The impact of cloud computing security on business operations

by

Bongani H.S. Sikhosana

201149033

Minor dissertation

Submitted in the fulfilment of the requirements for the degree

Masters

in

Computer Auditing

in the

FACULTY OF ECONOMIC AND FINANCIAL SCIENCES

at the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: Mrs Vanessa van Dyk

May 2015

Abstract

Cloud computing is a novel platform which affords users the opportunity to exploit the best that Information Technology (IT) infrastructure, platforms and software offer at a fraction of the cost to acquire such resources. Cloud computing has three delivery models, firstly, Infrastructure as a Service, secondly, Platform as a Service, and lastly, Software as a Service. Furthermore, cloud computing has four basic deployment models, namely, public, private, community and hybrid clouds. With all the opportunities presented by cloud computing as a business process, there are nonetheless potential risks associated with the process, especially in the area of security. The aim of this paper is to determine whether or not it is secure for businesses to utilise the services of cloud computing as part of their daily operations to meet the needs of their customers and to ultimately achieve their business objectives. Evidence was gathered through a detailed content analysis of existing research on the subject of cloud computing and cloud security. The paper concludes that with adequate security controls in place, cloud computing is a secure and efficient platform for businesses to utilise for their daily operations.

Keywords:

Cloud computing, cloud security, cloud user, cloud service provider.

Acknowledgement

I would first like to thank God for giving me the strength and perseverance to soldier on when I felt it was time to throw in the towel.

Secondly, I would like to thank my mom. Thanks for believing in me and being my pillar of strength. Your faith spoke to something deep in me and kept me going when times were tough. A wise man once said: “God answers all prayers, even those from unfamiliar voices”; thanks for your prayers, they did not fall on deaf ears.

My dad asked me: “What would it take to finish your research project?” I did not have a clear answer as to why I was not working on it. That was a little bit of a push, I realised I have all it takes to finish it. From then I started putting hours working on it; thank you.

To my brothers and sisters, thanks for looking up to me for it makes me want to become a better person so all of you can be better than me.

To Vanessa, thank you for your guidance throughout this journey. It wasn’t easy, yet you were patient with me.

Thanks to Veronica, you were always there for me and told me I could do it. To Mandla Spikiri, thank you for your understanding. Ndamu, thanks for sharing the journey with me, you were my third eye when I missed something in class.

Thanks to Justin, I now know “what happens to the cloud when it rains”.

Contents

Chapter 1: Introduction

1.1. Introduction

As times are changing and technology advances, the manner in which businesses strive to meet the needs of their customers also changes (Hugos & Hulitzky, 2010: 155). Keeping up with progress and development in the information age has been a defining factor in the success or failure of many organisations (Hugos & Hulitzky, 2010: 166). According to Hwang, Fox and Dongarra (2012: 4), from 1950 to 1970, mainframes, IBM 360 and CDC 6400 were built to satisfy the demands of large businesses and government organisations. This implies that the core activities of a business should not follow technology; technology should follow core business activities and be seen as an enabler in meeting the needs of customers and business objectives. This is supported by Hugos and Hulitzky (2010: 101) who state that "Business processes powered by technology generate revenue and profits".

Businesses relying on IT to serve the needs of their customers must ensure that the best systems are utilised to remain relevant or to have an edge over their competitors (Hurwitz, Bloor, Kaufman & Halper, 2009: 7). Utilising the latest technology can be expensive or, at times, impossible. In such instances, businesses may consider the use of cloud computing as an alternative to a traditional in-house IT function.

Cloud computing gives businesses access to IT infrastructure that may include components such as database, application or any computer resource that may be useful for daily operations (Miller, 2009: 9). This can reduce expenses associated with sourcing and using the latest systems through an in-house IT department. Cloud computing is a way of deploying IT to enable users to work on, store and share information through the internet anywhere in the world (Wang, Ranjan, Chen & Benatallah, 2012: 3). Cloud computing allows businesses to focus resources on their core activities and thus maximise profits for shareholders and meet other business objectives (Hugos & Hulitzky, 2010: 159).

Cloud computing presents security threats as much as a traditional in-house IT function (Speed, 2011; Hausman, Cook & Sampaio, 2013: 177). Therefore, cloud computing should not be seen as a simple transferral of risks associated with operating one's own IT function over to cloud service providers, since new security and privacy concerns may arise (Marinescu, 2013: 274). Cloud computing should be seen as a strategy for minimising investment in IT infrastructure and allowing an organisation to focus on its core activities (Chee & Franklin Jr, 2010: 92; Speed, 2011: 17).

A medical aid company or a bank, for example, which is considering the use of cloud computing services, will need to consider security measures to ensure the confidentiality and integrity of the records of their clients. A thorough risk assessment exercise is critical before making a final decision to utilise cloud computing. As per research conducted by analyst firm Gartner, there are certain security issues that cloud customers need to assess (Kaur & Kaushal, 2011: 4–5). "Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor" (Brodkin, 2008: 2).

1.2. Background of the study

Cloud computing is not a new concept in the IT environment as its roots can be traced back forty years (Winkler, 2011: 10). It is a concept that has evolved over time and has recently gained momentum as it is now more widely used than it was in the past. According to Wang *et al.* (2012: 5), "the first generation of cloud computing which evolved along with the 'Internet Era' was mainly intended for e-business. The current generation of cloud service has now progressed several steps to include IT as a service which can be thought of as a 'consumerized internet service".

With development, progress and innovation in technology, there are new risks that emerge. Such risks need to be explored and controls developed and implemented to minimise such risks (Hausman, Cook & Sampaio, 2013: 177–178). Along with the

benefits presented by cloud computing, one of these being investment in first class infrastructure by cloud service providers, there are also security risks linked to the cloud environment which need to be considered. Some of these risks may stem from legal compliance with the laws governing the geographic areas in which organisations operate (Winkler, 2011: 74).

This study explores the risks pertaining to the use of cloud computing as part of business operations and determines the saftey of such services in meeting the needs of customers and, as a result, those of the business.

1.3. Research problem, questions and objectives

1.3.1. Research problem

Although there are numerous benefits derived from cloud computing, cloud users face numerous risks that should be maintained at an acceptable level to maintain confidentiality, integrity and availability of data for daily business operations (McDonald, 2010: 43). Although risks associated with an in-house IT function are not transferred to the cloud service provider, there are nonetheless security risks which may arise from cloud computing in daily business operations (Chee & Franklin Jr, 2010: 167). It is important for cloud customers to conduct a thorough risk assessment to ensure that the cloud will meet their security requirements.

1.3.2. Research questions

The purpose of this study is to determine how safe it is for businesses to utilise the services of cloud computing in their daily operations in order to meet the needs of their customers, and ultimately, to achieve their business objectives. This was determined by answering the following research questions:

- What security risks are presented or intensified by the use of cloud computing for businesses?
- Can the safety and security of the cloud computing environment be independently evaluated to provide acceptable levels of assurance to organisations utilising cloud computing services?
- How safe is the use of cloud computing in the daily operation of businesses?

1.3.3. Research objectives

The evidence gathered in this study made it possible to answer the research questions stated in Section 1.3.2 above and to meet the following research objectives:

- Determine the security risks prevalent in the cloud computing environment;
- Determine the possibility of independent evaluation of the cloud environment to provide assurance on its security; and
- Establish whether it is safe for organisations to use the services of cloud computing providers in their daily operations in order to meet the needs of their customers.

1.4. Research methodology

A literature review on the security of cloud computing was performed. The review was conducted to understand the nature of cloud computing and current security issues and to determine security measures to minimise or mitigate those security risks.

Section 1.5 below examines the approach adopted to answer the research questions in order to meet the objectives. The time horizon, data collection and analysis methods as well as the manner in which ethics were dealt with in conducting the research were covered as part of this chapter. The interpretation and presentation of findings was also considered.

The research methodology in this study was a content analysis of secondary data in the field of cloud computing, and more specifically, cloud computing security. Secondary data is defined as data which has already been collected by others (Battacharyya, 2006: 52). Qualitative techniques for data collection and analysis were employed. A qualitative technique "is used predominantly as a synonym for any data collection technique (such as an interview) or data analysis procedures that generate or use non-numerical data" (Newman & Benz, 1998: 9; Saunders, Lewis & Thornhill, 2009: 151). In answering the research questions and meeting the research objectives, non-numerical and slight numerical data were used to analyse the current state of security in the cloud environment.

1.5. Research approach

A content analysis of literature between 2006 and 2015 was conducted to determine how secure it is for businesses to use cloud computing in their daily operations to meet the needs of customers, and ultimately, to achieve their business objectives.

Literature was reviewed, analysed and split into Chapter 2 and Chapter 3, as described in Sections 1.10.2 and 1.10.3. The first two research questions and objectives were answered in Chapter 3. Chapter 4 outlines conclusions on the last research question and objective.

1.6. Time horizon

Research can be conducted over a period of time or at a particular point in time (Kothari, 2004: 4; Sachdeva, 2009: 12). When conducted over a period of time, it is known as longitudinal. When conducted at a particular point in time, it is known as cross-sectional (Saunders, Lewis & Thornhill, 2009: 155).

Given the rapid changes within the IT environment, this study was conducted at a particular point in time (based on literature collected between 2006 and 2015) to eliminate the risks presented by time. This approach was appropriate given the time constraints in which this research project had to be conducted.

1.7. Ethics of the research design

The work of others was not subjected to misuse and credit was given where it was due through the use of an acceptable referencing style. Permission was obtained, ethically, wherever the need arose to request such permission in the process of conducting the research.

1.8. Methods of data collection and analysis

According to Saunders, Lewis and Thornhill (2009: 151), there are different research methods that can be used when conducting research. These are dependent on factors such as the underlying research assumptions, the purpose of the study, the research strategy to be adopted, resources required as well as the time horizon of the research.

In addition to the content analysis of literature, this research project was also a combination of an exploratory and a descriptive study. An exploratory study is an evaluation which seeks new insights, which asks questions and assesses a subject in a new light (Sachdeva, 2009: 14). Exploring can be seen as an engine of discovery and is

important when one wishes to obtain an understanding of a problem (Kothari, 2004: 4). A descriptive study, on the other hand, aims to portray an accurate profile of a person, event or situation (Battacharyya, 2006: 14).

The exploratory part of this study was used to determine how safe it is for businesses to use cloud computing in their daily operations in order to meet the needs of customers, and ultimately, to achieve their business objectives. According to Saunders, Lewis and Thornhill (2009: 140) and Sachdeva (2009: 14), there are three principal ways to conduct exploratory research: through a search of literature, by interviewing subject matter experts or by conducting focus group interviews. This study explored literature and content analysis of the existing body of knowledge (secondary data) in considering the research problem.

1.9. Interpretation and presentation of findings

Based on the content analysis of the literature, the impact of cloud computing on the security of business operations is discussed in Chapter 3 in an attempt to answer the research questions and research objectives mentioned in Sections 1.3.2 and 1.3.3 above.

1.10. Outline of chapters

Outlined below is a list of chapters and information covered in each chapter.

1.10.1. Chapter 1: Introduction

This chapter introduces the background of the study and the research problem, i.e. the safety of cloud computing when utilised by businesses in carrying out their daily operations to meet the needs of customers. The research problem is further broken

down into research questions and research objectives. The research methodology and approach are also covered in this chapter.

1.10.2. Chapter 2: Cloud computing definition, explanation and understanding of this concept

This chapter focuses on the body of knowledge that already exists in the field of cloud computing and safety and security measures. The following is covered:

- Nature of cloud computing and its definition;
- Characteristics of cloud computing;
- Delivery and deployment models of cloud computing;
- Benefits and disadvantages of using cloud computing; and
- Compliance and regulations on data privacy versus security on the cloud.

1.10.3. Chapter 3: The impact of cloud computing on the security of business operations

This chapter examines the impact of cloud computing on the security of business operations. Literature is reviewed and analysed according to the research methods explained in Section 1.8 in order to determine whether cloud computing is a secure platform for business operations. The following is covered in Chapter 3:

- Security responsibility;
- Risk assessment prior to migrating to the cloud environment;
- Security standards governing/applicable to the cloud;
- Security issues unique or prevalent in the cloud environment;
- Control measures that can be employed to mitigate security issues;
- Independent evaluation of cloud computing security; and
- Past security incidents related to cloud computing.

1.10.4. Chapter 4: Conclusion

The conclusion of the research project is discussed in this chapter. A summary of the research is provided to establish whether cloud computing is a safe platform in conducting business or not.

1.11. Conclusion

As times are changing, businesses are adopting new ways of serving the needs of their customers at minimum cost while maximising profits and meeting their business objectives. Alongside the benefits that can be derived from cloud computing services, there are also associated risks which need to be taken into consideration. This may involve conducting an assessment and implementing mitigating strategies to reduce such risks.

