud Computing. *IET Communications,* 7: 1185-1191.

Alloussi, H., Fetjah, L. and Chaichaa, A. (2016). Securing Card Data on the Cloud. *International Journal on Advances in Security,* 9 (2016): 36-48.

Al-Ruithe, M, Benkhelifa, E. and Hameed, K. (2016). A Conceptual Framework for Designing Data Governance for Cloud Computing. *Procedia Computer Science,* 94 (2016):160-167.

Anand, P., Ryoo, J., Kim, H. and Kim, E. (2016). Threat Assessment in the Cloud Environment- A Quantitative Approach for Security Pattern Selection. Available from: http://dx.doi.org/10.1145/2857546.285546.2857552.

Andry, J.F. and Hartono, H. (2017). Performance Measurement of IT Based on COBIT Assessment: A Case Study. *Association for Information Systems- Indonesia Chapter*

Arafat, M. (2018). Information Security Management System Challenges Within a Cloud Computing Environment. *Association for Computing Machinery.* Available from: https://doi.org/10.1145/3231053.3231127

Bailey, E and Becker, J.D. (2014). *A Comparison of IT Governance and Control Frameworks in Cloud Computing. Twentieth Americas Conference on Information Systems, Savannah.*

Bansidhar, J., Bineet, J. & Kritika, R. (2017). *Mitigating Data Segregation and Privacy Issues in Cloud Computing. Proceedings of International Conference on Communications and Networks:* 175-182

Binance Academy (2019). *What is a replay attack?* Available from: https://www.binance.vision/security/what-is-a-replay-attack.

Borgolte, K., Fiebig, T., Hao, S., Kruegel, C. and Vigna, G. (2018). Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates. Network and Distributed Systems Security (NDSS) Symposium.

Bounagui, Y., Mezrioui, A. & Hafiddi, H. (2019). Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models. *Computer Standards & Interfaces* 62 (2019) 98-118

Brandis, K., Dzombeta, S., Colomo-Palacios, R. and Stantchev, V. (2019). Governance, Risk and Compliance in Cloud Scenarios. *Applied Sciences.* Available from: https://www.mdpi.com/2076-3417/9/2/320.

Bryman, A and Bell, E. (2014). *Research methodology: Business and Management contexts* Cape Town: Oxford University Press Southern Africa (Pty) Limited.

Buchy, J. (2016). *Cyber Security vs. IT Security: Is There a Difference?* Available from: http://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference/.

Caldarelli, A., Ferri, L. and Maffei, M. (2016). Expected benefits and perceived risks of cloud computing: an investigation within an Italian setting [Abstract]. *Journal of Technology Analysis and Strategic Management,* 29: 167-180. Abstract available from: https://www.tandfonline.com/doi/abs/10.1080/09537325.2016.1210786.

Candiwan, C. and Priyadi, Y. (2016). Analysis of Information Security Audit Using ISO 27001:2013 and ISO 27002:2013 at IT Division- X Company, in Bandung, Indonesia. *International Journal of Basic and Applied Science.* 4(4): 77-88.

Cayirci. E., Garaga, A., Oliveira, A.S. and Roudier, Y. (2016). A Risk Assessment Model for Selecting Cloud Service Providers. *Journal of Cloud Computing: Advances, Systems and Applications,* 51(4): 1-12.

Chandiwala, B.D. (2016). Data Integrity Challenges in Cloud Computing. Available from: https://www.semanticscholar.org/paper/DATA-INTEGRITY-CHALLENGES-IN-CLOUD COMPUTING-Chandiwala/276046ac1e0fa92763a1444a8097bf81a79a54f9.

Chandran, S.P. and Angepat, M. (2012). Cloud Computing: Analysing the risks involved in cloud computing environments. *School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden.*

Changchit, C. and Chuchuen, C. (2016). Cloud Computing: An Examination of Factors Impacting Users' Adoption [Abstract]. *Journal of Computer Information Systems,* 58:1-9. Available from: https://www.tandfonline.com/doi/full/10.1080/08874417.2016.1180651?scroll=topandneedAccess=true.

