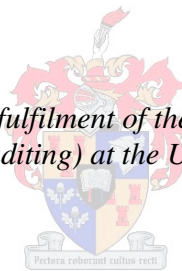


An investigation to determine incremental risks to software as a service from a user's perspective

by
Frederick Ferdinand Ipland

*Thesis presented in partial fulfilment of the requirements for the degree
MComm (Computer Auditing) at the University of Stellenbosch*



Supervisor: Mr LP Steenkamp
Faculty of Economic and Management Sciences
Department of Accounting

December 2011

Declaration

I, the undersigned, hereby declare that the work contained in this assignment is my original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Frederick Ferdinand Ipland

December 2011

Copyright © 2011 University of Stellenbosch

All rights reserved

Abstract

Software as a Service (SaaS) – which is a deployment model of cloud computing – is a developing trend in technology that brings with it new potential opportunities and consequently potential risk to enterprise. These incremental risks need to be identified in order to assist in risk management and therefore information technology (IT) governance.

IT governance is a cornerstone of enterprise-wide corporate governance. For many entities corporate governance has become a statutory requirement, due to the implementation of legislation such as Sarbanes-Oxley Act of the United States of America.

The research aims to assist in the IT governance of SaaS, by identifying risks and possible controls.

By means of an in-depth literature review, the study identified 30 key risks relating to the use and implementation of SaaS from the user's perspective. Different governance and risk frameworks were considered, including CobiT and The Risk IT Framework. In the extensive literature review, it was found that CobiT would be the most appropriate framework to use in this study. Mapping the risks and technologies from the user's perspective to one or more of the processes of the CobiT framework, the research found that not all processes were applicable. Merely 18 of 34 CobiT processes were applicable.

The study endeavoured to identify possible controls and safeguards for the risks identified. By using the technologies and risks that were mapped to the CobiT processes, a control framework was developed which included 11 key controls to possibly reduce, mitigate or accept the risks identified. Controls are merely incidental if it is not linked to a framework.

Opsomming

Software as a Service (SaaS) – ‘n ontplooiingsmodel van *cloud computing* – is ‘n ontwikkelende tegnologiese tendens wat verskeie moontlikhede, maar daarby ook verskeie risiko’s vir ondernemings inhou. Hierdie addisionele risiko’s moet geïdentifiseer word om te help met die bestuur van risiko’s en daarom ook die beheer van Informasie Tegnologie (IT).

IT beheer is ‘n belangrike deel van die grondslag van ondernemingswye korporatiewe beheer. As gevolg van die implimentering van wetgewing soos die Sarbanes-Oxley wetsontwerp van die Verenigde State van Amerika, het korporatiewe beheer ‘n statutêre vereiste geword vir verskeie ondernemings.

Hierdie studie poog om die IT beheer van SaaS by te staan, deur risiko’s en moontlike beheermaatreëls te identifiseer.

Deur middel van ‘n indiepte literatuur ondersoek het die studie 30 sleutelrisiko’s geïdentifiseer wat verband hou met die gebruik en implimentering van SaaS vanuit ‘n gebruikersoogpunt. Verskeie korporatiewe- en risiko raamwerke, insluitende CobiT en The Risk IT Framework, was oorweeg. Die literatuur ondersoek het egter bevind dat CobiT die mees toepaslikste raamwerk vir dié studie sal wees. Deur die risiko’s en tegnologieë vanuit ‘n gebruikers perspektief te laat pas met een of meer CobiT prosesse, het die navorsing bevind dat nie alle prosesse in CobiT van toepassing is nie. Slegs 18 van die 34 prosesse was van toepassing.

Die studie het ook gepoog om moontlike beheer- en voorsorgmaatreëls vir die risiko’s te identifiseer. Deur die tegnologieë en risiko’s te gebruik wat gepas is teen die CobiT prosesse, is ‘n beheer raamwerk ontwikkel wat 11 sleutel beheermaatreëls insluit, wat die geïdentifiseerde risiko’s kan verminder, temper of aanvaar. Beheermaatreëls is slegs bykomstig as dit nie direk aan ‘n raamwerk gekoppel is nie.

Table of Contents

Declaration.....	i
Abstract.....	ii
Opsomming.....	iii
Table of Contents.....	iv
List of Tables	v
List of Figures	vi
1. Introduction	1
1.1 Problem Statement	4
1.2 Aims and objectives	5
1.3 Methodology	6
1.4 Scope	8
1.5 Subsequent chapters.....	9
2. Background to SaaS, incremental risk and IT governance.....	10
2.1 Software as a Service and related technology.....	10
2.2 Control framework and IT governance	15
2.3 Risk in the context of the research performed.....	16
3. Literature review and prior studies	18
4. Research design and methodology.....	21
4.1 Investigation into SaaS	21
4.2 Identification of existing and possible risk relating to SaaS.....	22
4.3 Control framework evaluation and selection	23

4.4 Map technologies and risks to the selected framework.....	23
4.5 Investigation into possible controls and safeguards.....	24
5. Research findings	25
5.1 Investigation into SaaS	25
5.2 Risk identified by literature review	29
5.3 Framework selection	38
5.4 Identification of applicable CobiT processes to users of SaaS	42
5.5 Map risk to CobiT framework.....	48
5.6 Possible safeguards or controls.....	52
6. Conclusion and future research.....	74
6.1 Conclusion and findings	74
6.2 Future research	75
7. Bibliography	77
Appendix A – Glossary of terms.....	84
Appendix B –Common concepts and conventions used	85

List of Tables

Table 1 – Risk identified and description.....	30
Table 2 – Identification of applicable CobiT processes to users of SaaS	42
Table 3.1 – Risks relating to CobiT processes	49
Table 3.2 – Risks relating to CobiT processes (Continued)	50
Table 3.3 – Risks relating to CobiT processes (Continued)	51
Table 4 – Possible safeguards and controls for risks identified.....	55
Table 5 – Most significant controls identified to mitigate risk	72

List of Figures

Figure 1 – Research and conclusion methodology	7
Figure 2 – Illustrative description of the NIST definition of cloud computing (Ahmad & Janczewski, 2011: 2)	15
Figure 3 – SaaS Production Architecture (Al Zahir, 2011: 1)	28
Figure 4 – Processes most likely to be affected by risk relating to use and implementation of SaaS.	52

1. Introduction

“IT risk is business risk” (ISACA, 2009a: 7). According to Stoneburner, Goguen and Feringa (2002: 1) Information Technology (IT) risk is not a technical issue to be dealt with by IT departments, but an essential part of business management. Research conducted by Grant Thornton LLC (Nefdt, Miller, Spivack & McGee, 2011: 14) found that 39% of surveyed Software as a Service (SaaS) companies did not have formal risk management programs (or corporate governance frameworks).

SaaS – which is a deployment model of cloud computing – is a developing trend in technology that brings with it new potential risks and consequently potential opportunities to enterprises (Nefdt et al., 2011: 16). Incremental risks to business occur because of the natural progression or evolution of technologies, which may have a negative impact on business due to losses or missed opportunities. Cloud computing – and therefore SaaS – is a new technology, and brings with it the potential of high risk (ISACA, 2009c: 4). This is the reason why potential risk needs to be identified, in order to assist businesses in risk management and to grasp opportunities. Greg Hughes, Chief Strategy Officer, Symatec Corporation (2008: 2) expressed this best: “IT Risk Management is more than using technology to solve security problems. With proper planning and broad support, it can give an organization the confidence to innovate, using IT to outdistance competitors”. Jensen, Schwenk, Gruschka and Iacono (2009: 110) state that there is demand for an in-depth discussion as regards the requirement for cloud computing; they found that recent surveys on cloud security issues focussed on data confidentiality, safety and privacy.

Legislation on corporate governance – including the Sarbanes-Oxley Act of the United States of America and the King Code of Governance for South Africa 2009 (King III) report’s requirement for all listed companies on the Johannesburg Stock Exchange (JSE) – purports that corporate governance has become a statutory requirement. For all other companies in South Africa the King III report is on a “comply or explain” basis, in essence the company should comply

therewith, or document why it is unable to do so. The Institute of Directors of Southern Africa (2009: 6) state that there is a link between good corporate governance and statutory requirements; this is due to the legal duties which include fiduciary duties and the duty of care, skill and diligence. It notes further that IT is now being used as an enabler of business, which is so pervasive it mandates IT governance.

ITGI (2007: 5) states that some of the key cornerstones of an enterprise's governance includes the assurance about IT's value, IT risk management and controls surrounding information. IT governance incorporates and institutionalises good practice to guarantee that the enterprise's IT supports its business goals (ITGI, 2007: 5). According to ITGI (2007: 5) these goals require a framework of IT controls that matches the Committee of Sponsoring Organisations of the Treadway Commission's (COSO) Internal Control – Integrated framework; which is the most widely accepted control framework for enterprises. In addition thereto, data is distributed over different data centres and furthermore data-ownership and control is distributed in SaaS, which requires a different approach to data management, security and governance (Accenture, 2011: 5).

SaaS applications and software are accessed via the internet over a private or public domain by a web browser. Cloud Computing is a model for enabling convenient, on-demand network access to a shared infrastructure of configurable computing resources (e.g., servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes accessibility and is composed of five essential characteristics:

- On-demand self-service
- Wide-ranging network access
- Resource amalgamation
- Rapid elasticity
- Measured service

This is also based on three delivery models:

- SaaS
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Cloud computing can be deployed as a private cloud, community cloud, public cloud and a hybrid cloud (Mell & Grance, 2009: 1). This is further discussed in section 2.1. Cloud computing is further described and discussed in section 2.1. The definition of SaaS accepted for this study is that SaaS is the delivery of software or an application by a provider(s) over a network (Internet or intranet) for a pay per use or fixed per user rental fee and is accessed by a web browser. Refer to sections 2.1 and 4.1 for further discussions relating to SaaS and its definition.

The use of SaaS creates value by reducing costs of infrastructure investment and costs relating to software purchase, delivery time, agility and integration. SaaS will assist organisations to accomplish the future's tasks today, securing IT's role as an imperative for future success and growth (Accenture, 2011: 9). IT departments will be able to shift their focus from development and support to managing the services, which should provide more value as services can be aligned to business goals (Carraro & Chong, 2006). A significant advantage that SaaS has over perpetual licence software is that the provider can include updates and software enhancements as soon as it becomes available, in stark contrast to the decision by customers only to upgrade software once significant improvement is available (Choudhary, 2007a: 143).

Some of the risks identified and discussed in section 5.2 include opt-out risk, risk of data theft and data loss, business continuity risk etc. According to Nefdt et al. (2011: 7) there exists a lack of assessable information regarding the quality, magnitude and mitigation of risks relating to SaaS. Academic literature on SaaS has focused mostly on the pricing model (Choudhary, 2007a: 143).

The purpose of this study is to investigate incremental risk relating to the use or implementation of SaaS technology in an enterprise. Increment is defined as an increase, which could often be barely perceptible (Encarta Dictionary, 2011: 1). Risk in the context of this study includes the loss of opportunities for an enterprise or a negative impact on an enterprise. The evaluation of these risks will be performed by using internationally accepted frameworks. The study intends to recommend possible safeguards to identified risks, thereby developing a control framework for SaaS customers for integration into their enterprises overall corporate and IT governance framework. According to Accenture (2011: 14) enterprise architecture was historically created in an attempt for 100% security; however this must give way to a cascaded reactive security approach when implementing cloud solutions, including SaaS.

The remainder of this chapter is grouped as follows: The problem statement which identifies the necessity of the study along with the motivation thereof; from there the goals and purpose of the study is described. The remaining sections define the scope and methodology used in the study.

1.1 Problem Statement

The benefits arising from SaaS are widely available, as documented by some, including ISACA (2009c: 6); Jensen et al. (2009: 109); Petri (2010: 15, 20); Choudhary (2007b: 1); Benlian, Hess and Buxman (2009: 357) and Carraro and Chong (2006); however only limited risks or risk relating to specific aspects (such as service level agreement risk) have been identified. These risks relating to SaaS and the risks to related technologies were identified in texts such as Putri and Mganga (2011: 31); ISACA (2009c: 7); Rudman (2010: 3260); Walsh (2009: 7) & Raval (2010: 3). There is a need in the SaaS sector to quantify risks relating to SaaS (Nefdt et al., 2011: 1).

New technologies, such as SaaS, create incremental IT risks that affect businesses directly and should therefore be identified and managed. It is clear that the adoption or use of SaaS could lead to total enterprise failure, if the risks are not controlled or mitigated. This is due to the

reliance on the solution provider, which is one of many security concerns for possible customers. Many enterprises wish to implement SaaS, but are too concerned about the security issues relating to SaaS (Shey et al., cited in Subashini & Kavitha, 2010: 3). Feng, Chen and Liu (2010: 1) states that cloud computing security measures require more than those of conventional security measures.

Furthermore few safeguards and controls have been identified or developed in relation to the risks identified; some publications include Putri and Mganga (2010) and Raval (2010). The study aims to develop controls and safeguards for the risks identified, by linking the risks to a selected framework and developing controls from the framework. By linking the controls to the risks, a framework to govern risk could be developed.

1.2 Aims and objectives

The purpose of this study is to evaluate the most significant incremental risks for users of SaaS. Users of SaaS are the enterprises and people that make use of the software that is delivered to them by the solution provider. Enterprises that understand the incremental risks relating to SaaS will be able to adapt in order to mitigate these risks and to fulfil the full potential of implementing or using SaaS in their business.

It is not the purpose of the study to attempt to identify all risks relating to SaaS; therefore the risks identified cannot be used as a full, complete or comprehensive generic list of incremental risks. The users should assess whether all risks identified apply to them and whether other risks may also exist. The study will attempt to impose the importance of risks (relating to any facet of an enterprise), as noted by research conducted by Nefdt et al. (2011: 3): “In our work across industries, we have found that many companies do not appreciate how crucial it is to address and manage compliance risk “. The study will not pursue a definition of incremental risk relating to SaaS as it is a subjective observation.

The study will attempt to act as a catalyst for enterprises to assess whether SaaS may be a viable option for implementation into their enterprise. It may contribute to due diligence reporting, to assess whether SaaS should be adopted by an enterprise. From a client's perspective, the purchase of perpetual software licence and hardware investment becomes a sunk cost, which makes the investigation and adoption of SaaS a more attractive business decision (Choudhary, 2007a: 145). The study could aid enterprises that have implemented SaaS to update their risk management processes and assist in deploying a risk management process, if none exist. It may also assist internal and external auditors in identifying significant audit risks (when performing risk assessment procedures). As Nefdt et al. (2011: 2) state, very little research has been conducted regarding the quality, magnitude and mitigation of risks relating to SaaS.