Chapter 2: Cloud computing definition, explanation and understanding of this concept

2.1. Introduction to the literature review

IT managers need to ensure that users relying on IT to serve the needs of customers have the necessary tools and hardware to perform their work to satisfactory levels. This involves regular updates of computer resources for existing users and the installation of adequate tools for new users. It also means ensuring that users have the required tools and that licenses are valid. In modern times where high reliance is placed on IT for survival, it can be expensive to keep up with new systems and technological advancements. Expenses linked to IT could affect the profitability of a business given that investments in IT resources may be required on a daily basis to ensure optimal performance (Chee & Franklin Jr, 2010: 92; Marks & Lozano, 2010: 72). Taking these factors into account, many businesses are left with no option but to consider alternatives such as cloud computing because of its cost and flexibility (Wang, Qu & Sheng, 2013: 350).

The purpose of this study is to determine how secure it is for businesses to utilise the services of cloud computing in their daily operations to meet the needs of customers, and ultimately, to achieve their business objectives. The purpose of this study is all the more relevant given that the slow adoption of the cloud by businesses is driven by fears of inadequate security (Wang *et al*., 2012: 42; Raj, 2013: 357).

In this chapter, the existing body of knowledge on the subject of cloud computing security is reviewed in detail. Chapter 3 will focus on the impact of cloud computing on the security of business operations based on observations made in the literature review. Topics covered as part of the literature review in this chapter include:

- Definition of cloud computing;
- Characteristics of cloud computing;
- Delivery and deployment models;

- Benefits and disadvantages of cloud computing; and
- Compliance and regulations.

In the section below, the concept of cloud computing is explored in detail. Various definitions of cloud computing from different sources are considered and documented.

2.2. Definition of cloud computing

Cloud computing can be defined as "an IT model or computing environment composed of IT components (hardware, software, networking and services) as well as the processes around the deployment of these elements that together enable us to develop and deliver cloud services via the internet or private network" (Winkler, 2011: 2).

Furthermore, cloud computing is defined in the book Cloud Computing for Dummies as "a set of hardware, network storage, services and interfaces that enable the delivery of computing as a service" (Hurwitz *et al*., 2009: 7).

According to the ISACA Journal, Cloud Computing: An Auditor's Perspective (2009: 11), "cloud computing is performing computing tasks via a network connection while remaining isolated from the complex computing hardware and networking infrastructure that supports it. Cloud computing relies on virtualization technology to offer each subscriber one or more individual virtual instances".

Above the Clouds: A Berkeley View of Cloud Computing states that cloud computing includes application software delivered as services over the internet and the hardware and systems software in the datacentres that facilitate these services (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica & Zaharia, 2009: 4).

According to the National Institute of Standards and Technology (NIST) (2014) , cloud computing is a model which enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing has multiple definitions due to the fact that it can be used in various application scenarios (Qian, Luo, Du & Guo, 2009: 626). It is important to note that currently, there is no single cloud computing definition that is used universally. There are different definitions which are representations of various industries and academia (Li, Tian, Wei, & Sun, 2012: 1).

An example of the concept of cloud computing is provided by Google, Amazon and Microsoft. Google cloud consists of large servers that can be accessed by the public through personal computers. Although Google cloud is private as is owned by Google, it is accessible to Google users and the public at large (Bai & Policarpio, 2011: 389). Amazon (Amazon Simple Storage and Amazon Compute Cloud) provides cloud services to cloud customers through Virtual Machines (VMs), extra Central Processing Unit (CPU) cycles and storage services (Bai & Policarpio, 2011: 389; Carlin & Curran, 2011: 14). Microsoft provides cloud services in the form of Windows applications, datacentres and database services (Bai & Policarpio, 2011: 389).

Another example of cloud computing is the transferring of large files using services such as those provided by Dropbox (Munyaka, Noviansyah, Goel, Yenchik & Durham, 2012: 15–16). This service is also open to the public where large files can be stored on virtual storage and accessed or shared with other users anywhere in the world (Chee & Franklin Jr, 2010: 18).

However, storing files on virtual storage and sharing them with others can present security risks. This raises questions relating to the safety of cloud computing and what

security measures can be applied to mitigate such risks or reduce them to an acceptable level.

Currently, many companies considering cloud computing are running test cloud projects for straightforward IT services. According to ISACA, Cloud Computing as an Integral Part of a Modern IT Strategy (2012: 1), these projects indicate that there are challenges in the area of data security and compliance.

Cloud computing has evolved gradually over time, beginning in 1960 when John McCarthy stated that “computation may someday be organized as a public utility” (Wang *et al*., 2012: 5). According to Armbrust *et al*., (2009: 2), “Cloud Computing is a new term for a long-held dream of computing as a utility, which has recently emerged as a commercial reality”. Previous research on virtualisation, utility computing and grid computing suggests that the concept of cloud computing is not new *per se*; however, there are distinctive characteristics which separate cloud computing from virtualisation, utility computing and grid computing (Gong, Liu, Zhang, Chen & Gong, 2010: 279). These characteristics of cloud computing are examined in Section 2.3 below.

2.3. Characteristics of cloud computing

According to NIST, there are five characteristics that define the nature of cloud computing. These characteristics are listed below.

2.3.1. On-demand self-service

Cloud users can order cloud services without face-to-face interaction with cloud providers (Sabharwal & Wali, 2013: 2; Rountree & Castrillo, 2014: 3). They can order a service which adequately meets their needs through web portals and management interfaces (Chen, Paxson & Katz, 2010: 4; Grobauer, Walloschek & Stöcker, 2011: 52).

2.3.2. Broad network access

Cloud computing is accessed via a network, commonly through the internet, utilising standard mechanisms and protocols (Grobauer, Walloschek & Stöcker, 2011: 52).

2.3.3. Resource pooling

Cloud services are provided to cloud customers using a homogeneous infrastructure shared by users (Chen, Paxson & Katz, 2010: 4; Grobauer, Walloschek & Stöcker, 2011: 52). Resource pooling is achieved using virtualisation (Rountree & Castrillo, 2014: 5). It allows the cloud service provider to invest in the best technology and provide concentrated expertise in areas such as security (Sabharwal & Wali, 2013: 3). This is often referred to as economies of scale (Hurwitz *et al*., 2009: 11; Rountree & Castrillo, 2014: 12–13).

2.3.4. Rapid elasticity

Based on their needs at any point in time, cloud customers may increase or decrease the cloud services they require (Chen, Paxson & Katz, 2010: 4; Grobauer, Walloschek & Stöcker, 2011: 52). This is important in instances (often over years after building IT infrastructure) where greater system resources are required as the business grows. To meet the needs of increased system performance, cloud users may scale up the services received from providers (Sabharwal & Wali, 2013: 3; Rountree & Castrillo, 2014: 5).

2.3.5. Measured service

Linked to rapid elasticity, cloud services can be measured, thus allowing cloud users to determine whether services obtained are being used optimally or if there is a need to scale down. This also supports the pay-as-you-go business model for cloud users (Chen, Paxson & Katz, 2010: 4; Grobauer, Walloschek & Stöcker, 2011: 52).

Section 2.4 below provides a detailed discussion of the various delivery models of cloud computing services.

2.4. Delivery models

There are three delivery models within cloud computing (Hwang, Fox & Dongarra, 2012: 200). These models are:

- Infrastructure as a Service;
- Platform as a Service; and
- Software as a Service.

2.4.1. Infrastructure as a Service (IaaS)

In IaaS, the cloud service provider supplies cloud users with virtualised infrastructure and storage to enable the running and development of applications (Takabi, Joshi & Ahn, 2010: 25). The cloud user is provided with services such as hardware, datacentre space, network and storage (Smooth & Tan, 2013: 10). The cloud user does not control or manage the functionality of the infrastructure obtained from the cloud provider (Hurwitz *et al*., 2009: 21). This service allows businesses to use the latest technology without up-front investment in such technology (Sabharwal & Wali, 2013: 5). Users also utilise services according to their needs.

2.4.2. Platform as a Service (PaaS)

In PaaS, the cloud provider supplies the platform or programming environment that can be used to develop applications and services over the internet (Bai & Policarpio, 2011: 390; Smooth & Tan, 2013: 10). Cloud users can build any application to meet their needs in this environment. Well-known PaaS providers include Google and Microsoft Azure (Kaur & Kaushal, 2011: 106). According to NIST (2009: 22), "PaaS is the ability to provide a computing environment and the related development and deployment stack needed to deliver a solution to the consuming customer".

2.4.3. Software as a Service (SaaS)

In SaaS, the cloud provider supplies applications that may be useful to cloud users (Hwang, Fox & Dongarra, 2012: 205). These services are provided on-demand to customers (Takabi, Joshi & Ahn, 2010: 25). In SaaS, cloud customers do not need to make significant up-front investments in servers and software licences. The costs for cloud providers are considerably lower as they provide and maintain a single application to multiple users (Kaur & Kaushal, 2011: 105). Examples of SaaS include Google docs and the Microsoft online version of Office known as BPOS (Business Productivity Online Standard Suite) (Kaur & Kaushal, 2011: 105) or the latest version, Office 365.

Each of the delivery models can be deployed for cloud users based on four deployment models (Winkler, 2011: 40) which are examined in Section 2.5 below.

2.5. Deployment models

In the cloud environment there are four deployment models. These include public, private, community and hybrid cloud (Zissis & Lekkas, 2012: 584). These deployment models are explained in the following sections.

2.5.1. Public cloud

In public cloud, the provider can supply services from anywhere in the world to any cloud user (Sabharwal & Wali, 2013: 6). Cloud users have no control over the location of the computer infrastructure (Kaur & Kaushal, 2011: 105).

2.5.2. Private cloud

Private cloud is usually dedicated to one organisation (Sabharwal & Wali, 2013: 6). There are no other parties that share the service except those from the given organisation (or from different business units of the same organisation). It can be set up and managed by the organisation itself or by a third party (Ruhse, 2012: 6). It may exist on or off the premises of the business (Mell & Grance, 2011: 3).

2.5.3. Community cloud

This cloud service is shared by cloud users with communal concerns (Sabharwal & Wali, 2013: 6). It can be managed by the community of organisations or by a third party service provider. It may be hosted on the premises of one of the organisations or from an off-site location (Zissis & Lekkas, 2012: 584).

2.5.4. Hybrid cloud

Hybrid cloud is composed of two or more deployment models (private, public and community). Infrastructure in a hybrid cloud remains unique entities linked by standardised technology that enables data and application portability (Mell & Grance, 2011: 3).

With all the benefits presented by cloud computing, the purpose of this study is to examine security measures within the cloud environment to determine the safety of

cloud computing in the daily operations of businesses. The advantages and disadvantages of cloud computing are discussed in the section below.

2.6. Benefits of cloud computing

As much as there are numerous concerns surrounding cloud computing, specifically in relation to security, there are also many benefits that can be derived from the use of cloud computing. Firstly, users are not tied to a single workstation as they can use any computer anywhere in the world to conduct their daily activities (Miller, 2009: 27). For example, any user can access Gmail from anywhere in the world to retrieve e-mails or Google drive to retrieve documents.

Secondly, cloud computing allows collaborations between a group of people who might be working on the same project yet located in various parts of the world (Liu, 2012: 1216). Users working on the same document may use Dropbox for collaboration. This improves productivity, saves time and increases profitability for businesses.

The third benefit of cloud computing is that it allows organisations to focus on their core business while using the latest first class technology to conduct business and serve the needs of their customers (Miller, 2009: 27; Carlin & Curran, 2011: 18). It provides organisations with technology that might otherwise not have been affordable to them (Kaufman, 2009: 2). In addition, cloud computing keeps software and servers up to date (Carlin & Curran, 2011: 18).

The fourth benefit of cloud computing is its scalability (Wang *et al*., 2012: 4). Should more resources be required to handle increased load, more hardware can be added to improve system performance and capacity (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011: 2; Liu, 2012: 1216). Should the cloud user require less performance than previously required, services may be scaled down. Cloud services are thus provided as needed by the cloud user. Users are also allowed increased storage according to their needs (Carlin & Curran, 2011: 18).

Lastly, cloud computing is cost-effective and allows flexibility in infrastructure (Winkler, 2011: 24; Wang *et al*., 2012: 4). If a customer is not satisfied with the technology, service or cost of one cloud provider, it is a simple process to switch to another provider (Carlin & Curran, 2011: 18; Ruhse, 2012: 6). It is cost-effective because it allows organisations to focus on their returns and investments in other parts of the business while receiving the same level of IT support at a fraction of the cost when compared to operating an in-house IT function (Kaufman, 2009: 2). Cloud computing also allows small businesses to have access to IT infrastructure that would, under normal circumstances, only be available to large corporations (Marston *et al*., 2011: 2).