Choudhury, T., Gupta, A., Pradhan, S., Kumar, P. and Rathore, Y. S. (2017). *Privacy and Security of Cloud-Based Internet of Things (IoT). International Conference on Computational Intelligence and Networks*. 3:40-45.

Chunming, R., Nguyen, S.T. & Martin, G.J. (2013). Beyond Lightning: A Survey on Security Challenges in Cloud Computing. *Computers & Electrical Engineering,* 39(1): 47-54

Clouds Standards Customer Council (CSCC). (2015). *Security for Cloud Computing Ten Steps to Ensure Success Version 2.0***.** Available from: www.cloud-council.org>deliverables.

Control Objectives for Information and Related Technology (COBIT) 2019 Framework, (2018). Governance and Management Objectives. 2018 ISACA. ISBN 978-1-60420-764-4.

Collins, L. (2014). *Access Controls in Cyber Security and IT Infrastructure Protection*. Available from: https://www.sciencedirect.com/topics/computer-science/logical-access-control.

Crawford, K. (2018). Money Marketing: POPI and the Cloud Compliance Feature. *MoneyMarketing*, 11: 8-8.

Creswell, J.W. (2003). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* New York: Sage Publications.

Deacutis, M. (2015). *The Cloud and Security Governance.* (Master's Dissertation). New York: Utica College.

Dobrygowski, D. and Bohmayr, W. (2017). *Three big lessons to learn from the Equifax data breach.* Available from: https://www.cnbc.com/2017/09/20/cybersecurity-lessons-from-equifax-data-breach--commentary.html.

Enslin, Z. (2012). Cloud computing adoption: Control objectives for information and related technology (COBIT) -mapped risks and risk mitigating controls. *African journal of business management, 6(37*)· Available from: https://www.researchgate.net/publication/267366057.

Ernst and Young (2014). *Five insights for executives. Governing the cloud: Drive innovation and empower your workforce through responsible adoption of the cloud.* Available from: https://www.ey.com/Publication/vwLUAssets/EY_-_Governing_the_cloud/%24FILE/EY-Governing-the-cloud.pdf.

Faizi, S.M. and Rahman, S. (2019). Securing Cloud Computing Through IT Governance. *IT in Industry,* 7(2019).

Fajar, A.N., Christian, H. and Girsang,A.S. (2018). Evaluation of ISO 27001 Implementation Towards Information Security of Cloud Service Customer in PT. IndoDev Niaga Internet. *International Conference on Computation in Science and Engineering,* 1090(2018). Available at: 10.1088/1742-6596/1090/1/012060

Farrag, M.H. and Nasr, M.M. (2017). A Survey of Cloud Computing Approaches, Business Opportunities, Risk Analysis and Solving Approaches. *Int. J. Advanced Networking and Applications,* 9 (2): 3382-3386.

Gangan, S. (2015). *A Review of Man-in-the-Middle Attacks.* Available from: https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf.

Garrisona, G., Wakefield, R.L. and Kimc, S. (2015). The effects of IT capabilities and delivery model on cloud computing success and firm performance for cloud supported processes and operations. *International Journal of Information Management*, 35:377–393.

Gerber, P. (2015). *Addressing the Incremental Risks Associated with Social Media by Using the COBIT 5 Control Framework* (Master's Dissertation). Stellenbosch: Stellenbosch University.

Goyal, S. (2015). *Security, Privacy, Threats and Risks in Cloud Computing — a Vital Review.* DOI: 10.18100/ijamec.29177.

Grama, J.L. (2016). Understanding Information Security and Privacy in Postsecondary Education Data Systems. Available from: http://www.ihep.com/sites/default/files/uploads/postsecdata/docs/resources/information_security_and_privacy.pdf.

Griffin, P. (2016). Gaining Confidence in the Cloud. *ISSA Journal*, 14(1): 22-26.

