Cloud computing: COBIT-mapped benefits, risks and controls for consumer enterprises

by
Zacharias Enslin

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

Supervisor: Mr. Christiaan Lamprecht

March 2012

Declaration

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

_____

Zacharias Enslin

March 2012

Abstract

Cloud computing has emerged as one of the most hyped information technology topics of the decade. Accordingly, many information technology service offerings are now termed as cloud offerings. Cloud computing has attracted, and continues to attract, extensive technical research attention. However, little guidance is given to prospective consumers of the cloud computing services who may not possess technical knowledge, or be interested in the in-depth technical aspects aimed at information technology specialists. Yet these consumers need to make sense of the possible advantages that may be gained from utilising cloud services, as well as the possible incremental risks it may expose an enterprise to.

The aim of this study is to inform enterprise managers, who possess business knowledge and may also be knowledgeable on the main aspects of COBIT, on the topic of cloud computing. The study focuses on the significant benefits which the utilisation of cloud computing services may bring to a prospective consumer enterprise, as well as the significant incremental risks this new technological advancement may expose the enterprise to. Proposals of possible controls that the prospective consumer enterprise can implement to mitigate the incremental risks of cloud computing are also presented.

Uittreksel

"Cloud computing" (wolkbewerking) het na vore getree as een van die mees opspraakwekkende inligtingstegnologieverwante onderwerpe van die dekade. Gevolglik word talle inligtingstegnologie-dienste nou as "cloud"-dienste aangebied. Uitgebreide aandag in terme van tegnologiese navorsing is en word steeds deur "cloud computing" ontlok. Weinig aandag word egter geskenk aan leiding vir voornemende verbruikers van "cloud"-dienste, wie moontlik nie tegniese kennis besit nie, of nie belangstel in die diepgrondige tegniese aspekte wat op inligtingstegnologie-spesialiste gemik is nie. Tog moet hierdie verbruikers sin maak van die moontlike voordele wat die gebruik van "cloud"-dienste mag bied, asook die moontlike inkrementele risiko's waaraan die onderneming blootgestel mag word.

Die doel van hierdie studie is om die bestuurders van ondernemings, wie besigheidskennis besit en moontlik ook kundig is oor die hoof aspekte van COBIT, in te lig oor wat "cloud computing" is. Die studie fokus op die beduidende voordele wat die benutting van "cloud computing"-dienste aan die voornemende verbruikersonderneming mag bied, asook die beduidende inkrementele risiko's waaraan die onderneming blootgestel mag word as gevolg van hierdie tegnologiese vooruitgang. Voorstelle van moontlike beheermaatreëls wat die voornemende verbruikersonderneming kan implementeer ten einde die inkrementele risiko's van "cloud computing" teë te werk word ook aangebied.

Acknowledgement

I would like to express my sincere gratitude to the Lord God Triune for guiding and blessing me in life and in the completion of this assignment.

Table of contents

List of Tables and Figures

Section 1 - Introduction

1.1 - Background

Outsourcing of specialised activities, such as courier and telephony services, by enterprises is common practice in order to cut costs. Scale benefits are derived from outsourcing, as enterprises only pay for the services that they consume. If these functionalities were provided in-house, the enterprise would usually not be able to consume all the capacity on a continual and uninterrupted basis due to the fluctuating demand for these functionalities (Abraham & Taylor 1993). The same may be true with regard to an enterprise's Information Technology ('IT') functionality.

Research firm Gartner's inquiries reflect that most organisations over-provide their IT infrastructure by at least 100% (Mingay & Govekar 2010). This is done to provide infrastructure for peak utilisation periods and, additionally, to add safety margins to this provision.

Cloud computing is emerging as a possible cost saving solution to this capital intensive over-provision of capacity. Gartner defines cloud computing as "a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies" (Plummer, Smith, Bittman, Cearley, Cappuccio, Scott, Kumar & Robertson 2009). Consequently, by using cloud computing services a consumer enterprise will become critically reliant on an additional number of outside parties, as well as on Internet-based technologies with regard to its IT functionality and data security.