As much as there are benefits that can be derived from the use of cloud services, it is important to note that the cloud environment also presents some disadvantages. One of the main disadvantages is related to the security of cloud services in supporting critical processes within organisations. Section 2.7 below provides an overview of the disadvantages that may arise from the use of cloud computing services.

2.7. Disadvantages of cloud computing

Firstly, cloud computing requires constant internet connection to access services. In an area that lacks constant and high-speed internet connections, utilising cloud services may result in downtime for business operations (Miller, 2009: 29; Carlin & Curran, 2011: 18).

Cloud computing also requires adequate speed in order to work effectively. There is back and forth communication between the cloud provider and the cloud user in accessing data and applications on the cloud. A slow connection can have a severe impact on a business that requires accelerated service delivery through technology to its customers (Carlin & Curran, 2011: 18).

Data is the lifeline of many businesses and needs to be protected from loss or leakages to maintain confidentiality and integrity (Miller, 2009: 29). Multiple cloud users can utilise the same piece of hardware, but a compromise in one user's application could affect the applications of other users on the same hardware, thereby also compromising their data (Grossman, 2009: 25). This leads to concerns about the security of cloud computing.

Lastly, making data accessible to cloud providers (or other third parties) may present issues related to security, compliance and regulations on privacy (Grossman, 2009: 25). Cloud users, to some extent, lose full control of data kept in the cloud environment (Carlin & Curran, 2011: 15). Most of the time, cloud users will be unaware of the location of data (Robinson, Valeri & Cave, 2011: 27). The issue of compliance and regulations on data privacy is discussed in detail in Section 2.8 below.

2.8. Compliance and regulations on data privacy versus security on the cloud

Different countries have different laws related to the privacy of personal information (Winkler, 2011: 75). Entities that process personal information are required to ensure compliance with these laws, even when the data is held by third parties (Heiser & Nicolett, 2008: 3). However, the use of cloud computing in conducting a business may present compliance challenges (Krutz, Vines & Brunette, 2010: 130 – 131). The main challenge is the privacy of the data stored in the cloud. With an in-house IT function, businesses usually have a well-established compliance monitoring process. However, this is not always the case in the cloud environment (Takabi, Joshi & Ahn, 2010: 26). In a traditional IT function, businesses are subject to external audits and security audits which may not be the case for cloud service providers unless this is stipulated as part of a legal agreement (Kaur & Kaushal, 2011: 106).

Another challenge with regulatory compliance in the cloud is data location (Robinson, Valeri & Cave, 2011: 27). In most cases, cloud users will be unaware of where their data is located (Brodkin, 2008: 2). The nature of cloud computing and one of its advantages is that it allows users to access their information from anywhere in the

world, provided there is an internet connection. This implies that data can be located anywhere in the world (Chee & Franklin Jr, 2010: 18). This can present issues related to jurisdictions (Heiser & Nicolett, 2008: 3), especially in a country with laws to enforce privacy of personal information. Should a local company, operating in a country with laws on processing personal information, utilise cloud services which keep data in a foreign country with no laws on personal information, any violation of local laws in which the company operates may be difficult to prosecute and impose penalties due to jurisdiction restrictions (Rountree & Castrillo, 2014: 15).

In South Africa, a Protection of Personal Information Act was passed in November 2013 which safeguards the right to privacy of every person (data subject), in accordance with the South African Constitution, when processing personal information. It also regulates the manner in which information is processed, in harmony with international standards.

Any institution that has operations within South African borders and deals with personal information of a data subject protected by this Act needs to ensure compliance. Failure to comply may lead to heavy penalties imposed on the responsible party (Protection of Personal Information Act 4 of 2013, 2013: 96).

Businesses considering the use of cloud computing services will need to take all issues related to compliance with domestic laws into account when appointing a cloud service provider (Winkler, 2011: 75; Pearson & Yee, 2013: 249). For issues such as data location, there must be an explicit Service Level Agreement (SLA) or contractual clause regarding the location of the data (Raj, 2013: 382).

In summary, this chapter covered the definition and characteristics of cloud computing in order to understand the nature of this environment. Furthermore, the different delivery and deployment models of cloud computing were discussed. The chapter concluded by examining the advantages and disadvantages of cloud computing as well as issues related to compliance and regulations.

2.9. Conclusion

Based on the above analysis of existing literature, it is evident that there is extensive coverage of cloud computing concepts. Various research documents seem to concur on the common characteristics, as defined by NIST. The characteristics of the cloud environment include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services.

Furthermore, it was noted that there are currently three delivery models within the cloud environment. These delivery models include IaaS, PaaS and SaaS. Depending on the delivery model selected by the cloud customer, the level of security for each will vary. Cloud computing has four deployment models which include public, private, community and hybrid.

Businesses considering the use of cloud services should take into account compliance implications of utilising cloud computing. Laws such as the Protection of Personal Information Act in South Africa determine how personal information should be processed and stored. Businesses should ensure compliance when operating in a country with strict provisions on the processing of personal information. Heavy penalties can be imposed on businesses for non-compliance.

Overall, like any other IT environment, cloud computing has security issues although these can be addressed through security measures implemented over time. There are many benefits to be derived from utilising cloud computing services and there appears to be room for growth in this environment.

Chapter 3: The impact of cloud computing on the security of business operations

3.1. Introduction

The main objective of this study is to perform a content analysis to determine how safe it is for businesses to utilise the services of cloud computing in their daily operations to meet the needs of their customers, and ultimately, to achieve their business objectives. Chapter 3 answers the first two research questions as listed in Section 1.3.2. The third research question is answered in Chapter 4.

For businesses considering the use of cloud services, it is essential to define responsibilities related to security. This is discussed in detail in Section 3.2 below.

Furthermore, prior to using cloud services, it is important for organisations to perform a thorough risk assessment to determine whether the exposure that may result from security weaknesses in a cloud environment is within acceptable risk tolerance levels. This is discussed in detail in Section 3.3 below.

This study investigated standards dealing with security issues in a cloud environment and examined factors which can be used to determine whether a security issue is unique to cloud computing or common to any IT environment. Issues unique to the cloud environment are discussed in this chapter.

As with in-house IT functions, there are measures which can be implemented to minimise the impact of risk in a cloud environment. Such measures are evaluated in Sections 3.7 and 3.8 below. With so many threats associated with the cloud environment, an independent review or verification of security on the cloud may be conducted. Past incidents related to data loss by companies are also assessed in this chapter.

3.2. Responsibility for security in cloud computing

With all the benefits that can be derived from cloud computing, it should be noted that there are some responsibilities that can be carried out by cloud service providers, some that can be shared and some that can be carried out by the cloud customer (Hwang, Fox & Dongarra, 2012: 49). Security is one of the responsibilities that needs to be clearly defined in the SLA to mitigate or at least minimise any risks (Kandukuri, Reddy, Paturi & Rakshit, 2009: 518). According to Khan, Oriol, Kiran, Jiang and Djemame (2012: 121), the ultimate responsibility for data confidentiality, integrity and access controls still rests with the cloud user.

In the cloud environment, the responsibility for risks can be shared between the cloud service provider, the cloud user and a third party (in cases where a cloud user relies on such a party for security management) (Armbrust *et al*., 2010: 55). This is supported by Ramgovind, Eloff and Smith who state that security can be a shared responsibility for both cloud users and cloud service providers in enforcing security checks and validations across their systems (Ramgovind, Eloff & Smith, 2010: 2).

As security is a shared responsibility, prior to utilising a cloud service provider, it is important for the cloud user to perform a thorough risk assessment. Such an assessment will highlight the risks associated with cloud services and determine measures which can be implemented to mitigate or minimise those risks. The following section examines the risk assessment to be performed prior to the use of cloud services.

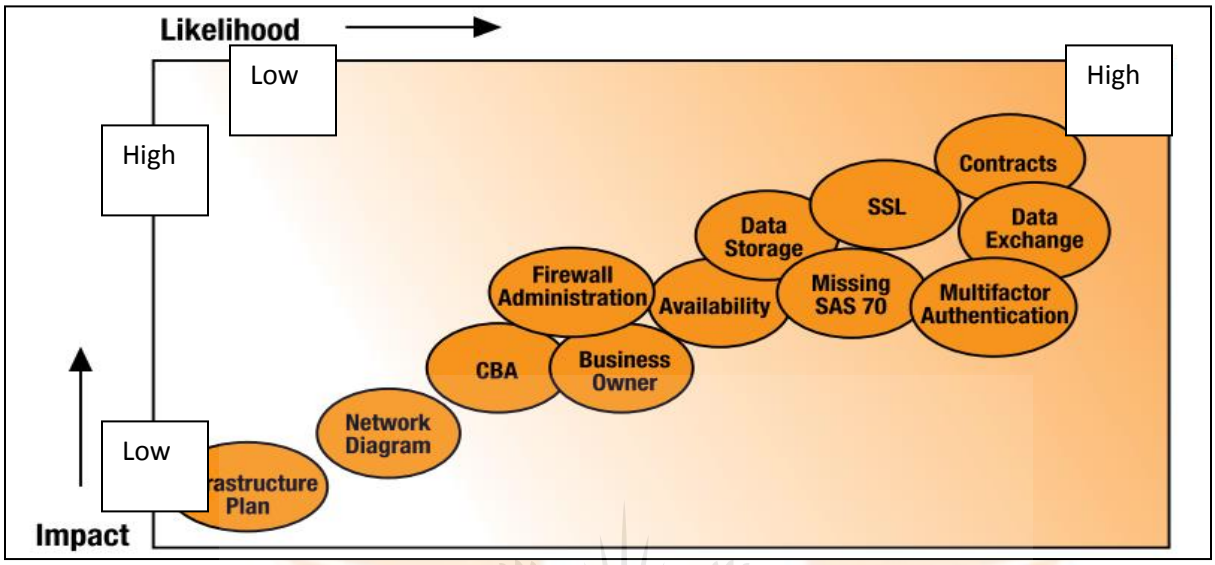
3.3. Risk assessment to be performed prior to adopting cloud services

According to Carroll, Van Der Merwe and Kotzé (2011: 3), “risk identification and analysis is important to prioritize the implementation (extent and time frame) of governance and controls, as well as to establish scope for reviewing or auditing cloud computing environments”. This is true for both the cloud environment and the in-house

IT environment. Based on the results of risk assessments, controls should be designed, implemented, monitored and evaluated to determine the extent to which desired outcomes are achieved. Risks can be assessed based on their impact and likelihood of occurrence (Hausman, Cook & Sampaio, 2013: 180). Risks with a high level of occurrence and impact should be on top of the priority list.

Figure 1 in the following page shows how risks can be plotted based on their impact and likelihood (Hausman, Cook & Sampaio, 2013: 181). It is noted that the impact and likelihood can be either high or low. The infrastructure plan has low likelihood and impact whereas contracts, data exchange and multifactor authentication have high impact and likelihood. Based on the example below, emphasis will be placed on areas of high impact and likelihood of occurrence. It should be noted that there are also risks that can fall in the middle. Based on the risk tolerance, corrective measures can be implemented to rectify such instances.

Figure 1: Impact and likelihood (risk assessment factors)



Source: (Gadia, 2011: 14)

According to Wilhelmsen and Ostrom (2012: 6), there is no rule as to how risk assessment should be performed or to what extent. Nonetheless, it is important to perform this kind of assessment in order to determine the likelihood and the impact of the risk.

For businesses considering the use of cloud services, it is critical to perform risk assessment prior to migrating to the cloud (Heiser & Nicolett, 2008: 1; Ramgovind, Eloff & Smith, 2010: 5). This will ensure that all risks, including those related to security, are identified, assessed and prioritised and that controls are designed and implemented to mitigate them. There is a close connection between risk assessment and cloud auditing. As part of their key findings, Heiser and Nicolett suggest the use of third parties to perform the risk assessment prior to migrating to the cloud (Heiser & Nicolett, 2008: 1).

According to research performed by Heiser and Nicolett for Gartner (2008: 1) on risk assesment, the following should be taken into account when using external IT services, including cloud computing (Heiser & Nicolett, 2008: 1):

- Assessment of security, privacy and regulatory compliance risks;

- Identification of use case not acceptable based on current risk levels and controls;
- Identification of use cases that pose acceptable levels of risk; and
- Design and implementation of compensating controls prior to going fully operational.

According to the Gartner research as documented by Brodkin (2008: 1-2), outlined below are items that cloud users, or third parties performing the risk assessment on behalf of cloud users, can evaluate.

3.3.1. Privileged user access

When the data of a business is processed by a third party, data owners or business users have less control over the risk related to processing that data (Winkler, 2011: 126). Data processed in the cloud bypasses critical security measures such as physical, least privileged principles and personnel controls usually implemented in a traditional IT environment (Winkler, 2011: 14). Cloud users need to obtain more information about who will be managing the processing of data in the cloud (Winkler, 2011: 131–132). The cloud provider needs to supply details of users who will be granted privileged administrator access and indicate how this access will be monitored (Brodkin, 2008: 1).