Grimes, R.A., (2013). *The 5 cloud risks you must stop ignoring.* Available from: https://www.csoontime.com/article/2614369/security/the-5cloud-risks-you-have-to-stop-ignoring.html. Accessed 5 October 2017.

Gunadham, T. and Kuacharoen, P. (2016). Security Concerns in Cloud Computing for Knowledge Management Systems. *Journal of Applied Statistics and information Technology*, 1(2). Available from: https://www.tci-thaijo.org/index.php/asit-journal/issue/view/12650.

Gunawan, W.W. (2019). Measuring Information Security and Cybersecurity on Private Cloud Computing. *Journal of Theoretical and Applied Information Technology,* 97(1):156-168.

Heale, R. and Twycross, A. (2015). Validity and Reliability in Quantitative Studies. *Evidence- Based Nursing*, 18(3). Available from: https://ebn.bmj.com/content/18/3/66.info.

Huang, J.K., Zhang, Z.X. Li and Xin, Y. (2018). Assessment of the Impacts of TLS Vulnerabilities in the HTTPS ecosystem of China. *Procedia Computer Science,* 147: 512-518.

Huang, Y., Debnath, J., Iorga, M., Kumar, A. and Xie, B. (2019). *CSAT: A User-interactive Cyber Security Architecture Tool Based on NIST- Compliance Security Controls for Risk Management. 0th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference.* New York City, USA

Hussain, S.A., Fatima, M., Saeed, A., Raza, I. and Shahzad, R.K., (2016). Multilevel classification of security concerns in cloud computing. *Applied Computing and Informatics*, 7(1):253-257.

Hussein, N.H. and Khalid, A. (2016). A survey of Cloud Computing Security challenges and solutions*. International Journal of Computer Science and Information Security (IJCSIS)*, 14(1): 52-56.

Ibrahim, A., Valli, C., McActeer, I. and Chaudhry, J. (2018). A Security Review of Local Government Using NIST CSF: A Case Study. *The Journal of Supercomputing,* 74(1): 5171-5189.

Ibrahim, A.S, Harris, J.A and Grundy J. (2010). *Emerging Security Challenges of Cloud Virtual Infrastructure. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia.*

Implementing the NIST Framework on Security and Privacy Controls for Information Systems and Organisations, (2014). ISBN 978-1-60420-358-2

Information Systems Audit and Control Association (ISACA). (2011). *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud.* Illinois: ISACA.

Institute of Directors Southern Africa (IoDSA). (2016). *King IV Report on Corporate Governance for South Africa.* Johannesburg: IoDSA.

International Standard ISO/IEC 27002, (2013). Information Technology-Security Techniques- Code of Practice for Information Security Controls. Reference number ISO/IEC 27002:2013 (E).

Iqbal, S., Kiah, L.M., Anuar, N.B., Daghighi, B., Wahab, A.W.A and Khan, S. (2016). Service Delivery Models of Cloud Computing: Security Issues and Open Challenges. *Security and communication networks*, 9 (17):4726–4750. DOI: 10.1002/sec.1585.

Information Systems Audit and Control Association (ISACA) (2014). Controls and Assurance in the Cloud: Using COBIT 5. IT Audit and Assurance Program for Cloud Computing Using COBIT.

Jackson, A.P. (2017). *Legal Concerns Arising from The Use of Cloud Technologies* (Doctoral Dissertation). Pretoria: University of Pretoria

Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing. *International Journal of Grid and Distributed Computing,* 9 (1):49-56. 10.14257/ijgdc.2016.9.1.05.

Jamal, I.M. (2019). *Security Issues in Cloud Computing and Security Standards of the Cloud: A Review.* Turkey: Ondokuz Mayis Universitesi.

Johnson, J.L., Adkins, D. & Chauvin, S. (2020). A Review of the Quality Indicators of Rigor in Qualitative Research. *American Journal of Pharmaceutical Education:* 84(1) 7120

Jones, S., Irani, Z., Sivarajah, U. and Love, P.E.D. (2017). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. Information Systems Frontiers 21(2): 359–382. DOI 10.1007/s10796-017-9756-0.