Guidance will also be provided in this study, based on a widely accepted framework(s), such as Control Objectives for Information and related Technology (CobiT), Risk IT and Enterprise Value: Governance of IT investments (Val IT) on how to manage the risks identified. The safeguards and controls identified in this framework cannot be accepted as complete, but rather as a baseline or checklist, as each type of risk response – and even risk itself – is unique to a situation, organisation or risk management.

1.3 Methodology

The study combined two research methods; firstly an extensive literature review was performed to define SaaS, to identify risks relating to SaaS and to identify a framework to assess risks. Refer to Chapters 3, 4 and Table 1 in section 5.2 for more details on this review. Secondly the information obtained relating to SaaS technologies and risks were analysed in the selected control framework (refer Table 2 in section 5.4), in order to map the technology to the framework. The literature review identified sources relating to the technologies of SaaS, risks identified in SaaS and whether safeguards have been identified.

For a complete review of literature on SaaS, other technologies were also considered, such as cloud computing and furthermore technologies that share some of the features of SaaS, such as Web 2.0 (Wang, Von Laszewski, Younge & He, 2008: 138). Risks identified from the literature review will be evaluated by mapping SaaS technologies against existing internationally accepted best practice frameworks. Mapping entails the allocation of technologies and risks to the most applicable process in the framework. SaaS in itself cannot be mapped against these frameworks; only the specific technology used for SaaS can be mapped against the processes in a framework.

An in-depth review of control frameworks available was performed, resulted in the most widely accepted framework to be identified, is noted in section 5.3. The research is focused on the users of SaaS, therefore only technology and risks relating / applicable to the users will be considered. Finally recommended controls and safeguards for identified risks were devised in a framework, linking the control or safeguard to the framework's process, as described in Table 4 of section 5.6.

The following diagram depicts the process, from risk identification to developing possible controls and safeguards:

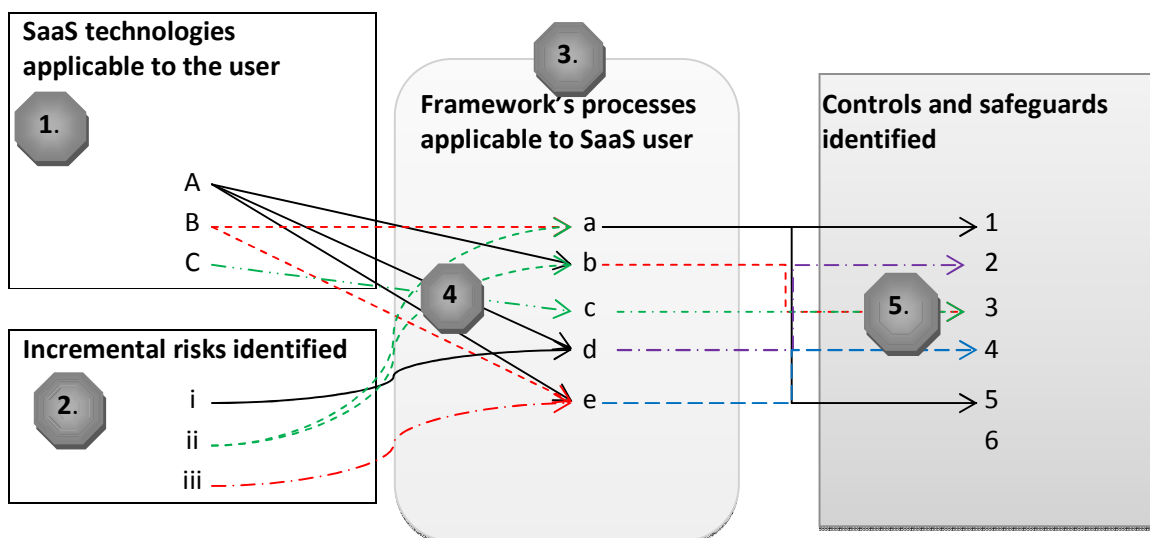


Figure 1 – Research and conclusion methodology

The figure illustrates that from step 1: The research on SaaS and the technology relating thereto, is mapped to the process. Step 2 was the research conducted into existing risks identified relating to SaaS and related technologies. Step 3 evaluates which processes are applicable (Table 2, section 5.4). The risks applicable are then mapped to the process in step 4 (Table 3.1 – 3.3, section 5.5). Lastly controls can be designed based on the framework selected (Table 4, section 5.6). This process maps the technology and the risk to the applicable control to prevent, detect or correct risk (step 5). It is also clear from the figure that some technologies and risks affect more than one process and that some controls are applicable to more than one process.

1.4 Scope

The research is focused on the users of SaaS; however some of the risks may be shared with the solution providers. The risks identified were based specifically on incremental risks, however this list cannot be regarded as a complete list and each enterprise should evaluate if all the identified risks apply, or whether additional risks may exist. As mentioned, incremental risks to business occur because of the natural progression or evolution of technologies, which increase the frequency and magnitude of IT risk. Furthermore, SaaS has been selected for evaluation in this study, as it is an up and coming trend (Nefdt et al., 2011: 2).

To define SaaS and its related technologies, it was first necessary to investigate cloud computing. Several definitions were identified for cloud computing. The SaaS platform of cloud computing was selected due to the surge of interest in SaaS which is owing to macroeconomic circumstances that have put pressure on enterprises to cut spending (Accenture, 2009: 3).

Several well-known entities have implemented SaaS, including Citigroup (Accenture, 2009: 10). Other well-known entities are campaigning for the adoption of SaaS, such as Salesforce.com, 3Tera, Microsoft, and Amazon (Pervez, Lee & Lee, 2010: 214).

SaaS can be deployed in public, private or hybrid clouds. The study did not attempt to differentiate, however the risks identified are more applicable to a public or hybrid cloud, due to the increased risk of public and hybrid deployment models.

1.5 Subsequent chapters

The research study continues with Chapter 2, which contains a description and background to SaaS, a discussion on incremental risk and an overview of IT governance. These 3 sections are the foundation of the research. Chapter 3 includes the literature review and prior studies concluded on SaaS. The literature review contains risk relating to SaaS and available IT governance frameworks to address these risks. Chapter 4 documents the research design and methodology in detail. Divided into 5 sections it first addresses how SaaS will be defined, and the process of identifying risks, thereafter how the IT governance framework will be selected, mapping SaaS technologies to the selected framework and lastly how controls and safeguards will be identified. Chapter 5 documents the research findings, in the same order as Chapter 4, with an additional table that maps the risk to the processes applicable in the framework. Chapter 6 contains the conclusion and identifies possible future research.

2. Background to SaaS, incremental risk and IT governance

This chapter endeavours to give the reader of the subject matter a broad understanding of the three core elements that were used to reach the conclusion, which include the risks and controls identified. The chapter will not focus on the technical aspects of these core elements, but will rather give a wide description.

2.1 Software as a Service and related technology

To define SaaS and its related technologies, it was first necessary to investigate cloud computing, as SaaS is a component of cloud computing. Several definitions were identified, some of which included:

- Accenture (2009: 4) who define cloud computing as IT capabilities over a network;
- Wang et al. (2008: 138) who define cloud computing as a set of network enabled services, which may be accessed pervasively; and
- Subashini and Kavitha (2010: 1) who define cloud computing as an alternative way to invest in capacity and capability, without investment in physical infrastructure.

This range of definitions for cloud computing is further underlined by IBM (2010: 2), Feng et al. (2010: 1) and Ahmad and Janczewski (2011: 1) in that there are different opinions of what cloud computing is. However, the definition that is widely accepted was developed by the National Institute of Standards and Technology (NIST) (Ahmad & Janczewski, 2011: 1; Petri, 2010: 5 & ISACA, 2009c: 4). The summarized NIST definition is as follows: Cloud Computing is a model for enabling convenient, on-demand network access to a shared infrastructure of configurable computing resources (e.g., servers, storage, applications, and services) that can rapidly be provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes accessibility and is composed of five essential characteristics:

- On-demand self-service;
- Wide-ranging network access;
- Resource amalgamation;
- Rapid elasticity;
- Measured Service.

This is also based on three service models:

- SaaS,
- Platform as a Service (PaaS), and
- Infrastructure as a Service (IaaS).

Cloud computing can be deployed as a private cloud, community cloud, public cloud and a hybrid cloud (Mell & Grance, 2009: 2 & Petri, 2010: 6). In a private cloud the infrastructure is deployed only for a single organisation, over an enterprise's intranet. The organisation normally owns the infrastructure, whether it is on or off the premises or externally managed (Petri, 2010: 9; IBM, 2010: 3 & PricewaterhouseCoopers, 2010: 14). The opposite is true for a public cloud, where the cloud is accessed over the internet and the client and provider are two different organisations and the ownership of infrastructure is with the provider (Petri, 2010: 9; IBM, 2010: 4 & PricewaterhouseCoopers, 2010: 14). In a community cloud, the cloud infrastructure is shared by several enterprises and supports a specific community (Putri & Mganga, 2011: 13). Lastly a hybrid cloud may contain multiple public and private clouds; multiple clients and providers will most likely be supplied in a multi-tenant infrastructure (IBM, 2010: 4 & Putri & Mganga, 2010: 14). Fishteyn (2009: 1) describes a multi-tenant infrastructure as "one that uses common resources and a single instance of both the object code of an application as well as the underlying database to support multiple customers simultaneously".

Due to the fact that SaaS is a deployment model of cloud computing, it was expected not to find a universal definition for it. The media has also labelled SaaS with a variety of names,

including on-demand computing, seamless computing and adaptive computing (Choudhary, 2007a: 142). In this study, SaaS is accepted as the most commonly used term. Nefdt et al. (2011: 2) states that the lack of clear criteria to define SaaS opened the door for solution providers to host widely different solutions and market these as SaaS. Several different descriptions for SaaS have been identified.

These definitions for SaaS include:

- Carraro and Chong (2006): a hosted service which is accessed via the internet.
- Pervez et al. (2010: 214): business functionality delivered by a network as a service.
- Petri (2010: 11): the capability to use a provider's applications, which are cloud based.
- IBM (2010: 7): an application delivered via a cloud where multiple enterprises share the single application and the provider implements virtualisation technologies to ensure security and data privacy.
- Putri and Mganga (2011: 11): renting a suppliers software over a network, where the provider runs the application in a multi-tenant infrastructure.
- Sääksjärvi, Lassila and Nordström (2005: 177): SaaS is time and location independent, allows for multi-tenancy by the provider, has greater economy of scale and allows for continues innovation of software.
- Kang, Myung, Yeon, Ha, Cho, Chung and Lee (2010: 338): have a similar definition as Sääksjärvi et al. (2005: 177) with the addition that the software may be owned by more than one provider.
- The Cloud Security Alliance (2009, 15): capabilities supplied to the SaaS user, accessed through thin client services that are web browser enabled.
- Wang et al. (2008: 139): software or applications that is hosted by the provider and accessed by the client over the internet.
- Choudhary (2007a: 142): offers a subscription model where the upgrades of the software is free and performed by the provider, in contrast to perpetual licencing that has a once-off purchase price and may have additional payment requirements for updates.

The definitions for SaaS share key denominators. This research does not attempt to define SaaS, for this reason the most common denominators were accepted. Therefore, the definitions accepted for this study are:

- that SaaS is the delivery of software or an application,
- by a provider(s),
- over a network (internet or intranet),
- for a pay per use or fixed per user rental fee,
- which is accessed by a web browser.

The costing system is one of many advantages to SaaS. Some of the other benefits to SaaS include, but is not limited to (ISACA, 2009c: 6; Petri, 2010: 14; Carraro & Chong, 2006):

- Cost management – This includes scalability without initial investment, cost prediction and optimal use management (especially in the event of fixed price per user). It allows for accurate prediction of costs, with the reduced risk of variance.
- Cash-flow management – Enterprises can predict the monthly fee in advance and allow sufficient cash to be available, as well as lower fixed initial investment cost (which normally needs to be financed).
- Immediate deployment – Faster implementation to value delivery.
- Availability – The service is always available, from anywhere in the world and can be accessed by various connections (i.e. fixed line or wirelessly).
- Scalability – Providers can give unconstrained capacity, which means a business' growth will not be limited to IT-investment.
- Efficiency – Data is less likely to be duplicated, information can be shared throughout the enterprise which may result in more innovation, which leads to business growth.
- Resiliency – Providers utilise mirrored solutions; in the event of a natural or other disaster, the service could continue unaffected.
- Resource pooling – The provider dedicates all resources to providing the solutions, which may be better than the resources which the client could afford to implement or would have implemented.

All these benefits vary between the solution-provider selected.

As IaaS and PaaS are not covered in this research a brief description follows, to enable the reader to differentiate the 3 deployment models (IBM, 2010: 7; Putri & Mganga, 2011: 12; Briscoe & Marinos, 2009: 3):

- IaaS – Infrastructure offered by a virtual machine to allow access to infrastructure services, servers and storage and clients are billed for amount of resources used. These essentially behave like dedicated servers for the customer.
- PaaS – The provider leases access of their platform for the users to run their own software from, in essence renting of processing power.

In this study the term user and client is used interchangeably. The user is the enterprise or person that uses the software deployed by a solution provider; therefore the solution provider delivers the software, application and other software related services (such as email). The customer refers to an enterprise's users.

The following figure depicts Cloud computing graphically, indicating the 3 delivery models, the deployment models and the essential characteristics per the NIST definition of cloud computing (Mell & Grance, 2009: 1):

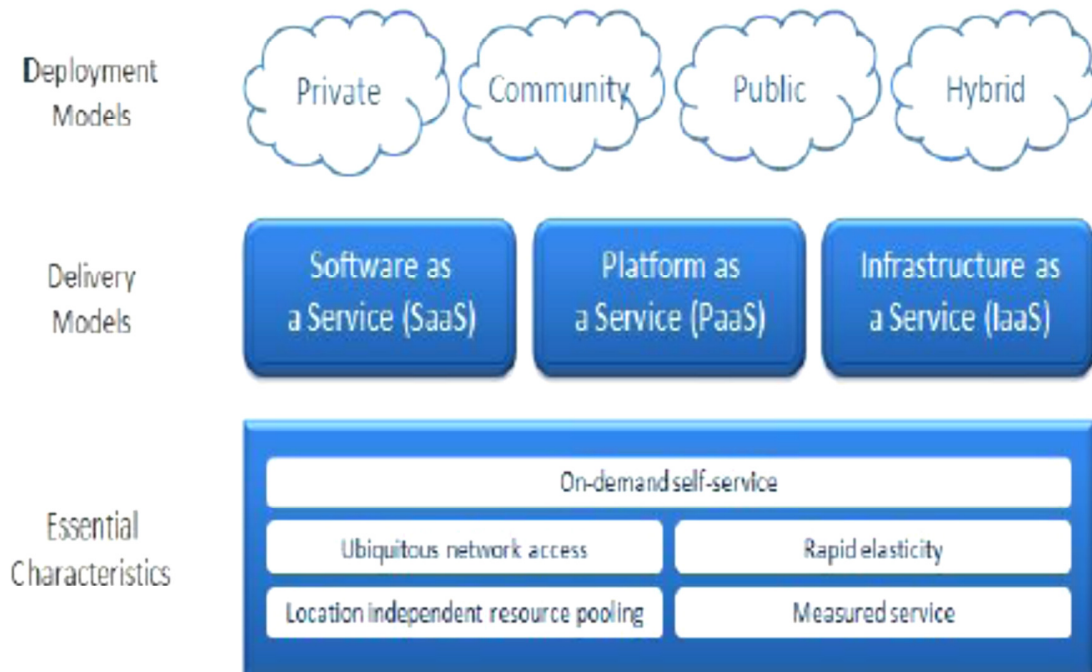


Figure 2 – Illustrative description of the NIST definition of cloud computing (Ahmad & Janczewski, 2011: 2)

2.2 Control framework and IT governance

Governance is the responsibility of good practices by the board and executive management. This includes the system of balances and checks to ensure that those charged with governance add long-term value to the shareholders of an enterprise. IT governance falls within the realm of overall governance, as IT risk has an impact on the entire enterprise. This is best summarised by ISACA (2009a: 7) stating that “IT risk is business risk”. Therefore, the governance of all IT processes is critical to ensure value delivery to the enterprise (Kieviet, 2006: 3).