3.3.2. Compliance

Even though data processing takes place on the cloud, the cloud user is still held accountable for the security of data through various laws and regulations (Heiser & Nicolett, 2008: 3). Cloud users must therefore ensure that contracts with cloud providers include protection and compliance with applicable laws (Krutz, Vines & Brunette, 2010: 26). As stated by Kandukuri *et al.*, (2009: 519), traditional IT environments are subject to external audits and security certification as part of compliance. Cloud service providers who refuse to add an audit clause as part of the SLA or contractual

agreement should only be used for minor services that are unlikely to result in major security concerns.

3.3.3. Data location

Data location has a direct correlation with compliance with laws and regulations (Chee & Franklin Jr, 2010: 93). In cloud computing, users can access their data from almost anywhere in the world (Chee & Franklin Jr, 2010: 18). This implies that the location of the data can be anywhere. It is important for the cloud user to ensure that the data is kept in a location that is in compliance with local laws under which they operate. This should be added to the contractual agreement between the cloud user and the cloud service provider (Heiser & Nicolett, 2008: 3; Kandukuri *et al.*, 2009: 519).

3.3.4. Data segregation

Services provided in the cloud environment often share the same infrastructure. Customers may thus be sharing resources with one another. In such cases, encryption can be used, however, it should be noted that this will not address all issues that may arise from sharing platforms. Cloud users need to pinpoint the exact strategy for data segregation prior to migrating to the cloud environment (Heiser & Nicolett, 2008: 3).

3.3.5. Availability

In an environment where most businesses rely on data to support critical processes, the reliability of cloud service providers is important (Raj, 2013: 66). Businesses should have a SLA with cloud service providers when considering the use of cloud computing (Hausman, Cook & Sampaio, 2013: 114). Cloud service providers should be held accountable for meeting service levels stipulated in the SLA. Penalties for not meeting minimum service levels should be defined in the agreement or contract (Raj, 2013: 66).

According Kandukuri *et al*., (2009: 519) as part of the SLA questionnaire, cloud users should ask if the service provider can sign for availability.

3.3.6. Recovery

Disaster can strike at any time. Businesses considering the use of cloud services need to evaluate the adequacy of the disaster recovery plans and programmes of cloud service providers. This should be included in the SLA between the cloud user and the cloud service provider (Hausman, Cook & Sampaio, 2013: 115). The provider should be able to indicate how recovery will be achieved in the case of a total disaster. This includes storing or processing data to multiple sites and performing regular back-ups (Heiser & Nicolett, 2008: 3). It should also take into account the time required to recover the data so that ideally, there will be little or no impact on data availability, as explained in Section 3.3.5 above (Brodkin, 2008: 2).

3.3.7. Investigative support

From time to time there may be a need to investigate illegal activities in the IT environment. In a traditional IT environment, audit log files can be utilised for investigative purposes. However, in a cloud environment, the use of log files to monitor activities of all cloud users may be difficult due to the amount of processing and activities (Sabahi, 2011: 246). Prior to moving to a cloud environment, cloud users need to evaluate the mechanism that the service provider will be using to monitor activities on the cloud. This is crucial given the nature of the cloud. Cloud users could be sharing resources with hackers posing as cloud users (Heiser & Nicolett, 2008: 4).

3.3.8. Viability

The possibility of a cloud service provider going out of business or being acquired is unlikely (Sabahi, 2011: 246). However, the cloud user should determine whether the cloud service provider supports adequate interoperability standards to enable migration of data and services to a new platform or cloud service provider (Carroll, Van Der Merwe & Kotzé, 2011: 6). Cloud users should also ascertain how they will retrieve their data and whether this will be in a usable format. This is critical in relation to the point raised in 3.3.5 on availability. Should the service provider go out of business, will the cloud user be able to continue with its primary business? (Heiser & Nicolett, 2008: 4; Hugos & Hulitzky, 2010: 63). This is one of the critical questions that needs to be answered prior to utilising cloud computing services.

It should be noted that there are more risk and control frameworks that can be used for risk assessment and that the above list should not be seen as an exhaustive.

Once risk assessment prior to migration to the cloud has been taken into account, it is critical to set standards that will deal with security issues prevalent in the cloud environment. The section below examines standards that govern the cloud computing environment.

3.4. Security standards governing the cloud

The content analysis revealed that currently there are no finalised standards governing security in the cloud environment (Tripathi & Mishra, 2011: 2). The security community is currently working on a number of initiatives to address security issues associated with the cloud environment (Pearson & Yee, 2013: 240; Raj, 2013: 369). Some of these initiatives include Cloud Security Alliance and ENISA Cloud Computing Information Assurance Framework (Pearson & Yee, 2013: 240). The current lack of uniform cloud standards makes it difficult to implement controls to mitigate security risk in the cloud environment (Carroll, Van Der Merwe & Kotzé, 2011: 1). Tripathi and Mishra (2011: 2)

add that it is important for cloud users to exercise consistent efforts for the execution of SLAs.

There are various international standards on information security; however these do not address the specific security issues identified in the cloud environment. NIST (2013: 5) has drafted a set of security standards for cloud computing although these are not yet finalised. Two international standards that address security risks are examined below.

3.4.1. ISO 27000

The International Organization for Standardization (ISO) has a series of standards; one of these relates to information security (ISO 27000). There are 133 controls grouped in 39 control objectives in this standard (Ristov & Kostoska, 2012: 1485).

According to Ristov and Kostoska (2012: 1489), general security standards do not address all the issues related to the cloud environment. Additions to the current security standards are required to accommodate cloud computing security issues. Winkler adds that although security requirements for the cloud environment may be unique, it is important that such requirements are nonetheless consistent with the appropriate standards such as the ISO 27000 (Winkler, 2011: 93).

3.4.2. NIST Cloud Computing Standards Roadmap

NIST was designated by the Federal Chief Information Officer (CIO) to accelerate the adoption of cloud computing by leading efforts to identify existing standards that can be used in the cloud environment (Marks & Lozano, 2010: 151). Where standards do not exist, NIST has been working closely with US industry leaders in developing security standards, government agencies and other relevant parties in securing the cloud computing environment (NIST, 2013: 5).

In 2013 the NIST Cloud Computing Standards Roadmap - NIST Special Publication 500-291, version 2 was published. This document has been prepared by NIST to describe the research in security standards supporting the NIST Cloud Computing Program (CCP) (NIST, 2013: 5).

The NIST Cloud Computing Program was formally launched in November 2010 and was created to "support federal government efforts to incorporate cloud computing as a replacement for, or enhancement to, traditional information system and application models where appropriate" (NIST, 2013: 5).

According to the NIST Cloud Computing Standards Roadmap (2013: 5), at the beginning of 2011, NIST created the following public working groups to provide a technically-oriented strategy and standards-based guidance for the federal cloud computing implementation effort:

- Cloud Computing Reference Architecture and Taxonomy Working Group;
- Cloud Computing Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) Working Group;
- Cloud Computing Security Working Group;
- Cloud Computing Standards Roadmap Working Group; and
- Cloud Computing Target Business Use Cases Working Group.

In summary, some of the items covered by the NIST Cloud Computing Standards Roadmap include:

- An overview of the cloud computing environment;
- Cloud computing use cases;
- Cloud computing standards;
- Cloud computing standards mapping;
- Analysis of use cases to identify standard gaps; and
- Priorities to fill cloud computing standards gaps

(NIST, 2013: 25-74).

Section 6.5 of the Cloud Computing Standards Roadmap deals specifically with standards for cloud computing security. In this section, it is acknowledged that there are many benefits that can be derived from cloud computing, however, with those benefits, there are associated security risks that need to be taken into account (NIST, 2013: 44). One of the main issues affecting the growth of cloud computing has been identified as security (Wang *et al*., 2012: 42). As noted by Chen, Paxson and Katz (2010: 3), "security has emerged as arguably the most significant barrier to faster and more widespread adoption of cloud computing". The NIST standards document also notes that to accelerate the adoption of cloud services, solutions to deal with threats need to be developed and implemented. It was further noted that most of the issues related to cloud computing can be addressed through traditional security processes and mechanisms (NIST, 2013: 44). The document also mentions some of the security challenges in the cloud.

It is safe to say that significant efforts have been made towards developing standards to address security issues within the cloud environment. Some existing standards (not developed specifically for the cloud environment) can be utilised to address certain issues identified in the cloud environment. Given the current work performed by NIST, it can be expected that in the next few years, final standards will be developed in alignment with the cloud environment, and specifically, standards dealing with security (Raj, 2013: 357).

Security risk in the IT environment is not new. There are numerous security issues that are well-known and more prevalent in an in-house IT function. However, cloud computing introduces new security issues or intensifies some of the existing challenges. In the section below, factors that determine whether a security issue is unique to the cloud environment are discussed. In addition, issues unique to the cloud environment are examined. This is followed by an analysis of security measures that can be used in the cloud environment as well as those that can be applied to both the cloud environment and an in-house IT function.

3.5. Factors that determine security issues unique to cloud computing

Although there are security risks common to both in-house IT functions and the cloud environment, there are specific security issues found exclusively in the cloud environment. According to Pearson and Yee (2013: 238), a security issue is unique to the cloud environment if it meets the following criteria:

- It is more prevalent in the cloud than it is in the traditional IT environment;
- It stems from the characteristics of cloud computing; and
- Security measures that were tried and tested in the traditional IT environment are difficult to implement in the cloud.

These factors unique to security in cloud computing are analysed in the section below.

3.5.1. Prevalence in a core cloud computing environment

Cloud computing core technology includes web applications, virtualisation and cryptography (Grobauer, Walloschek & Stöcker, 2011: 52; Sabharwal & Wali, 2013: 15). Each of these items presents various security risks that are more prevalent in the cloud computing environment. Some of these risks include VM escape, session riding, hijacking and insecure cryptography (Grobauer, Walloschek & Stöcker, 2011: 52).

Virtual escape is a process used by attackers to break out from the VM and thus gain direct access to the host operating system (Krutz, Vines & Brunette, 2010: 164). In 2008, Core Security Technologies discovered vulnerability in VMware's (a major player in the virtualisation domain) virtualisation software that allowed attackers to obtain full control of the system after gaining access through virtualisation (Dignan, 2008).

The implementation of web applications requires session handling techniques. Many of these session handling implementations are vulnerable to session hijacking and session riding (Grobauer, Walloschek & Stöcker, 2011: 52).

As with any technology, advances may render infrastructure insecure or obsolete and cryptography is no exception to the rule. Cryptographic mechanisms or algorithms may become insecure over time as new methods of breaking them are discovered (Grobauer, Walloschek & Stöcker, 2011: 52).

3.5.2. Stems from the characteristics of cloud computing

The vulnerabilities that can be linked to each one of the characteristics of cloud computing were described in Section 2.3 above. These include unauthorised access to management interfaces (Grobauer, Walloschek & Stöcker, 2011: 53). On-demand self-service requires the cloud users to access the cloud through a management interface. Such an interface is susceptible to unauthorised access by attackers.

In most cases, cloud users access cloud services through web browsers over the internet (Wang *et al*., 2012: 17). These may result in internet protocol vulnerabilities such as man-in-the-middle attacks (Grobauer, Walloschek & Stöcker, 2011: 53).

The cloud environment allows for elasticity, i.e. users only use the amount of services required at a particular point in time. Services can be re-allocated to different users and it is possible for new users to gain access to data written by previous users (Grobauer, Walloschek & Stöcker, 2011: 53).

3.5.3. Difficulty with the implementation of security controls

There are security controls that have been proven to work effectively in minimising security risks within an in-house or traditional IT function. However, these controls have proven to be difficult or impossible to implement within the cloud computing environment (Grobauer, Walloschek & Stöcker, 2011: 53). Any risk that cannot be minimised by these controls is considered to be cloud-specific. Some of these risks include:

- Virtualised networks offer insufficient network-based controls;

- Poor key management procedures; and
- Security metrics ill-adapted to the cloud environment.

The following section examines security issues unique to the cloud computing environment.

3.6. Security issues unique to cloud computing

Below is a list of issues unique or more prevalent in the cloud computing environment as opposed to an in-house IT function.

3.6.1. Side and covert channels

Cloud computing is a shared environment with multiple users (Pearson & Yee, 2013: 26). Some of these users may be competitors using the same system or hackers with the sole purpose of gaining unauthorised access to the data of other cloud users (Rountree & Castrillo, 2014: 15). These hackers may establish side channels (passively observing data on the cloud) or covert channels (actively sending data from the cloud by placing their VM on the same physical machine as that of the targeted VM (Chen, Paxson & Katz, 2010: 4).