Kalaiprasath, R., Elankavi, E. and Udayakumar, R. (2017). Cloud Security and Compliance- A Semantic Approach in End to End Security. *International Journal of Mechanical Engineering and Technology,* 8(5): 987-994. Available at: http://www.iaeme.com/IJMET/issues.asp?JType=IJMETandVType=8andIType=5.

Karajeh, H., Maqableh, M. and Masa'deh, R. (2016). *Privacy and Security Issues of Cloud Computing Environment.* Jordan: University of Jordan.

Ketwich, Van, W. (2012). *IT Governance of Cloud Computing: Performance Measures using an IT Outsourcing Perspective.* Melbourne School of Engineering Department of Computing and Information Systems. Melbourne: The University of Melbourne.

Khan, N. and Al-Yasiri, A. (2016). Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. *The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies*, 94: 485-490.

Khan, S.R. and Gouveia, L.B. (2018). Cloud Computing Service Level Agreement Issues and Challenges: A Bibliographic Review. *International Journal of Cyber Security and Digital Forensics,* 7(3): 209-229.

Khan, S.R. and Gouvia, L.B. (2017). The Implication and Challenges of GDPR's on Cloud Computing Industry. *International Journal of Computer Science*, 5(7): 106-112. Available from: http://www.ipasj.org/IIJCS?IIJCS.htm.

Kumar, D., Tyagi, K.A. and Nayeem, S. (2018). Handling of Incident, Challenges, Risks, Vulnerability and Implementing Detection Approaches Inside the Cloud. *International Journal of Computer Technology and Electronics Engineering,* 2(2): 136-146.

Kumar, P.R, Raj, P.H. and Jelcianac, P. (2017). *Exploring Data Security Issues and Solutions in Cloud Computing. 6th International Conference on Smart Computing and Communications, Kurukshetra, India.*

Kurniawan, E. and Riadi, I. (2018). Security Level Analysis of Academic Information Systems Based on Standard ISO 27002:2003 Using SSE-CMM. *International Journal of Computer Science and Information Security.* Available from: https://www.researchgate.net/publication/323029044.

Kusumawardhani, D. and Masyithah, D.C. (2017). Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. *Record and Library Journal,* 4(2): 2442-5168.

Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks*, 3(5): 247-255.

Langos, S. (2014). *Athens as an international tourism destination: An empirical investigation to the city's imagery and role of local DMO's.* Available from: https://www.researchgate.net/publication/270956555.

Ling Lin, K. (2019). Research Design and Methods. *Perspectives on the Introductory Phase of Empirical Research Articles:* 101-138

MacDonald, J. (2017). *Cloud Computing Framework for a Mid-Sized Financial Institution.* (Masters Dissertation). Minnesota: The College of St. Scholastica.

Madi, T. (2018). *Security Auditing and Multi-Tenancy Threat Evaluation in Public Cloud Infrastructures* (Doctor of Philosophy). Quebec: University Montreal. Available from: https://spectrum.library.concordia.ca/985048/.

Maduka, A.J., Aghili, S. and Butakov, S. (2017). A Proposed Assurance Model to Assess Security and Privacy Risks in IaaS and PaaS Environments. 12th Annual Symposium on Information Assurance (ASIA'17), Albany, USA.

Majid, U. (2018). Research Fundamentals: Study Design, Population and Sample Size. *Science and Technology Journal*, 2(1): 1-7.

Mamaile, L.J. (2018). *Developing of a Framework to Evaluate the Internal Audit Functions at Municipalities in South Africa* (Doctoral dissertation). North-West: North-West University.

Manivannan, T.I.D and Zeadally, S. (2016). A Classification and Characterization of Security Threats in Cloud Computing. *International Journal of Next-Generation Computing,* 7(1), 1-17. Available from: https://www.researchgate.net/publication/30817231.