As with all aspect of governance, the governance should be implemented using an acceptable framework. According to Rudman (2010: 3251), the implementation of controls on their own is

merely *ad hoc* if these controls are not linked to a proper control framework. Therefore an investigation into acceptable frameworks was concluded in this study.

The frameworks considered were identified by the literature review (discussed in Chapter 3) and research into possible acceptable frameworks for IT governance and controls.

2.3 Risk in the context of the research performed

A lack of corporate governance automatically increases risk in an enterprise. Therefore a lack of IT governance increases risk in an enterprise. From this analogy it is argued that an enterprise needs IT governance and should implement sufficient controls to mitigate and reduce risk.

IT risk is part of the overall business risks to which an enterprise is subject to (ISACA, 2009b: 11). IT risk differs between every enterprise due to the fact that each enterprise has different risk appetite and risk tolerance. ISACA (2009b: 15) defines risk appetite as the overall risk which an enterprise will accept to pursue its mission. This is impacted by the enterprise's ability and capacity to absorb losses and the risk-taking culture embedded in the enterprise. Risk tolerance is defined as the variation from the risk appetite to achieve a specific target. The IT risk is further affected by the frequency and the magnitude of the risk (ISACA, 2009b: 12). Frequency is defined as the "number of times an event occurs in a given time period" (ISACA, 2009b: 37).

From the research conducted, it is clear that risk differs substantially between enterprises. It is also concluded that IT risk differs; for instance where IT is a business imperative, IT affects all components of the enterprise, in comparison to a small business where IT is limited to a stand-alone computer for capturing invoices. Incremental risk is not defined in this study; it includes not only additional risk, but it includes significantly increased risk due to greater magnitude or frequency of a risk event.

Based on the overview of SaaS, control frameworks and risk, an extensive literature review on SaaS, frameworks available and risks were conducted. This is discussed in more detail in Chapter 3.

3. Literature review and prior studies

An extensive literature review was performed on SaaS and other technologies that share technological characteristics of SaaS as well as prior research conducted on SaaS and risks relating to SaaS. An in-depth literature review was also performed on possible control frameworks available to evaluate which framework would be acceptable for the purposes of this study; including Smit (2009); Kieviet (2006); Sherry (2007); Rudman (2010) and Putri and Mganga (2011). Lastly, an investigation was conducted on possible safeguards and control measures to prevent, detect or correct the risks identified, in accordance with a framework.

Resulting from extensive literature used in this study it is deduced that there are many articles detailing the risks of SaaS, however these articles were mostly based on general assumptions and observations (in essence not scientifically approached) or were in relation to a specific aspect of SaaS. It is noted that literature regarding the aspects of risk to cloud computing was found, but that these studies also focussed on specific identified risks and the impact thereof, especially security risks.

Not all literature reviewed in this study is discussed in this section, as some sources shared basic concepts as the literature chosen for the discussion below.

Literature used in this study relating to SaaS risk:

1. A study conducted by Grant Thornton LLC, utilising questionnaires issued to vendors and executives. The study groups risk relating to SaaS in financial, operating and compliance risk. The study identifies what respondents view as the most significant threats (Nefdt et al., 2011). The study was performed based on surveys of companies, SaaS clients and SaaS solution providers.
2. Subashini and Kavitha (2010) conducted a study focussing specifically on security issues relating to SaaS, PaaS and IaaS.

3. Fishteyn (2009) released a white paper on the challenges of implementing SaaS. This white paper did not list risks directly; however Aubert, Patry, and Rivard (1998: 3) noted that non-compliance of implementation can fall within the sphere of risk.
4. An article published on Network World magazine listed some hidden risks, these were mostly relating to Service Level Agreements (SLA's) and data integrity risks (Thompson, H.H., 2006).
5. Putri and Mganga (2011) conducted an in-depth literature review on risks relating to SaaS, which yielded good insight into possible risks, but the risks were once again limited to SLA's.
6. Carraro and Chong (2006) published an article in general of SaaS. The article included what SaaS is in general terms, what the benefits are, risks and possible architecture.
7. ISACA (2009c) is a white paper discussing the benefits to business when implementing good governance and security to cloud computing, documenting some possible risks.
8. Web 2.0 and Virtual Private Networks (VPN) share some of the technological characteristics of SaaS (Refer to section 5.1 for further discussion); therefore research conducted on risks to Web 2.0 and VPN's were investigated to identify further possible risks (Rudman, 2010; Sherry, 2007).

From the literature review it was found that research, both scientific and non-scientific exists about SaaS. The focus seems to be on what SaaS actually is; what business model is most suitable for SaaS (Choudhary, 2007b: 1); general discussion papers of SaaS or review into specific risks such as service level agreements (SLA) or data risk. It is therefore deduced that an opportunity exposed itself to review the overall risk relating to SaaS.

Literature relating to the use of Control Objectives for Information and related Technology (CobiT) to evaluate risks and governance:

1. Sherry (2007) conducted research as to whether it is possible to use the CobiT framework to identify risks relating to a Virtual Private Network (VPN). Sherry (2007: 50) established: "It was concluded that the CobiT framework is a suitable evaluation tool to

assist in the governance of VPN's, as all VPN risks identified could be associated with a CobiT control objective".

2. Rudman (2009) applied CobiT to Incremental risks relating to Web 2.0 applications and found CobiT to be suitable for the evaluation of risks.
3. Putri and Mganga (2011) conducted an in-depth literature review on possible framework to evaluate risks in SaaS; they found that CobiT was the most useful framework after completing a criteria evaluation of 8 possible frameworks identified.
4. Kieviet (2006) applied CobiT in an enterprise resource environment to evaluate whether it may be used as a governance and control model.
5. Smit (2009) attempted to use CobiT to reduce the gap between management's goals and IT goals (referred to as the IT gap).
6. No research could be identified that used the Risk IT Framework in a scientific study or a study that verified that the framework is acceptable in IT governance.

This study's aim was not to investigate whether a specific framework would work in the SaaS environment, rather which control framework could assist in the identification of risk and the implementation of controls to mitigate, prevent or detect those risks.

The literature review further underlined the necessity for a study on overall risks for the SaaS user, in the context of IT governance and the possible identification of controls and safeguards to prevent, detect and / or correct the risks identified.

The following section documents the process and procedures followed in the study in order to achieve the findings of Chapter 5 and finally the conclusion in Chapter 6.

4. Research design and methodology

This chapter of the research will depict and explain the research approach. It will also illustrate how the literature review and evaluation thereof against the selected framework will assist in the conclusions drawn as well as other findings made in this study. The Chapter describes how SaaS will be researched, followed by the risk identification methodology. Thereafter the control framework consideration, evaluation and selection are discussed and how SaaS will be mapped to this framework. Lastly, this chapter will describe how possible controls will be developed based on the framework selected.

4.1 Investigation into SaaS

An extensive literature review was performed to identify what SaaS is, including an identification of other technologies that share the same characteristics as SaaS. Possible risks relating to SaaS have been identified by prior research on SaaS and the technologies thereto, however other risks established from the literature review on technologies related to SaaS will also be included.

SaaS is a delivery model of cloud computing, which has two other delivery models commonly accepted as IaaS and PaaS. The research investigated whether there is a possible definition of SaaS accepted across the board. Technologies related to SaaS were identified and noted; this included a review of possible architectures for SaaS deployment, possible software used and also the users involved. The research will not be conducted on a highly technical level into the technologies of SaaS, but rather as an overview of technologies in order to assist in the mapping of SaaS to the selected framework, as will be discussed in section 4.4.

4.2 Identification of existing and possible risk relating to SaaS

An extensive literature review was performed to identify risks relating to SaaS, cloud computing and other technologies that may share the same or some of the same characteristics. From the literature review and further research conducted on prior risk identification a list of risks were developed from the studies performed. From these studies the risks applicable only to SaaS were documented. The research found that many of the research articles had overlapping risks which shared the same characteristics. In order to condense these risks, the common denominator of each risk was documented (from the literature review). Section 5.2 illustrates the abbreviated list of risks and their detailed descriptions from the research. The detailed description of the risk indicates the original reference to all sources and the applicable definition of the risk.

The study has not indicated frequency or magnitude of the risks identified, it is up to the user of the framework to evaluate whether the risk applies to its environment and thereafter what the impact and magnitude of the risks could be. This evaluation of the risks would assist management in deciding what controls, if any, should be implemented. Well implemented and monitored IT risk management practices will provide business opportunities while decreasing risks to which an entity is susceptible (ISACA, 2009a: 31). Magnitude and impact in terms of The Risk IT Framework (Risk IT) is defined as: “A measure of the potential severity of loss or the potential gain from a realised IT-related event” (ISACA, 2009a: 101).

Some risks were not specifically identified from the extensive literature review, these were identified by the use of the control framework or other sources of information and research not linked to a particular source.

4.3 Control framework evaluation and selection

Ahmad and Janczewski (2011: 2) defines IT governance in cloud computing as “the governance of application, services and processes between the two main entities; user and provider, by creating a balance between the shared set of responsibilities and liabilities for better control and accountability to sustain governance”.

A literature review on control frameworks was performed to identify the most used and widely accepted framework to implement, which may be used to evaluate and control risk. Several frameworks were identified; however only the frameworks considered for this study will be listed in Chapter 5. The framework selection was based solely on the acceptability thereof in prior studies. The framework selected is discussed in section 5.3.

4.4 Map technologies and risks to the selected framework

In order to ascertain which processes in the framework are applicable, it was necessary to map the technologies deployed in SaaS to the associated control objectives. Only the technologies deployed in SaaS can be mapped against the selected framework (Rudman, 2009: 211).

After the investigation into SaaS is completed in section 5.1 and the technologies identified, a table will be created listing all 34 processes included in CobiT, with 3 criteria ranges to evaluate whether the control objective is applicable.

The 3 criteria will include mapping SaaS technologies to CobiT, to evaluate whether the process is applicable to the technology; consideration whether the process has relevance to the SaaS client / user or to the solution provider; lastly it will consider whether there is a possible risk explicitly to the SaaS user. If all these are present, it can be assumed that the process is relevant to this study. The 34 processes, criteria and findings are documented in Table 2 (Section 5.4).

Subsequent to Table 2 (Section 5.4), the processes are described in a very brief matter. Where the process was considered not to be applicable to the SaaS user, the reason for this is included in the description of the process. This way the reader can familiarise him / herself with the thought process in the evaluation.

The risks identified (based on the condensed description) were then allocated to the framework's selected process(es) that could be affected. The risk identified will be evaluated based on the most likely impact of the risk as defined, as all risk impact a process, but not all processes are impacted by all risks. Most risks identified affected more than one of the processes of the framework.

4.5 Investigation into possible controls and safeguards

Possible safeguards were identified during the extensive literature review performed; however some of the controls identified were in relation to cloud computing as a whole or to the related technologies identified in Web 2.0 and VPN's etcetera. Not all of these identified controls are applicable to the client or user in the SaaS environment.

The controls to be implemented relate to section 4.2, the selection of a control framework. As mentioned before in this study, Rudman (2010: 3251) deduced that general controls that are not linked to a framework will be insufficient. Therefore the control or safeguard identified was developed based on the relation the risk had to the framework's identified process, in essence the process to which the risk relates was linked to the framework's controls. Subsequent to mapping the technologies of SaaS to the selected framework, the risks can also be mapped to the process it is most likely to affect. The framework selected will have guidance on possible controls to be implemented.

Chapter 5 documents the findings of the methodology followed.

5. Research findings

This chapter presents the research findings. It follows the same order as chapter 4's research design and methodology, however it distinguishes the evaluation of applicable processes and the risks mapped to the selected framework.

Section 5.1 documents the technical aspects behind SaaS, including a possible architectural outlay thereof (figure 3). Section 5.2 documents the literature review findings on the risks. Section 5.3 documents the frameworks considered followed by the evaluation of applicable processes. Section 5.5 links the risks identified in section 5.2 to the applicable processes, followed by safeguards identified from the framework.

5.1 Investigation into SaaS

The investigation was not concerned by the detail or technical technologies deployed in SaaS; it focused more on the overall elements included in the model, in order to evaluate the technologies against the selected control model. Risk cannot be evaluated without an overall understanding of these technologies. Furthermore the research was conducted from the perspective of the client, which – from the discussion below – will indicate that the provider implements and maintains most of the technologies used in SaaS.

The solution provider will design the SaaS architecture; this entails that the client is unaware of the technical architecture applied. The provider's architecture is influenced by factors such as the number, nature and needs of tenants – which are a cluster of clients, such as the various enterprises that use the service, but this may be subdivided to control data and other access within such an organisation (Chong, Carraro & Wolter, 2006). The user does however have different access paths to the cloud services. Jensen et al. (2009: 109) documented that there are two main technologies employed, web servers are commonly used for IaaS, whereas SaaS users use web browsers. PaaS on the other hand uses a combination of both these

technologies. This is an important differential, as it has an impact on the risks and controls affecting the user.

There are different methods of data division and access segregation by the service provider. Data can be segregated by storing it in separate databases; another method is having multiple tenants share the same database, with data-tables separating tenants; a third approach is to share the database and tables, but to include a user ID in the table (Chong et al., 2006) by virtualisation, which is the partitioning of hardware by the solution provider (Wang et al., 2008: 142). The providers implement virtualisation technology in order to partition hardware between tenants and allowing the multi-tenant architecture to exist. The techniques used include VMware and Xen (Wang et al., 2008: 142).