3.6.2. Fate-sharing

There is no doubt that there are many benefits that can be derived from cloud computing. One of these is the concentration of expertise in complex areas. However sharing resources may have implications for cloud users (Armbrust *et al*., 2009: 18). Compromise in the environment of one user in the same physical environment may result in the disruption of business for all other users (Chen, Paxson & Katz, 2010: 4). One noteworthy incident occurred in April 2009 when the Federal Bureau of

Investigation (FBI) raided a datacentre in Texas on the suspicion that it was facilitating cybercrime. The FBI seized equipment in the datacentre and all businesses that were co-located experienced business disruption, some even business failure (Chen, Paxson & Katz, 2010: 4).

3.6.3. Privacy compliance and legal issues

Please refer to Chapter 2, Section 2.8, which covers privacy and compliance issues in detail.

3.6.4. Availability

Cloud computing relies on resources such as the internet to deliver services and provide cloud users with access from anywhere in the world. Any cloud computing component which delivers services to users may face downtime (Raj, 2013: 360). This can also occur with an in-house IT function, however the impact can be far greater in a cloud environment (Fauzi, Noraziah, Herawan & Zin, 2012: 562; Catlett, Gentzsch & Grandinetti, 2013: 58).

For each of the security risks noted above, a set of security measures can be implemented to mitigate or minimise the risk to an acceptable level. In the following section, security measures are explained in detail.

3.7. Security measures for cloud computing

Outlined below is a list of security measures to mitigate or minimise security risk in cloud computing.

3.7.1. Validation and registration process

The nature of a public cloud environment is that any user is allowed to participate. This creates the risk of spammers and malicious code authors. Cloud service providers need to implement strict registration and validation processes for each of their cloud users. This also implies strong credit card fraud monitoring. The traffic flow of cloud users should also be monitored to ensure that no malicious activities are carried out in the cloud environment (Tripathi & Mishra, 2011: 2).

3.7.2. Private cloud

Companies may also consider having their own private cloud without multiple users, as is the case in public and hybrid cloud environments (Catlett, Gentzsch & Grandinetti, 2013: 57). This provides companies with a secure environment. Cloud service providers such as Amazon Web Service (AWS) offer private cloud services such as Amazon Virtual Private Cloud (VPC) (Carlin & Curran, 2011: 16). AWS allows companies to connect their existing IT infrastructure to a VPC through a Virtual Private Network (VPN) connection (Carlin & Curran, 2011: 16). Amazon offers the VPC services with security expertise such as firewalls and intrusion detection systems. It should be noted that Amazon is one of many cloud service providers with VPC and VPN.

3.7.3. Application Programme Interface (API)

Cloud users may not be fully satisfied with the level of services they receive from one cloud provider; as a result another cloud provider may be used to supplement the service of the initial provider. However, cloud users may be locked in, i.e. it may not be possible to migrate from one cloud provider to another (Kulkarni, Gambhir, Patil & Dongare, 2012: 550). To eliminate such a risk, cloud users should consider using the services of cloud providers where a standardised cloud API is utilised (Winkler, 2011: 39). However, API has its own security drawbacks such as a weak set of interfaces which may expose the cloud to anonymous access (Tripathi & Mishra, 2011: 3). Cloud service providers such as Microsoft, Amazon, IBM and Google all have their own clouds, however, these lack interoperability (Wang *et al*., 2012: 18).

3.7.4. Multifactor authentication

Attackers often use phishing techniques to obtain credentials in order to gain unauthorised access to critical systems, thereby compromising the confidentiality, integrity and availability of cloud services. Cloud users should consider using a cloud service that requires a multifactor authentication technique such as the use of a one-time password (OTP) in addition to a username and password (Tripathi & Mishra, 2011: 3).

3.8. Security measures applicable to both the in-house IT function and the cloud computing environment

The findings of the content analysis indicate that utilising cloud services does not completely shift the responsibility of security from the cloud user (Hwang, Fox & Dongarra, 2012: 49). It was noted that security is a shared responsibility. This implies that certain controls implemented in a traditional IT environment will remain applicable in the environment of a cloud user. These controls are primarily linked to security issues

on the application level. It was also noted that some controls that would be implemented in-house would also have to be implemented by the cloud service provider to mitigate or minimise security risk. This is in addition to control measures implemented by cloud service providers for security risks unique to the cloud environment, as explained in Section 3.6 above. The purpose of this section is to list security measures applicable to both environments (in-house and cloud).

3.8.1. Security policies and procedures

To establish a sound IT security environment, policies and procedures need to be defined and implemented (Krutz, Vines & Brunette, 2010: 154). When a business is considering the use of cloud services and migrating its data and applications to the cloud, IT security policies and procedures applicable to the in-house IT environment need to be extended to the cloud service provider (Surianarayanan & Santhanam, 2012: 75). The cloud service provider must ensure that the security policies and procedures of the cloud user are carried out. There should be a contractual agreement or a SLA between the cloud service provider and the cloud user to enforce compliance with security policies and procedures. Items to be included in the SLA or contractual agreement include the availability of audit log files, compliance with applicable legislation and regulations, types of access controls and encryption standards to be used for data in the cloud (Surianarayanan & Santhanam, 2012: 75).

3.8.2. Intrusion detection systems (IDS) and firewalls

Most cloud services are based on VM technology (Robinson, Valeri & Cave, 2011: 28). The technology relies on a hypervisor for implementation (Tripathi & Mishra, 2011: 2). A hypervisor “abstracts the hardware of a shared physical server into virtualized hardware” (Fehling, Leymann, Retter, Schupeck & Arbitter, 2014: 101). As mentioned in Section 3.6 above, for security risks unique to cloud computing, VM escape is a potential threat allowing attackers to break out from the VM into the host operating

system (Plankers, 2007; Raj, 2013: 364). The security measures that can be implemented to mitigate vulnerabilities in VM technology include IDS and firewalls (Smooth & Tan, 2013: 268). Firewalls prevent entry into the system while IDS monitors any attacking or suspicious activities (Tripathi & Mishra, 2011: 2) and shields the operating system and enterprise applications from known vulnerabilities until the system is once again operational (Raj, 2013: 369).

In addition to the above, firewalls can be used to prevent attacks such as man-in-the-middle or hackers (Hwang, Fox & Dongarra, 2012: 249). The strength of security in an IT environment is determined by the lowest common denominator. Firewalls, in most cases, are the first point of contact that separates internal and external networks (Sabharwal & Wali, 2013: 17).

This control mechanism is applicable in both cloud and traditional IT environments. In the cloud it protects the platform, applications and data kept by the cloud service provider. The cloud service provider should offer evidence of the adequacy of configuration and effectiveness of the firewall (Carroll, Van Der Merwe & Kotzé, 2011: 7).

3.8.3. Encryption and patch management

Encryption is not a new concept in the IT world and it is applicable to both the in-house and the cloud environment. As noted in Chapter 2, cloud users often use the internet to access data and applications in the cloud. The moment data is outside the firewall of a cloud user and a cloud service provider, it needs to be protected from any tampering by the man-in-the-middle (Chraibi & Harroud, 2013: 3). In such instances, encryption may be considered (Pearson & Yee, 2013: 247). Encryption not only protects data during transmission, it also protects data privacy should there be a compromise of the database or VM in which it is kept (Sosinsky, 2011: 260; Catlett, Gentzsch & Grandinetti, 2013: 59). This is supported by Pethuru (2013: 370) who states that “not

only is encrypting data during transmission important, but also imperative to provide data encryption facility while residing in a cloud storage".

However, encryption on its own is not a 'silver bullet' to ensure privacy and integrity. Encryption only guarantees privacy of the data; a different control mechanism is needed to ensure the integrity of the data (Chraibi & Harroud, 2013: 3). Patch management is another control used in the traditional IT environment to protect data integrity and it can also be applied in a cloud environment (Carroll, Van Der Merwe & Kotzé, 2011: 6; Tripathi & Mishra, 2011: 3).

3.8.4. Logical access control – authentication and authority

According to Qing-hai and Ying (2011: 830), "access control is one of the main strategies for network security prevention and protection. Its main task is to fully share system resources and manage user's access rights. Access control regulates the limitations about the access of the subject to the object and controls the request of resource access according to the identity authentication".

Not all users in a business have the same level of access to data, and as such, access is regulated based on what users need to perform (Winkler, 2011: 138). In a traditional IT environment, there are policies and procedures that provide guidance on access to particular sets of data (Raj, 2013: 373 –375). Such access needs to be authorised by relevant parties to allow the user access to given objects (Colantonio, Di Pietro & Ocello, 2012: 8). There are also controls for privileged access (Colantonio, Di Pietro & Ocello, 2012: 3). There should be regular reviews to monitor access levels of users to different applications, modules or data. Access of terminated users should be revoked on time to prevent unauthorised access (Colantonio, Di Pietro & Ocello, 2012: 3). These procedures and controls are also applicable in the cloud environment. According to Pethuru (2013: 90), access and identity management are critical components of cloud security. The most critical control is timeously revoking access of terminated employees (McDonald, 2010: 124). This is important given that cloud users can access data and

applications in the cloud from anywhere in the world (Carroll, Van Der Merwe & Kotzé, 2011: 7).

Access control is a mechanism that can be adopted to ensure privacy. Components of access control policy from an in-house IT environment should be part of the contractual agreement or SLA between the cloud user and cloud service provider. This will allow the cloud user to determine the level of access to be applied to each user group (Chraibi & Harroud, 2013: 3).

In addition to providing users with the adequate level of rights to access authorised data, the use of passwords (Colantonio, Di Pietro & Ocello, 2012: 7–8) or multifactor authentication should be considered to ensure that only authorised users can access data (Carroll, Van Der Merwe & Kotzé, 2011: 7).

3.8.5. Physical access controls

Physical access control regulates the flow of personnel to and from restricted areas such as property, a building or a room, thus providing assurance of the integrity of machines and the data they store (Pearson & Yee, 2013: 240). “They act as important points of demarcation between physical zones (areas/rooms)” (Fitzgerald, Turkmen, Foley & Sullivan, 2012: 1). According to Hwang, Fox and Dongarra (2012: 249), as part of the cloud service provider’s basic security for facilities, the following should be taken into account:

- On-site security year around;
- Biometric readers;
- Closed-Circuit TV (CCTV);
- Motion detectors; and
- Man traps.

With all the security measures that can be implemented in an IT environment, physical control is one of the most important (Winkler, 2011: 91–92). To have adequate logical access to an environment with weak physical access controls may result in an ineffective internal control system. It was also noted that new access rules are often added or removed; in such instances, it is important to consider the impact on interoperability with existing access rules (Fitzgerald *et al*., 2012: 1).

Physical access controls are widely used and have proven very useful in a traditional IT environment. In the same manner, they can be utilised in the cloud environment to improve security.

3.8.6. Back-ups and disaster recovery

Data is one of the most important assets in many businesses and should always be available when needed. Businesses often have back-up and disaster recovery plans to ensure continuity in case of severe disaster. Such policies and procedures must be incorporated into the contractual agreement or SLA between the cloud user and the cloud service provider. Cloud service providers should perform back-ups and disaster recovery plan testing on regular basis. Evidence of back-ups and disaster recovery testing should be kept and provided when needed (Carroll, Van Der Merwe & Kotzé, 2011: 6). The use of back-ups as a mechanism to counter data loss and disruption to operations is also supported by Surianarayanan and Santhanam (Surianarayanan & Santhanam, 2012: 74). Besides relying on the cloud service provider to perform back-ups on the cloud, cloud users can also perform their own data back-ups or use services of other third parties to assist with back-ups (Chraibi & Harroud, 2013: 4). This will ensure that data is always available when needed.

However, having control measures in place is pointless unless their effectiveness can be assessed through evaluation processes. It is therefore important to evaluate control measures on a regular basis to ensure that they work as intended. In the next section,

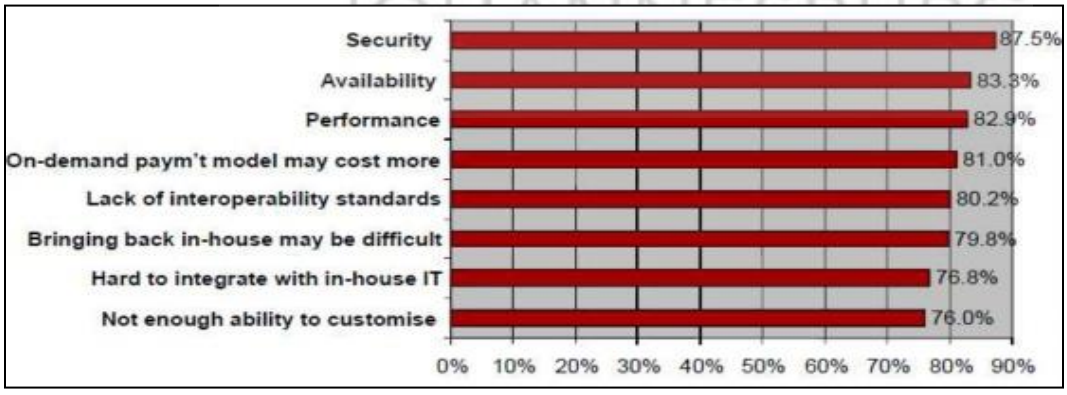
the study determines the possibility and the importance of the independent evaluation of cloud services to provide reasonable assurance on security.