Michalsons, (2020). POPI Commencement Date or POPI Effective Date starts the Clock. Available from: https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109.

Mitchell, B. (2017). *Introduction to Information Technology (IT).* Available from: https://www.lifewire.com.

Mohammad, R.M, Amir, M.R. and Mehdi, H. (2018). Reliability and High Availability in Cloud Computing Environments: A Reference Roadmap. *Human-centric Computing and Information Science,* 8 (20): 1-31.

Mohlameane, M. and Ruxwana, N. (2016). *The Impact of Existing South African ICT Policies and Regulatory Laws on Cloud Computing: A Literature Review Networks. Fifth International Conference on Advanced Information Technologies and Applications.* Available from: 10.5121/csit.2016.61302.

Morrow, T. (2019). Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud. Available at: http://www.sei.cmu.edu.

Morsy, M.A., Grundy, J. and Müller, I. (2016). *An Analysis of the Cloud Computing Security Problem.* University of Technology, Hawthorn, Victoria, Australia.

Motii, M. and Semma, E. (2017). Towards a New Approach to Pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for Better Use of ITG in the Morrocan Parliament. *International Journal of Computer Science Issues,* 14: 1694-0784. Available from: https://doi.org/10.20943/01201703.4958

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N. and Kumar, V. (2017). Security and Privacy in Fog Computing: Challenges*, IEEE Access*, 5:19293-19304. Doi 10.1109/ACCESS.2017.2749422.

Mukherjee, S. (2019). Information Governance for the Implementation of Cloud Computing. Available from: http://dx.doi.org/10.2139/ssrn.3405102.

Mutune, G. (2020). 23 Top Cybersecurity Frameworks. Available from: https://cyberexperts.com/cybersecurity-Frameworks/.

Nasseri, H.Al. and Duncan, I. (2016). Investigation of Virtual Network Isolation Security in Cloud Computing: Data Leakage Issues. Available from: https://core.ac.uk/display/41979750?source=2.

National Institute of Standards Technology (NIST). (2017). *Framework for Improving Critical Infrastructure Cybersecurity.* Maryland: NIST.

National Institute of Standards Technology (NIST) Special Publication 800-37, (2018). Risk Management Framework for Information Systems and Organisations. A System Life Cycle Approach for Security and Privacy. Available from: https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards Technology (NIST) Special Publication 800-53, (2020). Security and Privacy Controls for Information Systems and Organisations. Available from: https://doi.org/10.6028/NIST.SP.800-53r5-draft

Nyandongo, K.M. & Mxobo, N. (2018). Assessing the Effectiveness of an IT Governance Practices When Adopting Cloud Computing. *International Association for Management of Technology.*

Odun-Ayo, I., Mistra, S., Abayomi-Alli, O. and Ajayi, O. (2017). Cloud Multi-tenancy: Issues and Developments. Available from: https://core.ac.uk/display/154229956?source=2.

Omar, T. (2017). Protecting Sensitive Data in the IT Industry: A Review of Trends, Challenges and Mechanisms for Data-Protection. *International Journal of Advanced Computer Science and Applications,* 8(2): 46.

Onankunju, B.K. (2013). Access Control in Cloud Computing. *International Journal of Scientific and Research Publications,*3(9): 2250-3153.

Patil, M.B and Kulkarni, R.V. (2017). Role of DHCP Server in Network. *International Journal of Research in Advanced Engineering and Technology*, 3(2): 26-31.

Paquet, K.G. (2013). *Consumer Security Perceptions and the Perceived Influence on Adopting Cloud Computing: A Quantitative Study Using the Technology Acceptance Model* (Doctoral Dissertation). Minnesota: Capella University.

Rajasekar. S., Philominathan, P. and Chinnathambi, V. (2013). *Research methodology.* Available from: https://arxiv.org>pdf>physics.

Rama, P. (2016). *An evaluation of information technology security threats: A case study of the University of Johannesburg* (Limited Scope Dissertation). Auckland Park, Johannesburg: University of Johannesburg.