To implement the web services, the service providers implement Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP) and Universal Description, Discovery, and Integration (UDDI) (Wang et al., 2008: 142).

WSDL is an Extensible Markup Language (XML) which is a base to describe the services offered by the provider, by way of electronic access (Kooi, 2001) and what functions the enterprise or individual client can use. XML is a flexible way to create shared information formats and share the information on the World Wide Web (WWW) and intranets (Doszkocs, Hill, Lindgren & Yashinsky, 2001).

SOAP is the communication integrator between different programmes via the WWW, by using the WWW's Hypertext Transfer Protocol (HTTP) (Sivaram, 2000). HTTP is a protocol for the transfer of files on the WWW. HTTP is an application protocol which runs on Transmission Control Protocol/Internet Protocol (TCP/IP) (HTTP, 2000). TCP/IP is the basic communication protocol of the internet (TCP/IP, 2000).

UDDI is an XML-based registry for all enterprises in the world, in order to streamline transaction and set a standard protocol for their internet communication (UDDI, 2000).

The software is hosted by the provider over the internet with data stored centrally or distributed. There is an integration architectural structure, where external data may be accessed by the software and integrated into the logical infrastructure of the provider in order to interoperate the service and the data (Carraro & Chong, 2006). For data to be integrated, it will need to be synchronised by an integration broker. An integration broker unifies internal and external data as a whole (Carraro & Chong, 2006).

The SaaS user interface uses a standard web browser application (which comes standard on most operating systems), which is based on standardised protocols such as the HTTP-protocol (Cusumano, 2010: 28). Jensen et al. (2009: 112) documents that web browsers use techniques such as Asynchronous JavaScript and XML (AJAX). The user is all case in point a thin client of the cloud. The cloud application or software can be accessed in a variety of ways, whether it is with a desktop computer, laptop or handheld device. Jensen et al. (2009: 112) depicts the user interface as mere authentication and authorising device, with inputs and outputs to the solution provider.

The following is an illustration of possible outlay of SaaS architecture:

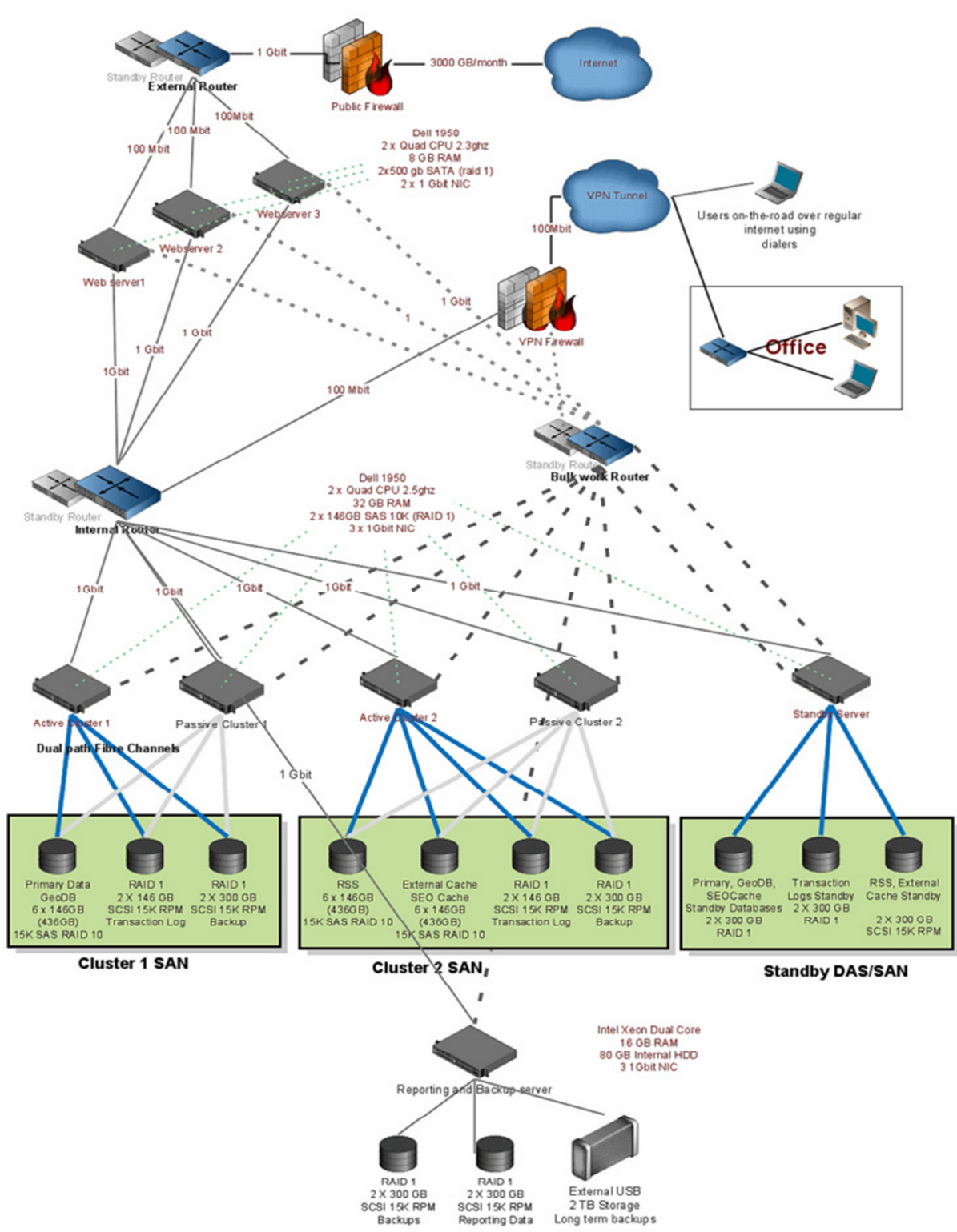


Figure 3 – SaaS Production Architecture (Al Zahir, 2011: 1)

From the illustrating figure, the user's technological resources are fairly simple, as it only needs network access and a web browser.

5.2 Risk identified by literature review

Many risks were identified during the extensive literature review performed. The risks identified had specific relation to SaaS and some had an indirect relation to SaaS, such as to cloud computing, VPN's and Web 2.0 technology. The multi-tenant deployment model is often used in Web 2.0 development, in which applications facilitate the sharing of information from different data sources (Fishteyn, 2009: 1; Jensen et al., 2009: 112). Therefore risks identified by research into Web 2.0 may be used. Virtualisation technologies are also applied to VPN's to allow access to cloud services (Wang et al., 2008: 138). Therefore some of the risks identified by prior VPN research may be used.

The risks identified will be discussed below. Section 5.3 illustrates the risk in relation to CobiT's processes. Table 2 (section 5.3) contains an evaluation of which processes are applicable to this study, but this will be expanded in section 5.3.

The table below lists the shortened description of the risk (for use in the mapping section 5.3), a detailed description of the risk and the source(s) of the risk identified. These risks are the incremental risks to enterprises using and / or adopting SaaS. The risks were ordered alphabetically and not in relation to possible impact or magnitude. Risks identified from general information will be marked with an asterisk.

Table 1 – Risk identified and description

No	Abbreviated Description	Detail of the risk	Original source
1	Audit difficulty	<ul style="list-style-type: none"> • The risk that an enterprise cannot be audited or restrictions to the data or audit trail exist. 	Putri and Mganga, 2011: 57
2	Business continuity / backup risk	<p>This risk includes:</p> <ul style="list-style-type: none"> • Unavailability of the service or unavailability of data due to loss in connection. • Improper backup of data in the event of data loss. • Risk over the solution provider going out of business. • Risk of data loss due to multi-tenancy architecture collapse. 	Putri and Mganga, 2011: 56; ISACA, 2009c: 7; Rudman, 2010: 3264; Walsh, 2009: 7; & Raval, 2010: 4
3	Compatibility risk	<p>This risk includes:</p> <ul style="list-style-type: none"> • The risk that in-house applications are not compatible with the SaaS functionality. • The risk of data inconsistency between the provider and the client which may result in corrupt data. 	Carraro and Chong, 2006; Putri and Mganga, 2011: 56; & Raval, 2010: 3

No	Abbreviated Description	Detail of the risk	Original source
4	Cost risk	<ul style="list-style-type: none"> • The risk of hidden or overhead costs from service providers and leverage risk, in essence where the solution provider has all the leverage in negotiations when price increases are necessary. • No upper lever or maximum charge is set, which could lead to unexpected high charges, especially if the service was flooded by a denial of service attack. 	Aubert et al., 1998: 1; Accenture, 2011: 10 & Jensen et al., 2009: 115
5	Customisation risk	<ul style="list-style-type: none"> • Risk that the solution cannot be tailored to every user's needs or to all the needs of an enterprise. Most solution providers do not have the functionality to allow general customisation, but do allow some configuration to aspects of the software, such as the user interface or reporting requirements. 	Sääksjärvi et al., 2005: 183
6	Data theft	<p>This risk includes:</p> <ul style="list-style-type: none"> • Unencrypted data stored by the solution provider that may be subject to theft. • Inadvertent exposure of confidential information. • Theft of proprietary data by the solution provider from the customer. • Inadvertent disclosure of a customer's personal details. 	Putri and Mganga, 2011: 57; Carraro and Chong, 2006; ISACA, 2009c: 7; Rudman, 2010: 3263 & Jensen et al., 2009: 109; Feng et al., 2010: 1

No	Abbreviated Description	Detail of the risk	Original source
7	Data transmission risk	This risk includes: <ul style="list-style-type: none"> • Limited bandwidth or latency in communication. • Data loss, corruption or theft during transmission. 	Carraro and Chong, 2006; Feng et al., 2010: 1
8	Delayed response	<ul style="list-style-type: none"> • The risk that information processing or data retrieval has latency due to data being distributed across various data warehouses or poor infrastructure from the internet provider or the solution provider. 	ISACA, 2009c: 7
9	Denial of service (DOS) / Distributed Denial of Service (DDOS) / Unavailability	This risk includes: <ul style="list-style-type: none"> • Attack from hackers and viruses make the web-based software susceptible to unavailability. • Insufficient resource capacity of the solution provider. 	Putri and Mganga, 2011: 56; Symatec Corporation, 2008: 4; Sääksjärvi et al., 2005: 183; Jensen et al., 2009: 115; Briscoe et al., 2009: 3 & Feng et al., 2010: 1
10	Difficult intruder (malicious user) detection	<ul style="list-style-type: none"> • Risk that an unauthorised or malicious user can access the data or service and is undetected or unprevented, this will give rise to other risks such as data theft. 	Putri and Mganga, 2011: 57; Raval, 2010: 3

No	Abbreviated Description	Detail of the risk	Original source
11	Difficult in bug detection in software	This includes: <ul style="list-style-type: none"> • Difficulty of detecting bugs due to the size of data and the transactions processed. • The customer cannot directly observe the provider to identify possible malicious or unseen problems. 	Putri and Mganga, 2011: 57; Aubert et al., 1998: 4 & Rudman, 2010: 3264
12	Eavesdropping and data interception	This risk includes: <ul style="list-style-type: none"> • The interception of non-encrypted data. • Transfer of data on insecure infrastructure. 	Putri and Mganga, 2011: 56; Rudman, 2010: 2363 & Gadia, 2009: 7
13	Environmental threats	<ul style="list-style-type: none"> • This is the risk of prolonged power outages at either the client or the solution provider due to natural disasters. 	Stoneburner et al., 2002: 13
14	Human threats	This risk includes: <ul style="list-style-type: none"> • Problems due to unintentional acts or malicious acts. • Employment off inadequately-skilled personnel at the solution provider. • Improper training of users. • Inadvertent disconnection, such as a break in the undersea communications cable between the customer and provider. 	Stoneburner et al., 2002: 13; Accenture, 2011: 10

No	Abbreviated Description	Detail of the risk	Original source
15	Inadequate authentication and / or authorisation	This risk includes: <ul style="list-style-type: none"> • Authorised users performing unauthorised activities or has access to unauthorised information. • Compromise to data security due to improper controls implemented by the solution provider. • Insufficient controls or not all controls agreed are implemented by the solution provider. 	Rudman, 2010: 3264; Putri and Mganga, 2011: 56 & Cloud Security Alliance, 2010: 9
16	Incorrect or inadequate risk response	<ul style="list-style-type: none"> • The risk that the solution provider does not respond to a threat or that the response is inadequate. 	Rudman, 2010: 3261
17	Insecure data storage	<ul style="list-style-type: none"> • The risk that the solution provider stores data in an insecure cloud, which may compromise security and confidentiality. 	Putri and Mganga, 2011: 57; Feng et al., 2010: 1
18	Lack of data segregation / improper data disclosure	This risk includes: <ul style="list-style-type: none"> • In a multi-tenancy environment there is a risk that the tenants have improper access to other tenant's data. • Information is improperly disclosed. • Loss of business critical information. • Improper disposal of "old" backup data (*). 	Putri and Mganga, 2011: 56; Rudman, 2010: 3264; Sääksjärvi et al., 2005: 183 & Gadia, 2009: 7

No	Abbreviated Description	Detail of the risk	Original source
19	Legal obligation risk	<p>This risk includes:</p> <ul style="list-style-type: none"> • Non-compliance to regulatory requirements, such as regulations to where data must reside. • Lack of clear ownership of data or lack of clear responsibilities. • Legal liability in the event of improper disclosure of a customer's client information. 	Symatec Corporation, 2008: 4; Putri and Mganga, 2011: 56; Rudman, 2010: 3263 & ISACA, 2009c: 7
20	Loss of innovative capacity	<ul style="list-style-type: none"> • This risk results in the outsourcing decision of the IT process, which could lead to loss of innovation in the IT of an enterprise. 	Aubert et al., 1998: 1.
21	Malicious code imbedded in software	<p>This risk includes:</p> <ul style="list-style-type: none"> • Malicious code implanted by the provider. • Malware attacks that inject malware into the code, such as rootkit attacks, Trojans and viruses. 	Rudman, 2010: 3256; Jensen et al., 2009: 114

No	Abbreviated Description	Detail of the risk	Original source
22	Non-compliance with policies	This risk includes: <ul style="list-style-type: none"> • Non-compliance by the solution provider of service level agreements. • Underperformance, diminished business value or low productivity by the solutions provider. • Non-compliance of enterprise policies and procedures internally implemented by the users of the organisation. • Policy is not effectively implemented at the solution provider or at the client. 	ISACA, 2009c: 7; Symatec Corporation, 2008: 4 & Rudman, 2010: 3260
23	Non-compliance with reporting or legal requirements	This risk includes: <ul style="list-style-type: none"> • Difficulty to enforce rules or regulations at the solution provider if data is stored off-site. • Solution provider does not comply with reporting standards set or the reports are non-compatible. 	Putri and Mganga, 2011: 57; Carraro and Chong, 2006 & Raval: 2010: 4