3.9. Independent evaluation of cloud computing security

In a traditional IT environment, regular audits are performed to provide assurance that controls to mitigate and minimise security risk are functioning as intended. According to a survey by International Data Corporation (IDC) performed in September 2009 (2010: 1328), it was noted that security heads the list of issues within the cloud environment. Independent assurance on security is therefore vital.

The findings of Zhang, Wuwong, Li and Zhang (2010: 1328) are illustrated in Figure 2 below which shows the results of a survey conducted by the IDC Enterprise Panel to highlight important issues in the cloud environment. This survey was conducted in consultation with 244 IT executives and their business colleagues regarding their use of IT cloud services. It was noted that their most significant challenge in the cloud was security at 87.5%.

Figure 2: Survey results of issues in cloud computing



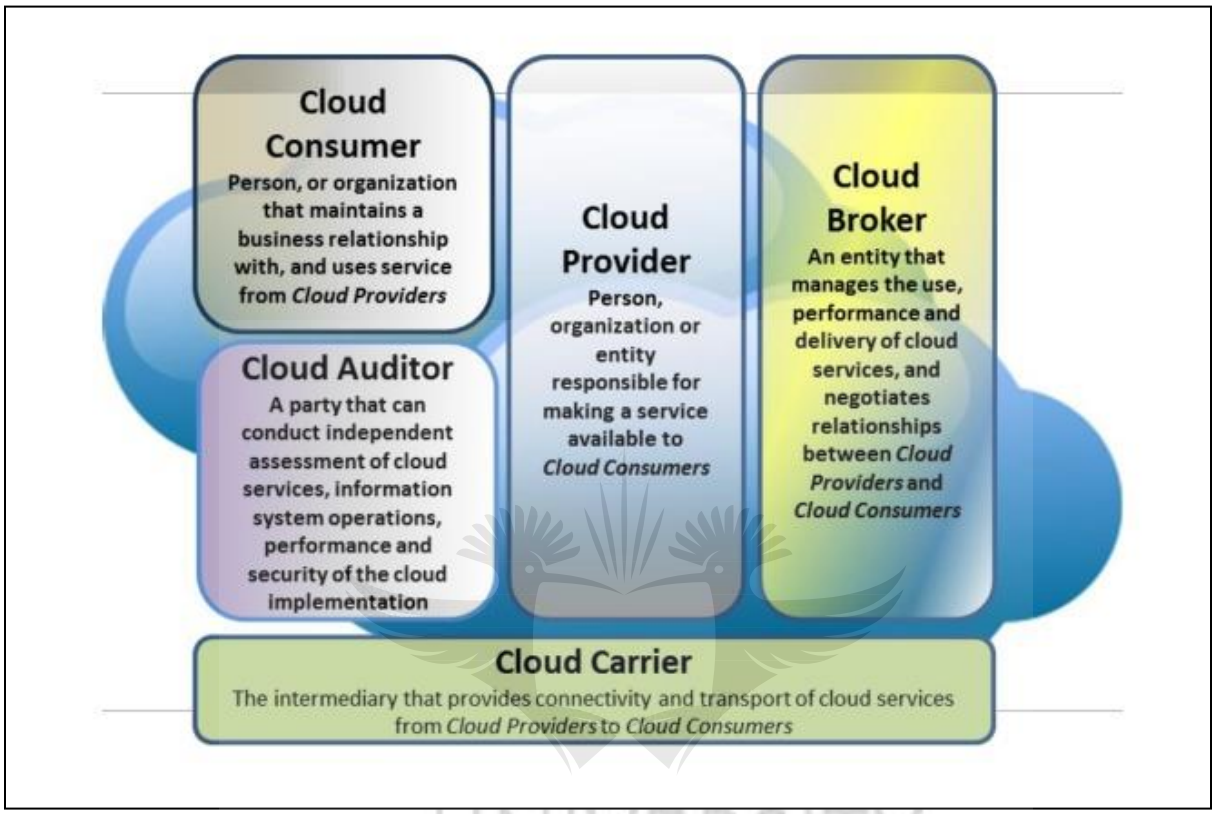
Source: (Zhang et al., 2010: 1328)

As part of this study, is was also noted that audits can either be voluntary, to provide assurance on security issues, or regulatory, to comply with laws and legislation (NIST, 2013: 23).

As per the ISACA Journal, IT Governance and the Cloud: Principles and Practice for Governing Adoption of Cloud Computing (2011: 22), many cloud service providers are now engaging the services of auditors to independently verify controls in the cloud environment and to make these assessment accessible to cloud users in the form of an independent audit report. These reports are often referred to as Statement Auditing Standards (SAS) No. 70.

According to NIST (2013: 12), there are five major players in the cloud environment. One of these is the cloud auditor. According to NIST (2013: 12), a cloud auditor is an independent party which conducts independent audits of cloud services, information system operations, performance and security. Cloud auditors conduct assessments which can provide assurance on the security controls of the cloud service provider and determine the extent to which these controls are correctly implemented and functioning as intended to achieve desired outcomes. Auditors also assess privacy impact, regulatory and security policy compliance, adherence to provisions of the SLAs and performance (NIST, 2013: 23). Figure 3 in the next page represents a diagram showing the five major players in the cloud environment, including the cloud auditor.

Figure 3: Five major players defined in the NIST cloud computing reference architecture



Source: (NIST, 2013: 12)

Based on the content analysis, it was noted that it is possible to audit cloud services, security controls and information. Cloud users should ensure that as part of their SLA there is a provision which addresses auditing of the cloud environment. According to Kandukuri *et al.*, (2009: 519), traditional IT environments are subject to audits and security certification. Cloud service providers who refuse to add this clause as part of the SLA or contractual agreement should only be used for trivial services that are unlikely to result in major security concerns. This is to ensure that cloud users are completely satisfied with the cloud services provided as they would with an in-house IT function. According to Carroll, Merwe and Kotzé (2011: 6), independent evaluations should be performed on a regular basis to monitor cloud services to assess compliance with agreed terms and adherence to standards, procedures and policies.

Security incidents which have occurred in the past can be utilised to determine the current or future state of security in the cloud environment. The following section examines past security incidents in the cloud environment.

3.10. Past security incidents related to the cloud environment

In the recent past, there have been several noticeable security breaches in the cloud environment. Companies affected by these security breaches include eHarmony, LinkedIn, Twitter, and most recently, Dropbox and Apple's iCloud. In the section below, a summary of each of these breaches is analysed and the Alert Logic Cloud Security Reports for 2012 and 2014 are reviewed.

3.10.1. Dropbox security breach

On 13 October 2014, hundreds of usernames and plaintext passwords were leaked from Dropbox by hackers. This was used as a 'teaser' of almost seven million accounts which had been compromised. The hackers promised to release more information in return for payment (Reilly, 2014).

According to an article on cnet.com (Reilly, 2014), Dropbox refused to admit that it had been hacked into; instead, the official statement released mentioned that the account credentials had been stolen from a third party service provider. It should be noted that this is not the first time there has been a security breach at Dropbox; another breach had occurred in 2012 (Steiner, 2012: 6).

3.10.2. Passwords stolen from eHarmony and LinkedIn

In 2012, business social network LinkedIn confirmed that the credentials of some of its users had been compromised. Approximately six million passwords and usernames had been leaked. Around the same period, the online dating service site, eHarmony, had the credentials of some of its users compromised. Although measures were taken by both companies to have the passwords of the members expire, the biggest concern was that many users utilise the same password on multiple platforms such as Gmail. Access to other platforms could therefore be obtained through the use of leaked data (CBS News Staff, 2012).

3.10.3. Twitter security breach

Since 2009, Twitter has been compromised several times. The Federal Trade Commission brought two charges for breach against Twitter in 2009 for deceiving consumers and putting their privacy at risk. This came after hackers managed to obtain administrator access to Twitter, allowing them to send tweets from any account. One of the high profile accounts affected was that of Barack Obama (Power, 2013).

In the second instance, a hacker managed to compromise the personal e-mail of one of the Twitter employees with administrator access. The e-mail contained a password in plain text which enabled the hacker to gain access to the Twitter administrator account (Power, 2013).

In 2010 there was a ‘mouse over link attack’. Certain tweets containing links had been hijacked. Whenever users hovered their mouse over the hijacked links, pop-up ads and links to adult sites were displayed (Power, 2013).

In May 2012, the credentials of approximately 60,000 users were published online by hackers. It was unclear how the hackers had gained access to the passwords and usernames. Twitter resolved the matter by resetting the passwords of the affected

accounts (Power, 2013). A similar incident was noted in 2013 when the accounts of 250,000 users had been compromised (McHugh, 2013).

3.10.4. iCloud security breach

The most recent security breach to occur was that of Apple's iCloud. This was perhaps the most talked about security breach following the unauthorised publication of personal photographs of American celebrities. However, after a thorough investigation, Apple denied that the security breach had been due to security flaws on its part or of any of its systems. The official statement asserted that accounts had been compromised as the result of a targeted attack on usernames and passwords (CBS News Staff, 2014).

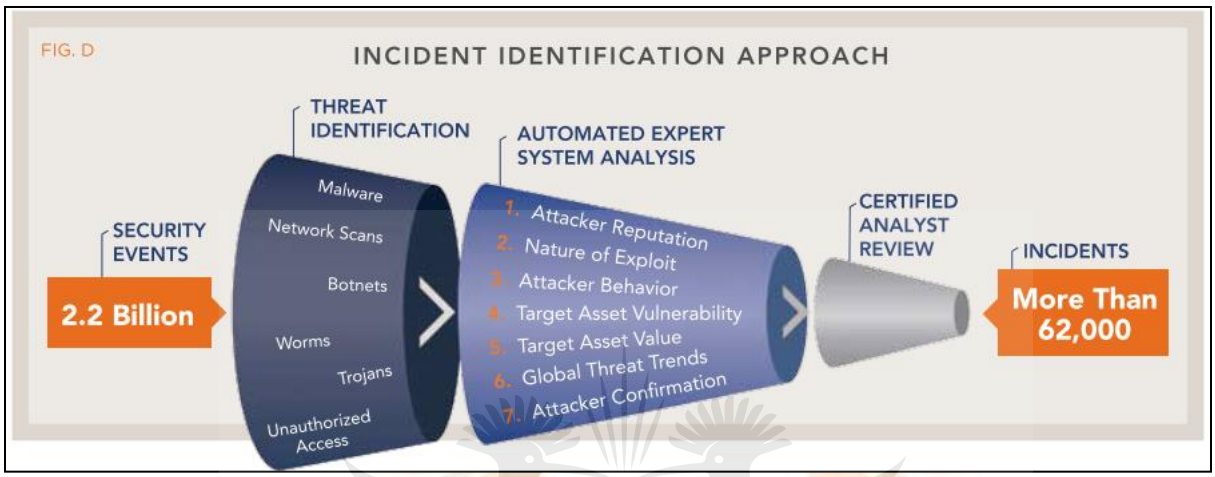
3.10.5. Alert Logic Cloud Security Report for 2012

"In early 2012, Alert Logic launched the first in a series of reports on cloud security, with the goal of creating the IT industry's assessment of security in the cloud for businesses considering the use of cloud computing platforms" (Rackspace Support, 2014). This report not only focuses on the security trends of the cloud but also on those of traditional in-house IT environments. The purpose of looking at this report in this study is to understand the differences between the different categories of threats encountered in both environments, i.e. in-house IT function and cloud.

In the 2012 report, the real-world findings from a base of 1,500 customers of Alert Logic were used to understand the differences in the categories of threats encountered in both environments, i.e. in-house and cloud (Alert Logic, 2012: 2). Security events over a period of twelve months between July 2010 and June 2011 were used to compile the 2012 security report. Figure 4 in the next page illustrates the approach adopted by Alert Logic. As part of the report, 2.2 billion security events were observed and the identified threats were classified into six different categories. Threats were analysed through an

automated system and 62,000 incidents classified into six categories of security risks were identified.

Figure 4: Alert Logic incident identification approach for 2012



Source: (Alert Logic, 2012: 6)

According to the Alert Logic report (Alert Logic, 2012: 3), the following key findings were noted in 2012:

- "When compared to traditional in-house managed IT environments, service provider environments show lower occurrence rates for every class of incident examined;
- Service provider customers experienced lower threat diversity (i.e. the number of unique incident classes experienced by a customer) than on-premise customers;
- On-premise environments were twelve times more likely than service provider environments to have common configuration issues, opening the door to compromise; and
- While conventional wisdom suggests a higher rate of web application attacks in the service provider environment, Alert Logic found a higher frequency of these incidents in on-premise environments".