Ramachandra, G., Iftikar, M and Khan, F.A. (2017). A Comprehensive Survey on Security in Cloud Computing. *Procedia Computer Science*, 110:465-472.

Ramgovind, S., Eloff, M.M. and Smith, E. (2010). *The management of security in cloud computing.* Pretoria: Unisa

Rashid, A. and Chaturvedi, A. (2019). Cloud Computing Characteristics and Services: A Brief Review. *International Journal of Computer Sciences and Engineering,* 7(2019): 2347-2693.

Rebollo, O., Mellado, D., Fernandez-Medina, E. and Mouratidis, H. (2014). Empirical Evaluation of a Cloud Computing Information Security Governance Framework. *Information and Software Technology*, 58: 44-57.

Republic of South Africa Protection of Personal Information Act No.4. (2013). Government Gazette. (No. 37067).

Retselisitsoe, L. (2016). *SDN Based Security Solutions for Multi-tenancy NFV* (Masters Dissertation). Cape Town: University of Capetown. Available from: https://core.ac.uk/display/185407040?source=2.

Rizwana, S. and Sasikumar, M. (2015). Data Classification for Achieving Security in Cloud Computing. *Procedia Computer Science,* 45:493-498.

Samer, O. (2019). The Impact of the Application of IT Governance According to (COBIT 5) Framework in Reduce Cloud Computing Risks. *Modern Applied Science,* 13(2019): 1913-1852.

Satya, R.D., Alo, S., Pranab,K.B. and Bhabani, S.P.M. (2018). Frameworks to Develop SLA Based Security Metrics in Cloud Environment. Available from: https://link.springer.com/book/10.1007/978-3-319-73676-1.

Saunders, M. and Lewis, P. (2018). *Doing Research in Business and Management.* London: Pearson.

Schluga, O., Bauer, E., Bicaku, A. and Maksuti, S. (2018). *Operations Security Evaluation of IaaS-Cloud Backend for Industry 4.0. In Proceedings of the 8th Conference on Cloud Computing and Services Science:* 392-399.

Schneider, S. and Sunyaev, A. (2016). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*, 31: 1–3.

Sehgal, N.K., Bhatt, P.C. and Acken, J.M. (2019). Cloud Computing and Information Security [Abstract]. Available from: https://link.springer.com/book/10.1007/978-3-030-24612-9.

Setiyawan, D. (2019). A Proposed Model of IT Governance Within Cloud Computing and Data Management in Higher Education. *International Journal of Advanced Engineering Research and Science,* 6(10): 2349-6495.

Shaikha, R. and Sasikumarb, M. (2015). *Trust Model for Measuring Security Strength of Cloud Computing Service. International Conference on Advanced Computing Technologies and Applications. Procedia Computer Science,* 45:380 – 389.

Silva, H.C.C., Silveira, D.S., Dornelas, J.S. and Ferreira, H.S. (2019). Information Technology Governance in Small and Medium Enterprises- A Systematic Mapping.

Journal of Information Systems and Technology Management. Available from: https://doi.org/10.4301/s1807-1775202017001.

Simorjay, F. (2014). Data Classification for Cloud Readiness: Microsoft Trustworthy Computing. Available from: https://cloudsecurityalliance.org/research/ccm/.

Simpson, A. C. (2016). Whither the privacy breach case studies? Department of Computer Science, Oxford University.

Skolmen, D.D. and Gerber, M. (2015). Protection of Personal Information in the South African Cloud Computing Environment: A Framework for Cloud Computing Adoption. *Information Security for South Africa (ISSA),* 1-10. Doi: 10.1109/ISSA.2015.7335049

Slaheddine, M. (2012). *Cloud computing in Africa: situations and perspectives.* Location: Tunisia, Regulatory and Markets Environment Division.

Solms, R von. and Willet, M. (2016). *Cloud computing assurance- a review of literature guidance,* 25(1):26-46. Doi: 10.1108/ICS-09-2015-0037.