No	Abbreviated Description	Detail of the risk	Original source
24	Opt-out risk	<p>This risk includes:</p> <ul style="list-style-type: none"> • The solution provider has tailored the application to such an extent that the client cannot change to a different solution provider. • Data recovered from the solution provider may not be usable by the client or another solution provider due to different meta-data and domain administration. • Risk that the data is irrecoverable due to data ownership disputes. • Poor solution provider selection from project initiation or moving to another solution provider. 	Cusumano, 2010: 28; Carraro and Chong, 2006; Accenture, 2011: 10; Aubert et al., 1998: 4 & Briscoe et al., 2009: 4
25	Out-dated access rights	<ul style="list-style-type: none"> • The risk that access rights are not updated with change in user's access rights or change in functionality. 	Rudman, 2010: 3264
26	Over-reliance of controls at the solution provider	<ul style="list-style-type: none"> • Over-reliance on ineffective or insufficient controls of the solution provider which could lead to unauthorised access. 	Rudman, 2010: 3264
27	Phishing attack	<p>This risk includes:</p> <ul style="list-style-type: none"> • User's identity theft and the risk of improper data disclosure or data theft. • Phishing or social engineering attack on the solution provider. 	Putri and Mganga, 2011: 57; Huang, Zhang and Hou, 2009: 237; Jensen et al. 2009: 111

No	Abbreviated Description	Detail of the risk	Original source
28	Unauthorised access	<p>This risk includes:</p> <ul style="list-style-type: none"> • Access by unauthorised users to data or unauthorised access to data by the service provider's personnel. • Rogue users gain access to restricted data. • Risk of data manipulation by unauthorised parties. • Poor security measures in the development of the software. 	Rudman, 2010: 3262; Putri and Mganga, 2011: 56; Symatec Corporation, 2008: 4; Gadia, 2009: 7 & Cloud Security Alliance, 2010: 10
29	Unauthorised modification to software	<ul style="list-style-type: none"> • The risk that the solution provider makes unauthorised changes to software images due to lack of controls (or maliciously). 	Putri and Mganga, 2011: 56
30	Updating and installation risk	<ul style="list-style-type: none"> • The risk that the service provider does not update the software sufficiently. 	Rudman, 2010: 3262

5.3 Framework selection

Several possible frameworks for the evaluation of risk and / or the implementation of controls were identified during the literature review. These include but are not limited to:

- CobiT: This framework sets out good practices for the means of risk management (ISACA, 2009a: 7).
- The Goal/Question/Metric Method (GQM), which is focussed on the improvement of software development (The Goal/Question/Metric Method (GQM), 1999).
- NIST SP800-55 is a practical approach to measure IT security (Lennon, 2008).
- Risk IT Framework, which identifies IT risk (ISACA, 2009a: 7).

- Enterprise Value: Governance of IT investments (Val IT), which is a framework, built on CobiT to provide enterprises with the structure to realise value from the enterprise investment (ITGI, 2008: 8).

Based on the evaluation, only CobiT and the Risk IT framework was considered due to the frameworks' use in prior studies and the recent release of the framework. On final selection however, CobiT was selected as the most appropriate framework; as CobiT is business focused and assists businesses to align IT to the organization's objectives to reach its goals. Furthermore CobiT is widely accepted as an international standard (ITGI, 2007: 5). Several studies have found it to be an acceptable framework to implement governance and evaluate risk (Smit, 2009: 16; Kieviet, 2006: 57; Sherry, 2007: 49; Rudman, 2010: 3253 & Putri & Mganga, 2011: 14).

IT governance incorporates and institutionalises good practice to guarantee that the enterprise's IT supports its business goals (ITGI, 2007: 5). ITGI (2007: 5) states that some of the key cornerstones of an enterprise's governance includes the assurance of IT's value, IT risk management and controls surrounding information. CobiT is an acronym for Control Objectives for Information and related Technology. This framework provides what it calls good practices across a domain-process oriented structure. The good practices are in concord with experts in the field (ITGI, 2007: 5).

According to ITGI (2007: 25) CobiT appeals to different users, such as:

- Executive management, as it assists in obtaining maximum value from IT investments and addresses risk and controls.
- Business management, as it provides assurance on the management and control of IT services provided by third parties.
- IT management, as it assists in compliance with business requirements.
- Auditors, as it assists in substantiating their opinions on management and internal control.

The main principle of CobiT is to assist enterprises in managing its IT resources by the means of structured processes in order to provide information to achieve enterprise goals and objectives (ITGI, 2007: 10).

CobiT's focus on information requirements leads it to define seven key criteria for information, which include:

- effectiveness,
- efficiency,
- confidentiality,
- integrity,
- availability,
- compliance and
- reliability (ITGI, 2007: 11).

CobiT was created based on its business-focussed process orientated nature, which was part of the reasons for selecting it, the other reason being acceptance in academic research. Risk evaluation and response is part of good governance, which is good practice and in some cases a statutory requirement. As noted, IT governance is one of the key cornerstones of IT governance. CobiT supports IT governance by establishing a framework that aligns IT and business goals, maximises business benefits from IT, establishes responsibility to IT resources and forms part of IT risk management. IT risk management is concerned with (ITGI, 2007: 6):

- Strategic alignment, which focusses on alignment of plans, enterprise value and operations between enterprise and IT.
- The value delivery, which focusses on executing the value proposition throughout the delivery cycle, by reducing cost and optimising benefits.
- Resource management, which focusses on managing IT resources, include applications, information, infrastructure and people.

- Risk managements, which include defining the enterprise's risk appetite, compliance requirements and implementing risk management responsibilities. Performance measurement is about the monitoring of implementation, resource usage and delivery.

The IT risk management aforementioned are the applications which constitute the automated systems and manual procedures necessary to process information. Information is the data in various forms such as input and output data; infrastructure is the technology deployed; and lastly people are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information (ITGI, 2007: 12).

The CobiT model is defined by four domains, which are Plan and Organise, Acquire and Implement, Deliver and Support and Monitor and Evaluate. According to ITGI (2007: 12) these domains are in accordance with the traditional IT responsibilities of plan, build, run and monitor (ITGI, 2007: 12).

Brief descriptions of the four domains are as follows (ITGI, 2007: 12):

- Plan and Organise: This domain is concerned with the strategy of how IT can best contribute to achieve the enterprise objectives. This includes planning and communication of the strategic vision.
- Acquire and Implement: This domain is concerned with the identification, acquisition and implementation of IT solutions.
- Deliver and Support: This domain is focussed on service delivery, security management, continuity management, help desk and the management of data.
- Monitor and Evaluate: This domain addresses performance management, internal control monitoring, compliance to laws and regulations and governance.

These domains include 34 identified processes, which are discussed in detail in section 5.4. These processes should be evaluated to ensure that all activities and responsibilities to IT are

complied with, however not all processes are applicable to all enterprises (or technologies such as SaaS).

5.4 Identification of applicable CobiT processes to users of SaaS

As noted in section 5.3, not all processes are applicable to all users of CobiT. Some processes are used in conjunction with one another and some are not applicable. In order to evaluate which processes are applicable to the users of SaaS, the study has developed Table 2 below which lists each of the 34 processes included in the four domains of CobiT, with three criterions to evaluate whether it is applicable to this study.

The first criterion is based on the mapping of the SaaS technology to the process. This was based on the literature review included in section 5.1. The second criterion is an evaluation whether the process is applicable to the SaaS user, or rather the solution provider, as the study purports only to identify risks from the user's perspective. Lastly there was an evaluation whether non-compliance to the process could yield an incremental risk to the SaaS user. If all 3 criteria were complied with, the process is regarded as applicable to this study. Subsequent to Table 2, the processes are briefly described.

Table 2 – Identification of applicable CobiT processes to users of SaaS

CobiT process	SaaS technology relevant to CobiT	Relevant to SaaS user	Possible risk for SaaS user	Applicable to this study
PO1 Define a Strategic IT Plan	Yes	Yes	Yes	Yes
PO2 Define the Information Architecture	Yes	Yes	Yes	Yes
PO3 Determine Technological Direction	Yes	Yes	Yes	Yes
PO4 Define the IT Processes, Organisation and Relationships	Yes	No	Yes	No
PO5 Manage the IT Investment	Yes	No	Yes	No
PO6 Communicate Management Aims and Direction	Yes	Yes	Yes	Yes
PO7 Manage IT Human Resources	Yes	No	Yes	No

CobiT process	SaaS technology relevant to CobiT	Relevant to SaaS user	Possible risk for SaaS user	Applicable to this study
PO8 Manage Quality	Yes	Yes	Yes	Yes
PO9 Assess and Manage IT Risks	Yes	Yes	Yes	Yes
PO10 Manage Projects	Yes	No	Yes	No
AI1 Identify Automated Solutions	Yes	Yes ***	Yes	Yes
AI2 Acquire and Maintain Application Software	Yes	No	Yes	No
AI3 Acquire and Maintain Technology Infrastructure	Yes	No ***	No	No
AI4 Enable Operation and Use	Yes	Yes	Yes	Yes
AI5 Procure IT Resources	Yes	Yes	Yes	Yes
AI6 Manage Changes	Yes	No	Yes	No
AI7 Install and Accredite Solutions and Changes	Yes	Yes	Yes	Yes
DS1 Define and Manage Service Levels	Yes	Yes	Yes	Yes
DS2 Manage Third-party Services	Yes	Yes	Yes	Yes
DS3 Manage Performance and Capacity	Yes	No	Yes	No
DS4 Ensure Continuous Service	Yes	Yes	Yes	Yes
DS5 Ensure Systems Security	Yes	Yes	Yes	Yes
DS6 Identify and Allocate Costs	Yes	No	No	No
DS7 Educate and Train Users	Yes	Yes	Yes	Yes
DS8 Manage Service Desk and Incidents	Yes	No	Yes	No
DS9 Manage the Configuration	Yes	No	Yes	No
DS10 Manage Problems	Yes	Yes	Yes	Yes
DS11 Manage Data	Yes	Yes	Yes	Yes
DS12 Manage the Physical Environment	Yes	No	Yes	No
DS13 Manage Operations	Yes	No	Yes	No
ME1 Monitor and Evaluate IT Performance	Yes	No	Yes	No
ME2 Monitor and Evaluate Internal Control	Yes	Yes	Yes	Yes
ME3 Ensure Compliance With External Requirements	Yes	No	Yes	No
ME4 Provide IT Governance	Yes	No	Yes	No

Yes *** - For initial implementation or change in service provider.

No *** - Assuming the user moved or has moved from server-centric (or more basic infrastructure) infrastructure to SaaS.

It is important to note that where the process is not considered to be applicable to SaaS users, it does not imply that this process is not applicable to the enterprise using SaaS. Enterprises should still consider the implementation of controls for all the CobiT processes, as other IT needs, investments and management is still required. Where Table 2 concluded that a process was not applicable, a brief reason for this is documented.

A summarized description of each of the CobiT processes applicable to SaaS follows, based on ITGI (2007: 29) description:

Plan and Organise

- PO1 Define a Strategic IT Plan: IT strategic planning is required to align the IT and enterprise strategy. The plan should be in place before the commencement of a new project or investment.
- PO2 Define the information architecture: This process improves the quality of decisions made due to the reliability and security of data.
- PO3 Determine the technological direction: This process defines the technological requirements to achieve an enterprise goal(s).
- PO4 Define the IT Process, Organisation and Relationship: The development of frameworks and committees to ensure enterprise agility was considered not to be relevant to the SaaS user, as it is more applicable to solution providers.
- PO5 Manage the IT investment: A framework to manage the IT investment and the cost management thereof was considered not to be relevant to the SaaS, as it is more applicable to solution providers.
- PO6 Communicate Management Aims and Direction: The implementation of an ongoing communication programme, by focussing on accurate and understandable policies.
- PO7 Manage IT Human Resources: This process includes appointing competent people to deliver IT services. This process was considered to be more applicable to the solution provider, as the customer receives the services.

- PO8 Manage quality: The quality management of IT services by implementation of a quality management service.
- PO9 Assess and Manage IT Risks: This process implements, maintains and creates a risk management framework which is linked to and aligned with the enterprise's risk management framework.
- PO10 Manage Projects: This process manages all IT projects, by defining a programme and budget to allow the stakeholders to assess each project's progress. This is applicable to an enterprise overall IT investment, but it is not applicable to the SaaS project alone.

Acquire and Implement

- AI1 Identify Automated Solutions: The defining of the enterprise's needs from the solution and to identify sources available. This includes translation of business needs and control requirements into the necessary solution.
- AI2 Acquire and Maintain Application Software: The acquisition of the application software and aligning it with the enterprise's requirements. In the case of SaaS, configuration is not usually available, this makes this process more applicable to the solution provider.
- AI3 Acquire and Maintain Technological Infrastructure: The acquisition of infrastructure; as the study is from the user's perspective and SaaS does not require complex infrastructure to be implemented, this process is regarded as not applicable.
- AI4 Enable Operation and Use: Documenting manuals and training of users to ensure proper use of the application.
- AI5 Procure IT Resources: This process covers procurement of IT resources, which includes people, hardware, software and services.
- AI6 Manage Changes: Changes to software and infrastructure are managed in order to respond to changes. The solution provider is tasked with this; however the user should consider this process to change between solution providers. For this study, however it is not applicable.

- A17 Install and Accredite Solutions and Changes: The process requires testing the solution selected. In a SaaS implementation there is normally no installation, but the solution is web based. Certain aspects of this process are applicable to the SaaS user.

Deliver and Support

- DS1 Define and Manage Service Levels: This process relates to the services between IT and management, including monitoring and reporting. In the context of SaaS it is the management of a SLA between the solution provider and client and the monitoring of compliance to the agreement. This is a core process in the adoption of SaaS and the most significant controls can be implemented in relation to this process.
- DS2 Manage Third-party Services: The definition of roles, responsibilities and third-party expectations and the monitoring of such services. For SaaS this process is fairly similar to DS1, but this process includes more risk management controls. This is a core process for the SaaS user. It is further important to note that third-party services include other services related to SaaS, such as the internet service provider.
- DS3 Manage Performance and Capacity: IT resources should be managed and performance reviewed. This process evaluates these requirements and predicts future requirements. This is not specifically necessary for a SaaS user, but for the solution provider. A key concept of SaaS is scalability by allowing a customer to adjust the required users.
- DS4 Ensure Continues Service: This process is tasked with minimising the risk and probability of major IT service interruption.
- DS5 Ensure System Security: This includes creating and maintaining IT security roles, responsibilities, polices, values, procedures and testing. In the SaaS environment this relates to securing the service by means of unique user names and passwords as well as securing data. Data should be secured on-site, in the cloud, during data processing and when transmitting data.