As per the Alert Logic report for 2012, there are more attacks that occur in the traditional IT environment than there are in a cloud environment. This finding suggests that, to some extent, with adequate security controls in the cloud environment, the impact of cloud computing on business processes can be kept to minimum.

3.11. Conclusion

In this chapter a content analysis was conducted to answer the following core questions of the study:

- What security risks are presented or intensified by the use of cloud computing for businesses?
- Can the safety of the cloud computing environment be independently evaluated to provide acceptable levels of assurance to organisations utilising cloud computing services?

It was noted that responsibility for security in the cloud environment was a task shared between the cloud service provider and the cloud user. In cases where third parties are used, those parties will also be responsible for security of the cloud. However, the cloud user has ultimate responsibility for data confidentiality, integrity and access controls (in terms of defining access parameters and levels of access for users) (Chee & Franklin Jr, 2010: 167). The cloud user should ensure that utilising a cloud service provider does not result in security issues that may compromise compliance with laws and regulations.

In any business, risk assessment is important in identifying risks, prioritising them based on likelihood and impact as well as designing controls to mitigate them. A report conducted by research firm Gartner was analysed and it was noted that cloud users, or those performing assessments of the cloud on their behalf, should evaluate the following:

- Privileged user access;
- Compliance;

- Data location;
- Data segregation;
- Availability;
- Recovery;
- Investigative support; and
- Viability.

The availability of security standards applicable to the cloud environment was discussed. It was noted that currently, there are no standards specific to the cloud. There are general security standards such as ISO standards (ISO 27000) that may be used; however, these are not sufficient to address all issues affecting the cloud environment. It was also noted that NIST is currently working on cloud standards that will be applicable specifically to the cloud environment. In the NIST standards, a section will be dedicated to security as a critical component. In 2013, NIST published the NIST Cloud Computing Standards Roadmap - NIST Special Publication 500-291, version 2. The NIST standard document describes the research in security standards supporting the NIST Cloud Computing Program.

This chapter summarised the security issues unique to cloud computing. Security measures critical for both the traditional IT and the cloud environment were discussed. Some of these issues included establishing security policies and procedures to secure both environments, firewalls to separate internal and external networks and physical access controls.

In traditional IT environments, it is standard procedure to perform an independent review of security controls to determine their adequacy in achieving desired results. In certain instances, independent evaluations are performed to comply with regulations. For businesses considering the use of cloud computing, it was noted that an independent evaluation is possible; however, cloud users should ensure that such an evaluation is included in the contractual or SLA.

The last part of this chapter focused on security incidents related to the cloud environment. It was noted that there were incidents in which attackers were able to gain access to user accounts in the cloud. One such incident recently affected Dropbox and iCloud. It was also noted that there was a case where attackers managed to gain administrator access allowing them to perform any activity they wished. A security breach at Twitter was another incident where administrator access was obtained. The Alert Logic report for 2012 was also reviewed. This report set down the IT industry's assessment of cloud security for businesses considering the use of cloud computing platforms and focused on different categories of threat encountered in the in-house IT function and cloud environments.

The following chapter which concludes this study assesses the impact of cloud computing security on businesses operations.

Chapter 4: Conclusion

4.1 Introduction

Chapter 4 presents the conclusion to this study, which aims to determine how safe it is for businesses to utilise the services of cloud computing for their daily operations in order to meet the needs of their customers, and ultimately, to achieve their business objectives.

As discussed in Chapter 1, with the changes brought about by time and progress in IT, businesses are almost forced to keep up. The manner in which businesses strive to meet the needs of their customers changes overtime. For businesses relying mainly on technology to serve their customers, keeping up with progress and changes in IT can be an expensive exercise with great impact on profitability. In such instances, businesses may consider alternatives to meet needs of customers economically while still achieving their objectives. One of the alternatives that can be considered regarding the IT function is cloud computing. Cloud computing was noted to have the following benefits:

- Users are not tied to a single workstation as they can use any computer anywhere in the world to conduct their daily activities;
- Cloud computing allows collaborations for a group of people working on the same project but located in different parts of the world;
- Cloud computing allows organisations to focus on their core business and innovation while using the latest, first class technology to conduct business and serve the needs of customers;
- Cloud computing allows scalability. Should more resources be required to handle increased activities, more hardware can be added to improve system performance and capacity; and
- Cloud computing is cost-effective and allows flexibility of infrastructure.

Alongside all the benefits that can be derived from utilising cloud computing, there are also disadvantages. The main disadvantage noted in the cloud environment was security which was discussed in Section 2.7 of Chapter 2.

The purpose of this study is to determine how secure it is for businesses to utilise the services of cloud computing in their daily operations to meet the needs of their customers, and ultimately, to achieve their business objectives. The research questions were discussed in Section 1.3.2 and research objectives in Section 1.3.3 of Chapter 1.

In order to answer the research questions and meet the research objectives of this study, a literature review was performed in Chapters 2 and 3. Chapter 2 focused on the concept of cloud computing, its definition, characteristics, advantages and disadvantages, deployment and delivery models as well as compliance with laws and regulations. The impact of cloud computing on the security of business operations was evaluated in Chapter 3.

4.2 Cloud computing and definition, explanation and understanding of this concept

As part of the literature review, the following was covered in Chapter 2:

- Definition of cloud computing;
- Characteristics of cloud computing;
- Delivery and deployment models;
- Benefits and disadvantages of cloud computing; and
- Compliance and regulations on data privacy versus security on the cloud.

Based on the content analysed, it was noted that there is a common understanding of the characteristics, delivery and deployment models of cloud computing.

Using cloud computing can present legal compliance complications. Different countries have different sets of rules and laws with regard to protection of information, specifically personal information. In South Africa, for example, organisations need to comply with the new Protection of Personal Information Act of 2013. Businesses considering the use of cloud computing services need to take into account applicable laws to ensure compliance.

4.3 The impact of cloud computing on the security of business operations

Chapter 4 concludes on the last question which was raised in Chapter 1:

- How safe is cloud computing for use by organisations in their daily operations?

4.4 How safe is cloud computing for use by organisations in their daily operations?

According to Winkler (2011: 25), “despite concerns from many security professionals, cloud computing isn’t innately secured. But the cloud model does force a movement toward a more robust and capable foundation of security services. The mere act of transition from legacy systems gives hope that we can regain control of the gaps and issues that stem from poorly integrated or after-thought security”.

Taking everything in the preceding chapters into account, it can be concluded that cloud computing does bring with it an increased level of security risk. This is as a result of issues that are unique to the cloud environment. Businesses considering the use of cloud services need to perform a thorough risk assessment to determine the level of risk presented by this alternative. As part of the risk assessment, businesses should also consider control measures that are currently in place to minimise or mitigate the risk. The adequacy of these control measures should be assessed, not only prior to migration, but also during the period in which cloud services are being utilised.

An additional critical element which needs to be reviewed prior to utilising the cloud is compliance. Businesses should consider all legal implications associated with cloud computing.

4.5 Conclusion

In Chapter 3 it was noted that when utilising cloud computing, users do not automatically transfer all security risk to the service provider. Although this remains a shared task, cloud users carry the ultimate responsibility for security.

With all the security risks presented by the use of cloud computing, there are nonetheless measures that can be adopted to mitigate or minimise security risk to acceptable levels. Cloud users should consider these measures and assess their adequacy in achieving the desired outcomes.

There are specific security issues which are unique to the cloud environment. However, it was noted that some of these threats can also be found in a traditional IT environment. This implies that mitigating measures may be similar across the two environments. Security measures common for both the cloud and the traditional IT environment include:

- Security policies and procedures;
- Firewalls;
- Encryption and patch management;
- Logical access controls;
- Access logs;
- Physical access controls; and
- Back-up and disaster recovery plans.

It was noted that although these security measures are useful, security standards, as discussed in Section 3.4, may be required to deal with risks specific to the cloud

environment. Currently, there are no final security standards applicable to the cloud environment. There are, however, general security standards such as those issued by the ISO, for example, ISO 27000 which may be applied in the cloud environment. NIST is currently focusing on the development of standards for the cloud environment, including those on security. A draft document with the standards was published in 2013. The purpose of this project is to support the NIST Cloud Computing Program.

In summary, some of the items covered by the NIST Cloud Computing Standards Roadmap draft document include:

- An overview of the cloud computing environment;
- Cloud computing use cases;
- Cloud computing standards;
- Cloud computing standards mapping;
- Analysing use cases to identify standard gaps; and
- Priorities to fill cloud computing standards gaps.

In Chapter 3 in Section 3.5, it was noted that an independent evaluation of cloud service activities and controls can be conducted to ensure security and compliance with applicable laws. As part of the SLA or contractual agreement, cloud users should ensure that there is a provision for the independent evaluation of controls and compliance. This is critical in ensuring that the cloud service provider adheres to the defined security parameters as part of the agreement. The evaluation is also important in ensuring that the cloud service provider does not perform activities that will compromise the compliance of the cloud user with applicable laws.

The study further evaluated past security incidents. It was noted that there have been security breaches in the cloud; in one case attackers managed to obtain the credentials of users whilst in another, attackers gained administrator access allowing them to perform any activity. The security report by Alert Logic for 2012 was assessed in Section 3.10.5. The key finding was that the cloud environment is as exposed to threat

as the traditional IT environment, although it was noted that most attacks still occur in the traditional environment.

For businesses considering the use of the cloud environment, performing a risk assessment is important, as was discussed in Section 3.3. This allows businesses to determine which risks should be prioritised based on their impact and likelihood and which control measures should be put into place to minimise or mitigate such risks. As part of a study performed by the Gartner research firm, cloud users need to evaluate the following as part of risk assessment prior to migrating to the cloud:

- Privileged user access;
- Compliance;
- Data location;
- Data segregation;
- Availability;
- Recovery;
- Investigative support; and
- Viability.

In conclusion, by performing all the necessary checks and assessments, the cloud computing environment may be seen as a viable and safe alternative for businesses to utilise in their daily operations to meet the needs of their customers.

4.6 References

Alert Logic. 2012. *Removing The cloud of insecurity State of Cloud Security Report*. Houston. Available: http://www.alertlogic.com/wp-content/uploads/2013/11/alertlogic_state-of-cloud-security%E2%80%93spring2012.pdf.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. 2009. *Above the Clouds: A Berkeley View of Cloud Computing*. California. Available: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. 2010. A View of Cloud Computing. *Communications of the ACM*. 53(4):50–58. DOI: 10.1145/1721654.1721672.

Bai, Y. & Policarpio, S. 2011. On Cloud Computing Security. In *Recent Trends in Wireless and Mobile Networks*. V. 162. A. Özcan, J. Zizka, & D. Nagamalai, Eds. Berlin Heidelberg: Springer. 388–396. DOI: 10.1007/978-3-642-21937-5_37.

Battacharyya, D.K. 2006. *Research Methodology*. 2nd ed. New Delhi: Anurag Jain.

Brodkin, J. 2008. Gartner: Seven cloud-computing security risks. *InfoWorld*. July:2–3. Available: http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf [2014, August 18].

Carlin, S. & Curran, K. 2011. Cloud computing security. *International Journal of Ambient Computing and Intelligence*. 3(1):14–19. DOI: 10.4018/jaci.2011010102.

Carroll, M., Van Der Merwe, A. & Kotzé, P. 2011. Secure Cloud Computing Benefits , Risks and Controls. In *Information Security South Africa (ISSA), 2011*. Johannesburg: IEEE. 1 – 9. DOI: 10.1109/ISSA.2011.6027519.

Catlett, C., Gentzsch, W. & Grandinetti, L. 2013. *Advances in Parallel Computing, Volume 23 : Cloud Computing and Big Data*. Amsterdam, Ed. IOS Press.

CBS News Staff. 2012. *eHarmony suffers password breach on the heels of LinkedIn*. Available: http://www.cbsnews.com/news/eharmony-suffers-password-breach-on-heels-of-linkedin/.

CBS News Staff. 2014. *Apple denies iCloud security breach in celebrity nude photo hacking*. Available: http://www.cbsnews.com/news/apple-denies-icloud-security-breach-in-celebrity-nude-photo-hacking/.

Chee, B. & Franklin Jr, C. 2010. *Cloud Computing - Technologies and Strategies of the Ubiquitous Data Centre*. Boca Raton, FL: CRC Press.

Chen, Y., Paxson, V. & Katz, R.H. 2010. What's New About Cloud Computing Security? *University of California, Berkeley Report No. UCB/EECS-2010-5 January*. 20:1–8. DOI: 10.1007/978-1-4419-6524-0.

Chraibi, M. & Harroud, H. 2013. Classification of Security Issues and Solutions in Cloud Environments. In *IIWAS '13: Proceedings of International Conference on Information Integration and Web-based Applications & Services*. New York, NY: ACM. 1 – 5. DOI: 10.1145/2539150.2539222.