Soubra, M. and Tanriover, O. O. (2017). An Assessment of Recent Cloud Security Measure Proposals in Comparison to their Support by Widely Used Cloud Service. *Mugla Journal of Science and Technology,* 3(2017): 122-130.

Suess, J.M.W. (2019). *An Exploration of the Perception of COBIT Control Failures In the Protection of Personally Identifiable Information*. (Doctoral Dissertation). Maryland: Capitol Technology University.

Taherdoost, H. (2016). Sampling Methods in Research Methodology: How to Choose a Sampling Technique for Research. *SSRN Electronic Journal*, 2:18-27.

Tariq, M.I and Santarcangelo, V. (2016). *Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing. ICISSP- 2nd International Conference on Information Systems Security and Privacy*. Rome, Italy.

Tariq, M.I, Tayyaba, S., Ashraf, M.W., Rasheed, H. and Khan, F. (2016). *Analysis of NIST SP 800-53 Rev.3 Controls Effectiveness for Cloud Computing. 1st National Conference on Emerging Trends and Innovations in Computing and Technology*. Jamshoro, Sindh, Pakistan.

Tiwari, P. and Mehta, A. (2019). *SLA Penalty and Reward Strategy for Cloud Computing.* London: Taylor and Francis Group.

Tsou, M.H. and Lusher, D. (2015). Mapping Web Pages by Internet Protocol (IP) addresses: Analyzing Spatial and Temporal Characteristics of Web Search Engine Results. *The International Symposium on Cartography in Internet and Ubiquitous Environments.* Available from: https://pdfs.semanticscholar.org/0d4a/a2e3fd6c283a0ee03bd405a74dea11a0dce4.pdf.

Ukidve, A., Mantha, S.S. and Tadvalkar, M. (2019). Analysis of Payment Card Industry Data Security Standard [PCI DSS] Compliance by Confluence of COBIT 5 Framework. *Int. Journal of Engineering Research and Application,* 7(2017): 42-48.

Van Ketwich, W. (2012). *IT Governance of cloud computing: performance measures using IT outsourcing perspective* (Master's dissertation). Melbourne: University of Melbourne.

Vani, B. and Priya, R.C.M. (2015). Availability in Cloud Computing*. International Journal of Innovative Research in Information Security,* 2 (4): 11-15.

Velumadhava Rao,R. and Selvamanib, K (2015). *Data Security Challenges and Its Solutions in Cloud Computing. Proceedings of the Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India.*

Viswanathan. S., and Senguttuvan, P. (2017). A Study on Influence of Cloud Computing on Business Developments. *International Journal of Pure and Applied Mathematics,* 23(116): 533-538

Von Solms, R. & Viljoen, M. (2012). Cloud Computing Service Value: A Message to the Board. *South African Journal of Business Management,* 43(4):43-81

Vumo, A.P., Spillner, J. and Kopsell, S. (2019). A Data Security Framework for Cloud Computing Adoption: Mozambican Government Cloud Computing. European Conference on Cyber Warfare and Security; *Department of Computer Science, Germany.*

Wang, R. (2017). Research on Data Security Technology Based on Cloud Storage. *Procedia Engineering,* 174: 1340-1355.

Weintraub, E. & Cohen, Y. (2016). Security Risk Assessment of Cloud Computing Services in a Networked Environment. *International Journal of Advanced Computer Science and Applications,* 7(11).

Welz, D. (2016). *A Summary of "POPI" The Protection of Personal Information Act, Act No.4 of 2013.* Available from: www.miltons.law.za.

Wild, J. (2018). Five Most Common Security Frameworks Explained. Available from: https://originit.co.nz/the-strongroom/five-most-common-security-Frameworks-explained/.

Yimam, D. and Fernandez, E.B., (2016). A Survey of Compliance Issues in Cloud Computing. *Journal of Internet Services and Applications*, 7:5.

Zissis, D. and Lekkas, D. (2010). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(2012):583-592.