- DS6 Identify and Allocate Costs: Development of a system to capture, allocate and report IT cost of projects. As a SaaS user is well aware of the cost of the service, this process is regarded as being more applicable to the solution provider.
- DS7 Educate and Train Users: Training users based on the needs of a user group and assessing the results of such training.
- DS8 Manage Service Desk and Incidents: Implementation of a well-executed service and incident management process. In the event of problems for users, this will be managed by the enterprise's overall management desk, or by the solution provider. This process is deemed to be not applicable to a SaaS user.
- DS9 Manage Configuration: The process establishes functions to ensure the integrity of hardware and software. As documented in AI2 most SaaS solutions are not configurable, therefore this process is not applicable.
- DS10 Manage Problems: This controls effective problem management and the improvement of corrective action when 'problems' are identified.
- DS11 Manage Data: This includes the implementation of effective procedures to manage a data library, backup and disposal of media.
- DS12 Manage the Physical Environment: Management of the physical environment, including physical access, selecting of facilities and implementing procedures in the event of environmental threats. This process is concerned with the physical environment, and is therefore more applicable to the solution provider, as the client only needs access to the internet.
- DS13 Manage Operations: This process is tasked with management of processing, protecting output, monitoring infrastructure and maintaining hardware. This process is more applicable to the solution provider.

Monitor and Evaluate:

- ME1 Monitor and Evaluate: The management of IT performance management, including defining performance indicators, performance reporting and incite action. This process is important to the enterprise as a whole, but the process shares common

characteristics with some of the other Monitor and Evaluate processes which are more applicable to the SaaS user.

- ME2 Monitor and Evaluate Internal Control: Effective internal control requires a well-defined monitoring process, which includes exception reporting and third party reviews.
- ME3 Ensure Compliance with External Requirements: This process ensures that an enterprise complies with laws, regulations and contractual stipulations. This is important to the enterprise, but is not considered to be a specific process relating to the SaaS user.
- ME4 Provide IT Governance: Establishing an effective framework is a key process for the enterprise as a whole, therefore not just specifically for a SaaS user.

5.5 Map risk to CobiT framework

The risks identified in Table 1 (section 5.2) were mapped to the applicable processes identified in Table 2 (section 5.4) based on the possibility that the risk could have an impact on a process, which could be a negative impact or a loss of opportunity.

Table 3.1 – Risks relating to CobiT processes

	Audit difficulty	Business continuity / backup risk	Compatibility risk	Cost risk	Customisation risk	Data theft	Data transmission risk	Delayed response	Denial of service (DOS) / Distributed Denial of Service (DDOS) / Unavailability	Difficult intruder (malicious user) detection
PO1 Define a Strategic IT Plan										
PO2 Define the Information Architecture					◆					
PO3 Determine Technological Direction										
PO6 Communicate Management Aims and Direction	◆									
PO8 Manage Quality										
PO9 Assess and Manage IT Risks										
AI1 Identify Automated Solutions			◆	◆	◆					
AI4 Enable Operation and Use										
AI5 Procure IT Resources			◆							
AI7 Install and Accredite Solution Changes			◆		◆			◆		
DS1 Define and Manage Service Levels		◆				◆	◆	◆	◆	
DS2 Manage Third-party Services		◆		◆		◆	◆	◆	◆	
DS4 Ensure Continuous Service		◆							◆	
DS5 Ensure Systems Security						◆	◆		◆	◆
DS7 Educate and Train Users										
DS10 Manage Problems										
DS11 Manage Data		◆	◆			◆	◆			
ME2 Monitor and Evaluate Internal Control	◆									

◆ - Indicates that the process selected is mapped to the risk identified.

Table 3.2 – Risks relating to CobiT processes (Continued)

	Difficulty bug detection in software	Eavesdropping and data interception	Environmental threats	Human threats	Inadequate authentication and / or authorisation	Incorrect or inadequate response to risk	Insecure data storage	Lack of data segregation/ improper data disclosure	Legal obligation risk	Loss of innovative capacity
PO1 Define a Strategic IT Plan										
PO2 Define the Information Architecture							◆			
PO3 Determine Technological Direction										◆
PO6 Communicate Management Aims and Direction									◆	
PO8 Manage Quality										
PO9 Assess and Manage IT Risks					◆	◆				
AI1 Identify Automated Solutions									◆	
AI4 Enable Operation and Use				◆		◆				
AI5 Procure IT Resources										
AI7 Install and Accredite Solution Changes	◆									
DS1 Define and Manage Service Levels			◆	◆			◆	◆	◆	
DS2 Manage Third-party Services			◆					◆	◆	
DS4 Ensure Continuous Service										
DS5 Ensure Systems Security		◆			◆		◆	◆		
DS7 Educate and Train Users				◆		◆				
DS10 Manage Problems						◆				
DS11 Manage Data		◆					◆	◆		
ME2 Monitor and Evaluate Internal Control										

Table 3.3 – Risks relating to CobiT processes (Continued)

	Malicious code imbedded in software	Non-compliance with policies	Non-compliance with reporting or legal requirements	Opt-out risk	Out-dated access rights	Over-reliance of controls at the solution provider	Phishing attack	Unauthorized access	Unauthorized modification to software	Updating and installation risk
PO1 Define a Strategic IT Plan				◆						
PO2 Define the Information Architecture						◆		◆		
PO3 Determine Technological Direction										
PO6 Communicate Management Aims and Direction		◆								
PO8 Manage Quality		◆		◆						
PO9 Assess and Manage IT Risks					◆					◆
AI1 Identify Automated Solutions			◆							
AI4 Enable Operation and Use										
AI5 Procure IT Resources		◆		◆						
AI7 Install and Accredite Solution Changes	◆	◆	◆	◆				◆		
DS1 Define and Manage Service Levels		◆		◆				◆	◆	◆
DS2 Manage Third-party Services		◆		◆					◆	◆
DS4 Ensure Continuous Service										
DS5 Ensure Systems Security	◆				◆	◆	◆	◆	◆	◆
DS7 Educate and Train Users		◆					◆			
DS10 Manage Problems										
DS11 Manage Data										
ME2 Monitor and Evaluate Internal Control										

In evaluating the risks mapped to the processes, the trend of most significant and / or most frequent risks can be developed. The following figure illustrates the number of times a process could be affected:

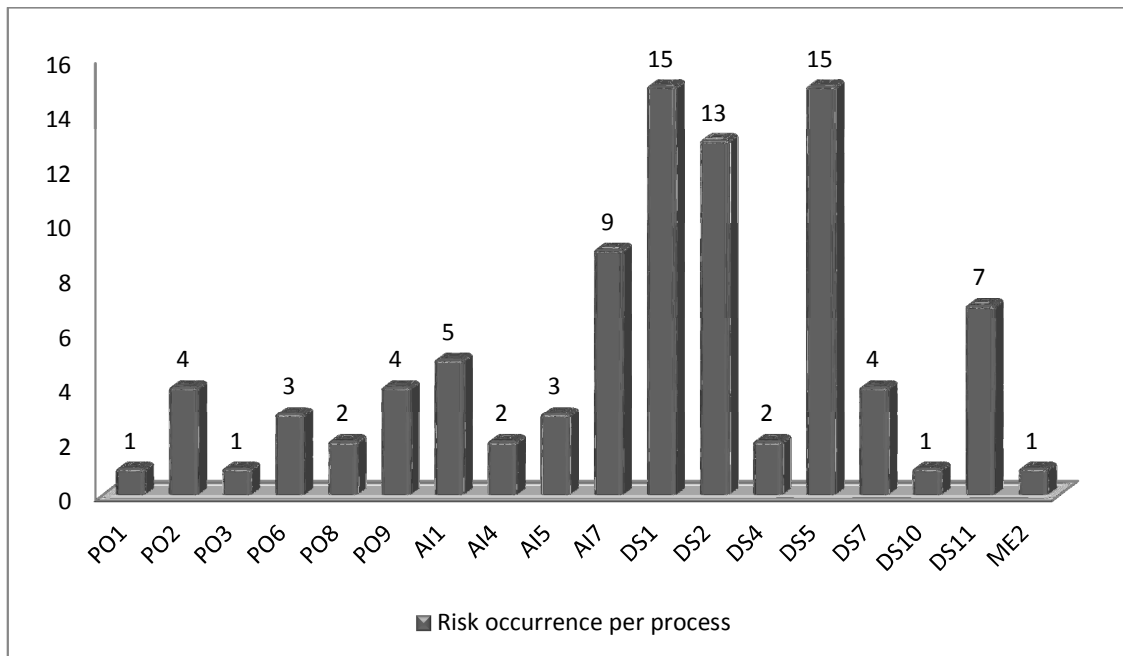


Figure 4 - Processes most likely to be affected by risk relating to use and implementation of SaaS.

From the evaluation it is clear that service levels management (DS1), the management of third-party services (DS2) and ensuring system security are the most likely affected processes in an enterprise due to the use or implementation of SaaS (DS5). This was to be expected, based solely on the investigation into SaaS and its related technologies. Not too far behind the aforementioned is the installation of accredited solutions (AI7), which was also to be expected.

5.6 Possible safeguards or controls

CobiT defines control objectives for all 34 processes and controls. CobiT defines control as: “the policies, procedures, practices and organisational structures designed to provide reasonable

assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected” (ITGI, 2007: 13).

Table 4 below indicates the risks identified in section 5.2. Using the risk mapping tables in section 5.5 (Tables 3.1 to 3.3) it is possible to identify possible controls and safeguards for the risk identified. Column 3 in Table 4 indicates the control objective linked to the process in CobiT. The control stems from the control objective in the CobiT framework, linking the control to a framework.

Refer to Table 2 (section 5.4) for a description of the process. The reference indicates the process and the control implemented by using CobiT. This is best illustrated by means of an example, where the first risk identified was audit difficulty (with the full description of audit risk in section 5.2, Table 1), and the processes it relates to, PO6 and ME2, were mapped in Table 3.1 (section 5.5). There is an additional reference added to the process reference which indicates the control from the CobiT framework. In this example PO6.1 yielded a possible control (where PO6 relates to Communicate Management Aims and Direction process and the “1” relates to control number 1 of PO6 was selected as applicable).

Therefore in the SaaS control framework, for audit risk process PO6, control “1” would be described as “defining control elements of the IT environment with assistance from internal and external auditors, ensuring that these controls are implemented and that there is a sufficient audit trail available”. Column 4 in Table 4 describes the control(s) identified.

Not all controls identified by CobiT are applicable to the risk identified. It should be noted that not all processes that were mapped to a process in Table 3.1 to Table 3.3 of section 5.5 had a sufficient control available to prevent, detect or correct risks; these process references were excluded from the table after the consideration of possible controls and safeguards. Where the control is identified from external sources not linked to specific research conducted, those

controls are identified by an external reference. Controls that are developed from general information will be marked with an asterisk.

The primary purpose of this study was to identify risk; therefore Table 4 indicates the possibility of identifying controls by using the CobiT framework. The list of controls and safeguards cannot be accepted as complete or sufficient to address the risk identified.

Table 4 – Possible safeguards and controls for risks identified

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
1	Audit difficulty	PO6.1, ME2.6	<ul style="list-style-type: none"> • With the assistance of external or internal auditors, define the control elements of the IT environment and ensure the controls are implemented and have an audit trail available. • Continuously monitor the control environment to ensure it meets the organisations objectives. This includes the status of the solution provider’s internal control and compliance with laws and regulations. One option to ensure this is stipulating in the SLA that a Statement on Standards for Attestation Engagements No. 16 (SSAE 16) (that replaced Statements on Auditing Standards No 70, Service Organisations – SAS 70) report on the implementation and effectiveness of controls be performed by external auditors on the solution provider. • Stipulate access to data for the customer’s auditors in the SLA (if permission is granted). <p>(*)</p>

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
2	Business continuity / backup risk	DS1.1 – DS1.6, DS2.2, DS4.2, DS4.5, DS4.8, DS4.9, DS4.10, DS11.5	<ul style="list-style-type: none"> • The Service level agreement with the solution provider should: <ul style="list-style-type: none"> ▪ Stipulate a data-backup schedule and where the backup should be kept (off site, other country, etcetera). ▪ The backup process should be monitored by the enterprise and the backup should be tested according to a schedule a regularly. ▪ Detail how data is stored, for example in a public deployment model, data could be encrypted. • Implement redundancy plans in the event of lost connection, such as wireless connectivity if the wired connection fails and test these plans on a regular scheduled basis. • Document a service recovery and resumption plan that should be followed in the case of service disruption, data loss or change in solution provider.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
3	Compatibility risk	AI1.3, AI5.3, DS11.1, AI7.5	<ul style="list-style-type: none"> • Perform a due diligence exercise or feasibility study and evaluate whether current data, software and reporting tools (such as eXtensible Business Reporting Language (XBRL)) are compatible with the solution provider and that the solution provider's data and reporting is compatible with the enterprise. • Implement a solution provider selection matrix, based on due diligence performed and select the providers (or even a combination of providers) that comply with the selected criteria. • In the event of data conversion, implement a data conversion plan that stipulates the conversion method, audit trails, rollback and data backup. • All data, processing and reporting requirements must be documented in advance and the enterprise should ensure that the solution provider can comply with the requirements by testing the software / application.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
4	Cost risk	DS2.2	<ul style="list-style-type: none"> • Implement a fixed cost structure in the SLA which is based on a per-user or a data usage matrix. These costs should be predetermined and fixed or have fixed escalation clauses. • Implement a maximum cost ceiling in the SLA, with an option to increase the ceiling based on pre-approval. (*)
5	Customisation risk	AI1.1, AI1.3	<ul style="list-style-type: none"> • Identify, prioritise and specify the business needs and technical requirements for the SaaS solution, from this point a due diligence should be conducted on all identified solution providers. The solution provider should be selected based on this outcome.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
6	Data theft	DS1.6, DS2.3, DS5.3, DS5.4, DS11.6	<ul style="list-style-type: none"> • The SLA agreement should: <ul style="list-style-type: none"> ▪ Include a confidentiality agreement between the parties involved and any external parties that may have access to confidential data. ▪ Define policies and procedures for data security and storage. • The user should implement an identity management programme to ensure all users are uniquely identifiable. Access rights to services and data should be controlled by a data access matrix. • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts. • Select well established solution providers with a verifiable track record. (*)