Colantonio, A., Di Pietro, R. & Ocello, A. 2012. *Role Mining in Business : Taming Rose-Based Access Control Administration*. Singapore: World Scientific Publishing Co.

Dignan, L. 2008. *Researcher: Critical vulnerability found in VMware's desktop apps*. Available: http://www.zdnet.com/blog/security/researcher-critical-vulnerability-found-in-vmwares-desktop-apps/902.

Fauzi, A.A.C., Noraziah, A., Herawan, T. & Zin, N.M. 2012. On Cloud Computing Security Issues. In *Intelligent Information and Database Systems*. V. 7197. J.-S. Pan, S.-M. Chen, & N.T. Nguyen, Eds. Taiwan: Springer. 560–569. DOI: 10.1007/978-3-642-28490-8_58.

Fehling, C., Leymann, F., Retter, R., Schupeck, W. & Arbitter, P. 2014. *Cloud computing patterns : fundamentals to design, build, and manage cloud applications*. New York, NY: Springer-Verlag Wien 2014.

Fitzgerald, W.M., Turkmen, F., Foley, S.N. & Sullivan, B.O. 2012. Anomaly Analysis for Physical Access Control Security Configuration. In *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference*. Cork: IEEE. 1 – 8. DOI: 10.1109/CRISIS.2012.6378953.

Gadia, S. 2009. Cloud Computing: An Auditor's Perspective. *ISACA Jornal - Expanding Business Horizons Through IT*. 6:1–5. Available: http://www.isaca.org/Journal/Past-Issues/2009/Volume-6/Pages/default.aspx.

Gadia, S. 2011. Cloud Computing Risk Assessment. *ISACA Jornal - Security in a Box*. 4:11–15. Available: http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/default.aspx.

Gong, C., Liu, J., Zhang, Q., Chen, H. & Gong, Z. 2010. The characteristics of cloud computing. In *Proceedings of the International Conference on Parallel Processing Workshops*. San Diego, CA: IEEE. 275–279. DOI: 10.1109/ICPPW.2010.45.

Grobauer, B., Walloschek, T. & Stöcker, E. 2011. Understanding cloud computing vulnerabilities. *IEEE Security and Privacy*. 9:50–57. DOI: 10.1109/MSP.2010.115.

Grossman, R.L. 2009. The case for cloud computing. *IT Professional*. 11:23–27. DOI: 10.1109/MITP.2009.40.

Hausman, K., Cook, S.L. & Sampaio, T. 2013. *Cloud Essentials : CompTIA Authorized Courseware for Exam CLO-001*. Indianapolis, Ind: John Wiley & Sons.

Heiser, J. & Nicolett, M. 2008. *Assessing the Security Risks of Cloud Computing*. Available: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing.

Hugos, M.H. & Hulitzky, D. 2010. *Business in the Cloud : What Every Business Needs to Know about Cloud Computing*. New Jersey: John Wiley & Sons.

Hurwitz, J., Bloor, R., Kaufman, M. & Halper, F. 2009. *Cloud Computing For Dummies*. Hoboken, NJ, USA: For Dummies.

Hwang, K., Fox, G. & Dongarra, J. 2012. *Distributed and Cloud Computing*. Waltham: Elsevier.

Kandukuri, Reddy, B., Paturi, R. & Rakshit, A. 2009. Cloud Security Issues. In *2009 IEEE International Conference on Services Computing*. Bangalore: IEEE. 517–520. DOI: 10.1109/SCC.2009.84.

Kaufman, L.M. 2009. Data security in the world of cloud computing. *IEEE Security and Privacy*. 7:61–64. DOI: 10.1109/MSP.2009.87.

Kaur, P.J. & Kaushal, S. 2011. Security Concerns in Cloud Computing. *Communications in Computer and Information Science Volume*. 169:103–112. DOI: 10.1007/978-3-642-22577-2_14.

Khan, A.U., Oriol, M., Kiran, M., Jiang, M. & Djemame, K. 2012. Security Risks and their Management in Cloud Computing. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference*. Taipei: IEEE. 121–128. DOI: 10.1109/CloudCom.2012.6427574.

Kothari, C.R. 2004. *Research Methodology - Methods & Techniques*. 2nd ed. New Delhi: New Age International Publishers.

Krutz, R.L., Vines, R.D. & Brunette, G. 2010. *Cloud Security : A Comprehensive Guide to Secure Cloud Computing*. Indianapolis, Ind: John Wiley & Sons.

Kulkarni, G., Gambhir, J., Patil, T. & Dongare, A. 2012. A security aspects in cloud computing. In *2012 IEEE International Conference on Computer Science and Automation Engineering*. Beijing: IEEE. 547–550. DOI: 10.1109/ICSESS.2012.6269525.

Li, H., Tian, X., Wei, W. & Sun, C. 2012. A Deep Understanding of Cloud Computing Security Security Issues in Cloud Computing. *Network Computing and Information Security*. 345:98–105. DOI: 10.1007/978-3-642-35211-9_13.

Liu, W. 2012. Research on Cloud Computing Security Problem and Strategy. In *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference*. Yichang: IEEE. 1216–1219. DOI: 10.1109/CECNet.2012.6202020.

Marinescu, D.C. 2013. *Cloud Computing : Theory and Practice*. Saint Louis, MO, USA: Morgan Kaufmann.

Marks, E.A. & Lozano, B. 2010. *Cloud Computing*. New Jersey: John Wiley & Sons.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. 2011. Cloud computing - The business perspective. *Decision Support Systems*. 51:176–189. DOI: 10.1016/j.dss.2010.12.006.

McDonald, K. 2010. *Above the Clouds : Managing Risk in the World of Cloud Computing*. Cambridgeshire: IT Governance Publishing.

McHugh, M. 2013. *250,000 User Accounts Attacked in Twitter Security Breach*. Available: http://www.digitaltrends.com/social-media/twitter-security-breach/.

Mell, P. & Grance, T. 2011. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Miller, M. 2009. *Cloud Computing: Weba Based Applications That Change The Way You Work and Collaborate Online*. Indianapolis, Ind: Que Publishing.

Munyaka, D., Noviansyah, B., Goel, V., Yenchik, A. & Durham, S. 2012. *Cloud computing security*. V. 3. Available: http://www.vibhanshu.com/courses/telecom/wp-content/uploads/2013/09/CloudComputingSecurity.pdf [2014, August 18].

Newman, I. & Benz, C. 1998. *Qualitative-quantitative research methodology: Exploring the continuum*. Illinois: SIU Press.

NIST. 2013. *NIST Cloud Computing Standards Roadmap*. Gaithersburg, MD. DOI: 10.6028/NIST.SP.500-291r2.

NIST. 2014. *NIST Cloud Computing Program*. Available: http://www.nist.gov/itl/cloud/index.cfm.

Pearson, S. & Yee, G. 2013. *Privacy And Security For Cloud Computing*. London ; New York: Springer.

Plankers, B. 2007. *VM Escape & VMware Critical vmkernel Updates*. Available: http://lonesysadmin.net/2007/09/22/vm-escape-vmware-critical-vmkernel-updates/.

Power, D. 2013. *A History of Twitter Security Breaches (And How to Protect Yourself)*. Available: http://sproutsocial.com/insights/twitter-security-breaches/.

Protection of Personal Information Act 4 of 2013. 2013. Republic of South Africa: Online. Available: http://us-cdn.creamermedia.co.za/assets/articles/attachments/47193_37067_26-11_act4of2013protectionofpersonalinfor_correct.pdf.

Qian, L., Luo, Z., Du, Y. & Guo, L. 2009. Cloud computing: An overview. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 5931:626–631. DOI: 10.1007/978-3-642-10665-1_63.

Qing-hai, B. & Ying, Z. 2011. Study on the Access Control Model in Information Security. In *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011 (Volume:1)*. Harbin: IEEE. 830–834. DOI: 10.1109/CSQRWC.2011.6036867.

Rackspace Support. 2014. *ALERT LOGIC CLOUD SECURITY REPORT SPRING 2014: Research on the Evolving State of Cloud Security*. Available: http://www.rackspace.com/knowledge_center/whitepaper/alert-logic-cloud-security-report-spring-2014-research-on-the-evolving-state-of-cloud.

Raj, P. 2013. *Cloud Enteprise Architecture*. Boca Raton, FL: CSC Print.

Ramgovind, S., Eloff, M. & Smith, E. 2010. The Management of Security in Cloud Computing. In *Information Security for South Africa (ISSA)*. Sandton, Johannesburg: IEEE. 1–7. DOI: 10.1109/ISSA.2010.5588290.

Reilly, C. 2014. *Hackers hold 7 million Dropbox password ransom*. Available: http://www.cnet.com/news/hackers-hold-7-million-dropbox-passwords-ransom/.

Ristov, S. & Kostoska, M. 2012. A New Methodology for Security Evaluation in Cloud Computing. In *MIPRO, 2012 Proceedings of the 35th International Convention*. Opatija: IEEE. 1484–1489. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6240887&queryText%3DA+New+Methodology+for+Security+Evaluation+in+Cloud+Computing.

Robinson, N., Valeri, L. & Cave, J. 2011. *Cloud*. Santa Monica: RAND Corporation.

Rountree, D. & Castrillo, I. 2014. *Basics of cloud computing understanding the fundamentals of cloud computing in Theory and Practice*. J. Jiang, Ed. Amsterdam: Elsevier Syngress.

Ruhse, K.-U. 2012. Cloud Computing as an Integral Part of a Modern IT Strategy. *ISACA Jornal - Audit Process*. 3:6–9. Available: http://www.isaca.org/Journal/Past-Issues/2012/Volume-3/Pages/default.aspx.

Sabahi, F. 2011. Cloud Computing Security Threats and Responses. In *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference*. Xi'an: IEEE. 245–249. DOI: 10.1109/ICCSN.2011.6014715.

Sabharwal, N. & Wali, P. 2013. *Cloud Capacity Management*. New York, NY: Springer Science and Business Media.

Sachdeva, J.K. 2009. *Business Research Mathodology*. Mumbai: Himalaya Publishing House.

Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research methods for business students*. 5th ed. ed. London: Prentice Hall.

Smooth, S.R. & Tan, N.K. 2013. *Private Cloud Computing*. Waltham: Elsevier.

Sosinsky, B. 2011. *Cloud Computing Bible*. Indianapolis, IN: Wiley Publishing, Inc.

Speed, R. 2011. IT Governance and the Cloud: Principles and Practice for Governing Adoption of Cloud Computing. *ISACA Jornal - Governance, Tying Together the Three Lines of Defense*. 5:17–22. Available: http://www.isaca.org/Journal/Past-Issues/2011/Volume-5/Documents/11v5-IT-Governance-and-the-Cloud-Principles-and-Practice-for-Governing-Adoption-of-Cloud-Computing.pdf.

Steiner, T. 2012. *An Introduction to Securing a Cloud Environment*. Available: http://www.sans.org/reading-room/whitepapers/cloud/introduction-securing-cloud-environment-34052.

Surianarayanan, S. & Santhanam, T. 2012. Security Issues and Control Mechanisms in Cloud. In *Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference*. Dubai: IEEE. 74–76. DOI: 10.1109/ICCCTAM.2012.6488075.

Takabi, H., Joshi, J.B.D. & Ahn, G.-J. 2010. Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine*. 8:24–31. DOI: 10.1109/MSP.2010.186.

Tripathi, A. & Mishra, A. 2011. Cloud computing security considerations. In *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. Xi'an: IEEE. 1–5. DOI: 10.1109/ICSPCC.2011.6061557.

Wang, C., Qu, H.P. & Sheng, Z.Y. 2013. Cloud Computing Security Analysis and Reinforcement of Hadoop Environment. *Advanced Materials Research*. 709(1):646–649. DOI: 10.4028/www.scientific.net/AMR.709.646.

Wang, L., Ranjan, R., Chen, J. & Benatallah, B. 2012. *Cloud computing : methodology, systems, and applications*. Boca Raton, FL: CRC Press, c2012.

Wilhelmsen, C. & Ostrom, L.T. 2012. *Risk Assessment : Tools, Techniques, and Their Applications*. New Jersey: John Wiley & Sons.

Winkler, V. 2011. *Securing The Cloud - Cloud Computer Security Techniques and Techtics*. Waltham: Elsevier.

Zhang, X., Wuwong, N., Li, H. & Zhang, X. 2010. Information Security Risk Management Framework for the Cloud Computing Environments. In *2010 10th IEEE International Conference on Computer and Information Technology*. Bradford: IEEE. 1328–1334. DOI: 10.1109/CIT.2010.501.

Zissis, D. & Lekkas, D. 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*. 28(3):583–592. DOI: 10.1016/j.future.2010.12.006.