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
7	Data transmission risk	DS2.2, DS2.3, DS5.11	<ul style="list-style-type: none"> • Define minimum data transfer standards in a SLA with the internet service provider and monitor the performance to the standards set. Alternative measures and backup systems should be implemented to reduce extended loss in connectivity. • All sensitive data must be transmitted over a trusted path, with controls such as encryption, non-repudiation and proof of receipt. • Implementing third authorities' certificates or the secret key sharing technique (Feng et al., 2010: 2). • Implementation of Transport Layer Security (TLS) (Jensen et al., 2009: 112).
8	Delayed response	AI7.9, DS1.2, DS1.3, DS2.2	<ul style="list-style-type: none"> • Define minimum standards for service delivery between third-party service providers in a SLA and monitor the performance. • Establish procedures in post implementation in line with the minimum requirements of an SLA and evaluate possible delayed responses and act on the evaluation's findings.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
9	Denial of service (DOS) / Distributed Denial of Service (DDOS) / Unavailability	DS1.1, DS2.2, DS4.2, DS5.9	<ul style="list-style-type: none"> • Implement an opt-out clause in the SLA in the event where an enterprise could outgrow the solution provider. • Define minimum standards for service delivery between third-party service providers in a SLA and monitor the performance. • Install preventative, detective and corrective software and hardware measures (such as firewalls) to reduce risk to malicious software such as viruses.
10	Difficult intruder (malicious user) detection	DS5.10	<ul style="list-style-type: none"> • Implement network security measures and procedures, such as firewalls, segmentation of services and data and intrusion detection software.
11	Difficulty bug detection in software	AI7.7	<ul style="list-style-type: none"> • Software should be sufficiently tested before final selection of the solution provider.
12	Eavesdropping and data interception	DS5.10, DS5.11	<ul style="list-style-type: none"> • Implement network security measures and procedures, such as firewalls, segmentation of services and data and intrusion detection software. • All sensitive data must be transmitted over a trusted path, with controls such as encryption, non-repudiation and proof of receipt.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
13	Environmental threats	DS2.3	<ul style="list-style-type: none"> • Identify and implement procedures to mitigate the risk, such as pre-approved alternative solution providers and backup and restoration plans.
14	Human threats	AI4.2 – AI4.4, DS7.2, DS7.3	<ul style="list-style-type: none"> • Train users on the proper use of the SaaS applications and the related requirements. The training material, educators and users should be evaluated. Evaluate the training to identify possible problems and improvement of the training programme. • Implement redundancy plans, such as alternative solution providers, backup and restoration procedures. (*) • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
15	Inadequate authentication and / or authorisation	PO9.3, PO9.4, DS5.3, DS5.4	<ul style="list-style-type: none"> • Develop risk scenarios and tests that could identify possible improper controls. These should be recorded, maintained, updated and performed on a scheduled basis. • The user should implement an identity management programme to ensure all users are uniquely identifiable. Access rights to services and data should be controlled by a data access matrix. • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts. • Monitor and test the controls implemented by the solution provider in terms of the SLA.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
16	Incorrect or inadequate risk response	PO9.5, AI4.3, DS7.2, DS10.1, DS10.2, ME4	<ul style="list-style-type: none"> • Develop and maintain a risk response process that is proactive to assessed risk. The process does not need to list all possible responses, but rather response based on the type of risk, its frequency and magnitude. • Problems and solutions should be logged. If the solution failed, this should also be logged and alternative course of action should be available (secondary responses). The failed solution should be reviewed and updated if necessary. • Develop and train users to respond adequately in the event of detection of a risk by developing risk scenarios and tests that could identify possible improper controls.
17	Insecure data storage	PO2.4, DS1.3, DS5.5, DS11.6	<ul style="list-style-type: none"> • Implement a data storage matrix, the client and solution provider can implement storage, encryption and archiving requirements in the SLA. • Monitor that the solution provider stores data in terms of the SLA to a predefined data access matrix. Test that the controls related to data sets are implemented and sufficient in terms of the matrix.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
18	Lack of data segregation / improper data disclosure	DS2.3, DS2.4, DS5.3, DS5.4, DS11.4	<ul style="list-style-type: none"> • The user should implement an identity management programme to ensure all users are uniquely identifiable. Access rights to services and data should be controlled by a data access matrix. • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts. • The SLA should include: <ul style="list-style-type: none"> ▪ Non-disclosure agreements. ▪ Predefined procedures on disposal of data and “old” backups, to ensure data security. • Data access should be logged and monitored by clients to inspect possible improper data access and should react thereon to stop further improper disclosure. • Data backup should be scheduled and checked regularly. (*) • Predefine data storage in the SLA. This should include data storage options in multi-tenant deployments, to prevent inadequate disclosure to other tenants. (*)

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
19	Legal obligation risk	DS1.3, DS2.3	<ul style="list-style-type: none"> • Implement a SLA that: <ul style="list-style-type: none"> ▪ Stipulate ownership of data and reports. ▪ Stipulate retention periods for data, data security measures and other legal requirements that may be applicable to the enterprise's laws and regulations environment. • Obtain third party liability insurance, where confidential data of client's are subject to the cloud infrastructure.
20	Loss of innovative capacity	PO3.1, ME4	<ul style="list-style-type: none"> • Document a technological direction plan, which enables the identification of emerging trends and technologies that could impact the competitive environment and assist in change of technological direction.
21	Malicious code imbedded in software	DS5.9	<ul style="list-style-type: none"> • Put preventative, detective and corrective measures in place such as firewalls and antivirus software.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
22	Non-compliance with policies	PO8.6, AI5.2.3, AI7.9, DS1.3, DS2.2, DS2.4, DS7.2, ME3, ME4	<ul style="list-style-type: none"> • Define, plan and implement service delivery according to predetermined standards and practices and evaluate the service delivery to these standards. • Users should be sufficiently informed about the policies that exist. An acknowledgement register of policies should be implemented. • Monitor compliance to SLA terms by the solution provider. • Stipulate minimum service standards in the SLA, as well as maximum tolerable errors with penalty for non-compliance and opt-out clauses.
23	Non-compliance with reporting or legal requirements	AI1.3, AI7.6, ME3, ME4	<ul style="list-style-type: none"> • Perform a feasibility study to evaluate whether the solution provider will be able to comply with reporting requirements. • Perform tests on test data and evaluate whether the provider complies with the required reporting requirements.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
24	Opt-out risk	PO1.4, PO8.3, AI5.2, AI7.6, DS1.3, DS2.3	<ul style="list-style-type: none"> • Create and implement a strategic IT plan that defines how IT goals will contribute to the enterprise’s strategic objectives. This should include the IT strategy. • Develop acquisition standards that incorporate the preliminary testing of solution providers. • The implementation of a SLA that: <ul style="list-style-type: none"> ▪ Includes a “cooling off” clause to provide the possibility of changing solution providers. ▪ Stipulate data recovery procedures that ensure data will be useable, transferrable and recoverable in the event of termination of services. ▪ Document ownership of data in the SLA.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
25	Out-dated access rights	PO9.5, DS5.4	<ul style="list-style-type: none"> • Implement a risk monitoring committee compelled with the review of the IT risk management framework to ensure it is enforced. This committee should review the execution of all risk management practices and report any deviations to those charged with governance. • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts.
26	Over-reliance of controls at the solution provider	DS5.5, ME4	<ul style="list-style-type: none"> • Test and monitor the controls implemented in a proactive way. Threats and possible risks should be logged and followed up by implementing controls to reduce or mitigate the risk. This should be linked to a monitoring framework.
27	Phishing attack	DS5.4, DS7.2	<ul style="list-style-type: none"> • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts. • Users should be trained on identifying possible phishing attacks and how to respond thereto.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
28	Unauthorised access	PO2.3, AI7.4, DS5.3, DS5.4	<ul style="list-style-type: none"> • Test the solution provider’s access controls before implementation. Insufficient controls can be identified and proactively implemented and controlled. • Implement a data access matrix for all users and data (and information requirements). This can be used to apply access controls, archiving and encryption. • The user should implement an identity management programme to ensure all users are uniquely identifiable. Access rights to services and data should be controlled by a data access matrix. • User accounts must be managed on a high level, including alterations to the data access matrix and associated access rights, suspension, addition and closing user accounts.
29	Unauthorised modification to software	DS2.3, DS2.4, DS5.5	<ul style="list-style-type: none"> • Implement an update schedule and an update log. The updates should be preapproved by the client (if possible) and the log should be reviewed for unauthorised updates and changes.

No	Risk identified	CobiT Control reference	Possible safeguard or control from CobiT and literature review
30	Updating and installation risk	DS2.3, ME1.1	<ul style="list-style-type: none"> • Implement an update schedule and an update log. The updates log should be reviewed to ensure updates are installed timely and that the updates are implemented. • Implement a general monitoring framework and processes to measure compliance with service levels.

Many of the risks share the same controls, specifically controls and terms defined in a SLA agreement and reviewing the services provided by third parties. From an evaluation the following key controls were found:

- Backup and recovery plan and procedures.
- Data access matrix.
- Due diligence evaluation of solution providers and feasibility study.
- IT strategic plan.
- Monitoring framework, including review and responses to matters identified.
- Network and workstation security measures.
- Preliminary and pre-implementation testing.
- Service level agreement, including all factors noted above.
- SSAE 16 compliance reporting on the solution provider.
- Training of all parties involved.
- User matrix or user account control framework.

To illustrate that these few controls could reduce risk to the SaaS user, Table 5 illustrates the risks and only the significant controls identified that could reduce the specific risk:

Table 5 – Most significant controls identified to mitigate risk

		Backup	Data-access matrix	Due diligence	IT plan	Monitoring	Network security	Preliminary testing	SLA	SSAE16 report	Training	User matrix
1	Audit difficulty								•	•		
2	Business continuity/ backup risk	•							•			
3	Compatibility risk	•		•					•			
4	Cost risk								•			
5	Customisation risk			•								
6	Data theft		•						•			•
7	Data transmission risk						•		•			
8	Delayed response								•			
9	Denial of service (DOS) / Distributed Denial of Service DDOS) / Unavailability					•	•		•			
10	Difficult intruder (malicious user) detection						•					
11	Difficulty bug detection in software							•				
12	Eavesdropping and data interception						•					
13	Environmental threats	•										
14	Human threats										•	
15	Inadequate authentication and / or authorisation		•					•				•
16	Incorrect or inadequate risk response										•	
17	Insecure data storage		•						•			
18	Lack of data segregation / improper data disclosure	•				•			•			•

		Backup	Data-access matrix	Due diligence	IT plan	Monitoring	Network security	Preliminary testing	SLA	SSAE16 report	Training	User matrix
19	Legal obligation risk								•			
20	Loss of innovative capacity				•							
21	Malicious code imbedded in software							•				
22	Non-compliance with policies								•		•	
23	Non-compliance with reporting or legal requirements			•				•				
24	Opt-out risk				•				•			
25	Out-dated access rights					•						•
26	Over-reliance of controls at the solution provider					•						
27	Phishing attack										•	•
28	Unauthorised access		•					•	•			
29	Unauthorised modification to software					•						
30	Updating and installation risk					•						

• - Indicates that for the risk identified, the corresponding control could reduce risk.

As with Figure 4 (section 5.5), there is a trend in which some controls feature more prominently for the SaaS user. These include the implementation of a well thought out and well-constructed SLA with the solution provider and other third party services. This was also the finding of Putri and Mganga (2011: 46) in their study on enhancing cloud security with the use of SLA's. These controls alone would assist an enterprise to reduce risk, however due to constant technological change, an enterprise must update its controls and IT governance framework to adapt to these changes and the possibility of new risks.

6. Conclusion and future research

6.1 Conclusion and findings

The research was concerned with the identification of risks relating to the use and implementation of SaaS from a user's perspective. There was a necessity identified for the research due to the regulatory obligation and good practice which compel enterprises to implement corporate governance and therefore IT governance. This was further compounded by the identification of a possible lack in academic research on SaaS risks and possible safeguards and controls.

In order to identify risks and controls, the research set out to identify what SaaS is. Section 2.1 documents the overall aspects of SaaS, where section 5.1 went into a more technical documentation of SaaS based on the literature review. The study deduced a definition for SaaS, but no universally acceptable definition was identified during the literature review. The next step was to identify a control framework that was acceptable and allowed the implementation of a framework to assist IT governance. The research concluded that the CobiT framework was the most applicable for this specific scenario.

The CobiT framework contains 34 processes in 4 domains, Table 2 (section 5.3) evaluated which of these processes are applicable to the SaaS user, as some processes are not applicable to SaaS technology and other are more applicable to the solution provider. It was determined after the evaluation that 18 of these processes were applicable to the SaaS user. It is important to note that all the processes may be applicable to the enterprise as a whole.

The CobiT framework was used, in conjunction with an in-depth literature review to identify risks relating to SaaS. A wide range of risks were identified from many sources. The paper selected the common characteristics to identify 30 condensed risks, as described in Table 1

(section 5.2). The next process included mapping the 30 risks identified with the 18 processes identified (Table 3.1 - Table 3.3 of section 5.5). Figure 4 from section 5.5 identified a pattern to the risks and the related processes of an enterprise wishing to adopt or that has adopted SaaS, in that certain processes are more likely to be directly affected by SaaS, due to the nature of SaaS. It was also noted, due to the technologically evolving environment, that the control framework and IT governance should be constantly evaluated and updated to manage these environmental changes that will inevitably lead to new risks.

Users of the framework should evaluate whether all the risks apply to their enterprise, or whether they have identified additional risks. Based on this, the frequency of the risk occurrence and the magnitude or impact on the enterprise should be evaluated, by using either case studies or past experience. These findings would assist management in the decision of what type of controls to implement, if any.

The study's primary aim was to identify incremental risks to SaaS and allocate these risks to a framework; however the research endeavoured to develop a possible control framework from the CobiT framework. These controls are not technically orientated, but rather intend to give the reader an idea of how to develop controls by using CobiT as the IT governance control framework.

The research identified 30 incremental risks to software as a service from a user's perspective. A framework was developed which included 11 key controls to reduce, mitigate or accept the risks. Other secondary controls were also identified.

6.2 Future research

Possible future research could include building on the control framework developed, by developing a highly technical good practice standard control or safeguard to each of the risks identified. This could assist enterprises, based on the evaluation of the risks in this research in

their own environment, to implement the controls developed to prevent, detect or correct risks. These controls should mitigate, distribute or absorb the risks identified. Another possible research avenue could include the expansion of the risk framework to a technical IT orientated level. This may identify additional risks that the research has not yet identified.

7. Bibliography

- Accenture. 2009. *What the enterprise needs to know about cloud computing*. [Online]. Available: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Technology_Labs_What_the_Enterprise_Needs_to_Know_About_Cloud_CoComputi.pdf. [July 10, 2011].
- Accenture. 2011. *Accenture Technology Vision 2011 - The Technology Waves That Are Reshaping the Business Landscape*. [Online]. Available: <http://www.accenture.com/us-en/technology/technology-labs/Pages/insight-accenture-technology-vision-2011.aspx>. [March 6, 2011].
- Ahmad, R. & Janczewski, L. 2011. *Triangulation Theory: An approach to mitigate governance risk in clouds*. [Online]. Available: http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_subsubmis_153.pdf. [July 9, 2011].
- Al Zabir, O. 2011. *99.99% available ASP.NET and SQL Server SaaS Production Architecture*. [Online]. Available: <http://www.codeproject.com/KB/aspnet/ProdArch.aspx>. [September 4, 2011].
- Aubert, B.A., Patry, M. & Rivard, S. 1998. *Assessing the Risk of IT Outsourcing*. [Online]. Available: <http://origin-www.computer.org/plugins/dl/pdf/proceedings/hicss/1998/8248/06/82480685.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253AAddress%253A%2B41.5.97.42%252C%2B%255B172.16.161.5%252C%2B127.0.0.1%252C%2B41.5.97.42%255D>. [May 28, 2011].
- Benlian, A., Hess, T. & Buxman P. 2009. Drivers of SaaS Adoption – An Empirical Study of Different Application Types. *Business & Information Systems Engineering*. Edition 5, 2009: 357-369. [Online]. Available: <http://www.springerlink.com/content/m05ph11j5845w071/fulltext.pdf>. [July 3, 2011].

- Briscoe, G. & Marinos, A. 2009. Community cloud computing. *LSE Research Online*. December 2009: 1-12. [Online]. Available: [http://eprints.lse.ac.uk/26516/1/community_cloud_computing_\(LSERO_version\).pdf](http://eprints.lse.ac.uk/26516/1/community_cloud_computing_(LSERO_version).pdf). [August 26, 2011].
- Carraro, G. & Chong, F. 2006. *Software as a Service (SaaS): An Enterprise Perspective*. [Online]. Available: <http://msdn.microsoft.com/en-us/library/aa905332.aspx>. [March 25, 2011].
- Chong, F., Carraro, G. & Wolter, R. 2006. *Multi-Tenant Data Architecture*. [Online]. Available: <http://msdn.microsoft.com/en-us/library/aa905332.aspx>. [March 25, 2011].
- Choudhary, V. 2007a. Comparison of Software Quality Under Perpetual Licensing and Software as a Service. *Journal of Management Information Systems*. Vol. 24, No. 2: 141–165. [Online]. Available: <http://web.merage.uci.edu/~veecee/saasvsperpetualjmis.pdf>. [May 28, 2011].
- Choudhary, V. 2007b. Software as a service: implications for investment in software development. *International conference on system sciences*. 2007. [Online]. Available: <http://academic.research.microsoft.com/Publication/2432954/software-as-a-service-implications-for-investment-in-software-development>. [May 29, 2011].
- Cloud Security Alliance. 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. [Online]. Available: <https://cloudsecurityalliance.org/csaguide.pdf>. [September 1, 2011].
- Cloud Security Alliance. 2010. *Top Threats to Cloud Computing V1.0*. [Online]. Available: <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>. [August 26, 2011].
- Cusumano, M. 2010. Technology Strategy and Management: Cloud Computing and SaaS as New Computing Platforms. *Communications of the ACM*. April 2010, Vol. 53, No. 4: 27-29. [August 4, 2011].

- Doszkocs, T.E., Hill, G., Lindgren, F. & Yashinsky, N. 2001. *XML (Extensible Markup Language)*. [Online]. Available: <http://searchsoa.techtarget.com/definition/XML>. [September 4, 2011].
- Encarta Dictionary*. 2011.
- Feng, J., Chen, Y. & Liu, P. 2010. Bridging the missing link of cloud data storage security in AWS. *2010 7th IEEE Consumer communications and Networking Conference: 2-3*. [Online]. Available: <http://pods.binghamton.edu/~ychen/PID990602.pdf>. [August 26, 2011].
- Fishteyn, D. 2009. *Deploying Software as a Service (SaaS)*. [Online]. Available: http://www.saas.com/homepage/pdf/SaaS.com_Whitepaper_Part1.pdf. [March 24, 2011].
- Gadia, S. 2009. Cloud computing – an auditor’s perspective. *ISACA Round Table Presentation*. [Online]. Available: http://www.mnisaca.org/_RoundTable_Resources/Cloud%20Computing%20Presentation%20v4.pdf. [August 26, 2011].
- HTTP (Hypertext Transfer Protocol). 2000. [Online]. Available: <http://searchwindevelopment.techtarget.com/definition/HTTP>. [September 4, 2011].
- Huang, X., Zhang, T. & Hou, Y. 2009. ID Management among Clouds. *2009 First International Conference on Future Information Networks: 237-241*. [August 26, 2011].
- IBM. 2010. Defining a framework for cloud adoption. *Thought Leadership White Paper*. [Online]. Available: <ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/ciw03067usen/CIW03060USEN.PDF>. [August 18, 2011].
- Institute of Directors of Southern Africa. 2009. *King Code of Governance for South Africa 2009*. [September 10, 2011].

- ISACA. 2009a. *The Risk IT Framework*. [Online]. Available:
<http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx?gclid=CleSte6juqcCFQP1bwodiz3MAA>. [March 6, 2011].
- ISACA. 2009b. *The Risk IT Practitioner Guide*. [Online]. Available:
<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx>. [March 6, 2011].
- ISACA. 2009c. Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. *White paper on emerging technology*. [Online]. Available:
http://www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_&_Governance-ISACA.pdf. [August 18, 2011].
- IT Governance Institute (ITGI). 2007. *CobIT 4.1*. [Online]. Available:
<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx>. [March 21, 2011].
- IT Governance Institute (ITGI). 2008. *The Val IT Framework 2.0 Extract*. [Online]. Available: <http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery/Documents/Val-IT-Framework-2.0-Extract-Jul-2008.pdf>. [March 24, 2011].
- Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L.L. 2009. On Technical Security Issues in Cloud Computing. *2009 IEEE International Conference on Cloud Computing*. 2009: 109-116. [August 26, 2011].
- Kang, S., Myung, J., Yeon, J., Ha, S., Cho, T., Chung, J. & Lee, S. 2010. A General Maturity Model and Reference Architecture for SaaS Service. *Database Systems for Advanced Applications*. Lecture Notes in Computer Science, 2010, Volume 5982/2010: 337-346. [August 4, 2011].
- Kieviet, F. 2006. *Applying COBIT in an ERP environment, with specific reference to Qmuzik*. Master's thesis. Stellenbosch. University of Stellenbosch. [Online]. Available:
<http://scholar.sun.ac.za/bitstream/handle/10019.1/3390/Kieviet%2c%20F.pdf?sequence=1>. [July 7, 2011]

- Kooi. 2001. *Web Services Description Language (WSDL)*. [Online]. Available: <http://searchsoa.techtarget.com/definition/Web-Services-Description-Language>. [September 4, 2011].
- Lennon, E.B. 2008. *IT Security metrics*. [Online]. Available: <http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm>. [August 24, 2011].
- Mell, P. & Grance, T. 2009. *The NIST Definition of Cloud Computing*. [Online]. Available: <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>. [August 18, 2011].
- Nefdt, R., Miller, D., Spivack, J. & McGee, S. 2011. *Issues and trends: Assessing and managing SaaS risk*. [Online]. Available: <http://www.grantthornton.com/staticfiles/GTCom/Technology/SaaS%20survey%20series/SaaS%20Survey.pdf>. [March 27, 2011].
- Pervez, Z., Lee, S. & Lee, Y. 2010. Multi-Tenant, Secure, Load Disseminated SaaS Architecture. *Database Systems for Advanced Applications*. Lecture Notes in Computer Science. Volume 5982/2010: 214-219. [August 4, 2011].
- Petri, G. 2010. *Shedding light on cloud computing*. [Online]. Available: http://www.ca.com/files/WhitePapers/mpe_cloud_primer_0110_226890.pdf. [July 9, 2011].
- PricewaterhouseCoopers. 2010. *Global Software Leaders: Key players & market trends*. December 2010. [Online]. Available: <http://www.pwc.com/za/en/publications/index.jhtml>. [August 4, 2011].
- Putri, N.R., Mganga, M.C. 2011. *Enhancing Information Security in Cloud Computing Services using SLA Based Metrics*. Master's thesis: Blekinge Institute of Technology. [Online]. Available: [http://www.bth.se/fou/cuppsats.nsf/all/780daa1ef3027f82c1257864001c2d87/\\$file/MCS-2011-03.pdf](http://www.bth.se/fou/cuppsats.nsf/all/780daa1ef3027f82c1257864001c2d87/$file/MCS-2011-03.pdf). [July 9, 2011].
- Raval, V. 2010. Risk landscape of cloud computing. *ISACA Journal*. Volume 1 2010: 1-5. [Online]. Available: http://www.infotex.com/portal_blog/white_papers/risk_landscape_of_cloud_computing_isaca.pdf. [August 26, 2011].

- Rudman, R. J. 2009 Incremental risks in Web 2.0 applications. *Emerald insight*. Vol. 28(2): 210-230. [Online]. Available: http://www.emeraldinsight.com/Insight_ViewContentServlet_contentType=Article&Filename=_published_emeraldfulltextarticle_pdf_2630280202. [March 23, 2011].
- Rudman, R. J. 2010. Framework to identify and manage risks in Web 2.0. *African Journal of Business Management*. Vol. 4(13): 3251-3264. [Online]. Available: <http://www.academicjournals.org/ajbm/pdf/pdf2010/4Nov/Rudman.pdf>. [March 23, 2011].
- Sääksjärvi, M., Lassila, A. & Nordström, H. 2005. *Evaluating the Software as a Service Business model: From CPU time-sharing to online innovation sharing*: 177-186 [Online]. Available: http://scholar.google.co.za/scholar?q=Software+as+a+service+risk&hl=en&as_sdt=1%2C5. [2011, May 24].
- Sherry, Z. 2007. *Governance of Virtual Private Networks using COBIT as framework*. Master's thesis. Stellenbosch. University of Stellenbosch. [Online]. Available: <http://scholar.sun.ac.za/bitstream/handle/10019.1/3389/Sherry.pdf?sequence=1>. [March 24, 2011].
- Sivaram, D. 2000. *SOAP (Simple Object Access Protocol)*. [Online]. Available: <http://searchsoa.techtarget.com/definition/SOAP>. [September 4, 2011].
- Smit, S. 2009. *Defining and reducing the IT gap by means of comprehensive alignment*. Master's thesis. Stellenbosch. University of Stellenbosch. [Online]. Available: https://ir1.sun.ac.za/bitstream/handle/10019.1/15038/smit_defining_2009.pdf?sequence=1. [July 9, 2011].
- Stoneburner, G., Goguen, A. & Feringa, A. 2002. Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology*. Special Publication 800-30. [Online]. Available: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. [March 23, 2011].

- Subashini, S. & Kavitha, V., 2010. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*. 34 (2011): 1–11. [Online]. Available: http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6WKB-50J4MMN-2-5&_cdi=6902&_user=10&_pii=S1084804510001281&_origin=&_coverDate=01%2F31%2F2011&_sk=999659998&view=c&wchp=dGLzVtb-zSkWA&md5=f23115212a2d608165691f642f3199e8&ie=/sdarticle.pdf. [May 28, 2011].
- Symantec Corporation. 2008. *IT Risk Management Report 2: Myths and Realities*. [Online]. Available: http://eval.symantec.com/mktginfo/enterprise/other_resources/bit_risk_management_report_2_01-2008_12818026.en-us.pdf. [March 23, 2011].
- TCP/IP (Transmission Control Protocol/Internet Protocol). 2000. [Online]. Available: <http://searchnetworking.techtarget.com/definition/TCP-IP>. [September 4, 2011].
- The Goal/Question/Metric Method (GQM)*. 1999. [Online]. Available: <http://www.gqm.nl/>. [August 26, 2011].
- Thompson, H.H. *Hidden risks of software-as-a-service*. [Online]. Available: <http://www.networkworld.com/columnists/2006/073106thompson.html?page=1>. [March 25, 2011].
- UDDI (Universal Description, Discovery, and Integration). 2000. [Online]. Available: <http://searchsoa.techtarget.com/definition/UDDI>. [September 4, 2011].
- Walsh, P.J. 2009. The brightening future of cloud security. *Network Security*. October 2009: 7-10. [August 26, 2011].
- Wang, L., Von Laszewski, G., Younge, A. & He, X. 2008. *Cloud Computing: a Perspective Study*. *New Generation Computing*, 28 (2010): 137-146. [August 4, 2011].

Appendix A – Glossary of terms

Term	Description
AJAX	Asynchronous JavaScript and XML
AWS	Amazon web services
CobIT	Control Objectives for Information and related Technology
IaaS	Infrastructure as a service
IT	Information technology
King III	King Code of Governance for South Africa 2009
PaaS	Platform as a service
SaaS	Software as a service
SLA	Service level agreement
XBRL	eXtensible Business Reporting Language

Appendix B –Common concepts and conventions used

Concept	Description
Cloud computing	A model for enabling convenient, on-demand network access to a shared infrastructure of configurable computing resources (e.g., servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Configuration	To customise aspects of the application or software (Where only certain aspects are normally configurable).
Customer	Refers to an enterprise, which may consist of many users.
Framework	A model on reference guide.
Frequency	“... number of times an event occurs in a given time period” (ISACA, 2009b: 37).
Incremental risk	Not only additional risk, it includes significantly increased risk and greater magnitude or frequency of a risk event.
ITGI	IT Governance Institute
Magnitude	“A measure of the potential severity of loss or the potential gain from a realised IT-related event” (ISACA, 2009a: 101).
Map	Mapping entails the allocation of technologies and risks to the most applicable process in the framework.
Multi-tenant architecture	“one that uses common resources and a single instance of both the object code of an application as well as the underlying database to support multiple customers simultaneously” (Fishteyn, 2009: 1).
Perpetual licence software	Applications or software that is purchased once-off or has an annual fee to use the software.

Concept	Description
Private domain	Infrastructure is deployed only for a single organisation, over an enterprise's intranet. The organisation normally owns the infrastructure, whether it is on or off the premises or externally managed (Petri, 2010: 9; IBM, 2010: 3-4 & PricewaterhouseCoopers, 2010: 14)
Public domain	The cloud is accessed over the internet and the client and provider are two different organisations and the ownership of infrastructure is with the provider (Petri, 2010: 9; IBM, 2010: 4 & PricewaterhouseCoopers, 2010: 14)
Risk	Loss of opportunities for an enterprise or a negative impact to an enterprise
SaaS	The delivery of software or an application by a provider(s) over a network (internet or intranet) for a pay per use or fixed per user rental fee
Solution provider	The application or software supplier in the SaaS concept.
Tenant	In a multi-tenant deployment model, each customer occupies a section of the solution provider's architecture, including data and processing space.
User / client	The user / client is the enterprise or person that uses the software deployed by a solution provider