Recently "cloud failures" have occurred at some high level cloud computing service providers, of which Amazon (Amazon Web Services 2011) was the most notable. Security breaches at Sony Online Entertainment (Sony Online Entertainment 2011) also highlighted some of the risks involved in using Internet-based technologies.

The above-mentioned "cloud failures" and Internet-based technology security breaches have highlighted the fact that incremental risks are involved in this environment. These risks must be identified and mitigated to an acceptable level.

1.2 - Purpose of this study

Cloud computing has emerged as one of the most hyped topics in computing at present (Smith 2010). However, research thus far has focused solely on the technical aspects thereof. There is a shortage of research literature aimed at guiding consumer enterprises (including business) in the adoption of cloud computing (Marston, Li, Bandyopadhyay & Ghalsasi 2011).

This study assists in fulfilling the need for consumer guidance by, firstly, defining cloud computing and subsequently identifying significant benefits, incremental risks and possible risk mitigating controls for businesses and other enterprises who may be considering the adoption of cloud computing as part of their strategic IT plan. The study is the first comprehensive study to map the benefits and risks to a recognised IT risk control and governance framework.

1.3 - Scope and limitations of study

This study is presented on a business and control framework knowledge level in order to empower business professionals and enterprise managers with knowledge on cloud computing. It does not cover technical discussions on the risks and the technical implementation techniques and procedures needed to activate the identified controls.

Furthermore, only significant benefits and significant incremental risks are identified as the study does not attempt to represent an exhaustive list of all benefits and risks. Cloud computing is an evolving paradigm (Smith 2010; Mell & Grance 2011) with new benefits and risks certain to develop as the computing paradigm matures.

1.4 - Research study methodology

Considerable uncertainty exists among consumers regarding what cloud computing is and which services can be classified as cloud services (Smith 2010; Kushida, Murray & Zysman 2011; Rimal & Choi 2011). A literature review was therefore performed to define cloud computing more comprehensively, thereby enabling consumers to better comprehend what it encompasses. It also explores the different deployment and service models of cloud computing services and provides some examples of providers of these services.

A control framework was then selected to assist in systematically identifying and classifying significant benefits, as well as significant incremental risks of adopting cloud computing, by means of the framework's specified control processes. The control framework that was selected is Control Objectives for Information and related Technology (COBIT) version 4.1. After classification of the incremental risks, COBIT's control processes were used to select risk mitigating controls.

Lastly, the identified significant benefits, significant incremental risks and selected risk mitigating controls were confirmed, by referencing literature that discusses the relevant issue as a benefit, risk and/or control. A consumer enterprise can thus refer to the literature if further detail on a specific issue is required.

1.5 - Organisation of the research

Section 2 presents the literature review on the definition of, and introduction to, cloud computing. This is followed by the introduction to, and motivation for, utilising COBIT 4.1 as a control framework in Section 3. Section 4 contains the significant benefits identified, classified ('mapped') according to COBIT 4.1's control processes. Section 5 subsequently contains the significant incremental risks, as well as the proposed risk mitigating controls and high level control procedures identified, also classified according to COBIT 4.1's control processes. Section 6 concludes the study with final conclusions and recommendations for further research.

Section 2 - Defining cloud computing

2.1 - Background

In Section 1 cloud computing was briefly defined with reference to the Gartner definition of cloud computing (Plummer *et al.* 2009). During the recent years, the word "cloud", used in reference to IT services, has become a vague and flexible term (Giglia & De Orlov 2011; Kushida, Murray & Zysman 2011). The lack of a clear comprehension of what cloud computing entails can cause confusion for a prospective cloud service consumer enterprise when the adoption of cloud computing is considered as part of an enterprise's IT strategy.

To further complicate matters, cloud computing includes an array of different IT-related services, which could each potentially be acquired on its own (Vaquero, Rodero-Meniro, Caceres & Lindner 2009), such as Internet accessible remote storage space, word and spreadsheet processing services and Internet-based e-mail services.

Section 2 aims to provide the reader with a better comprehension of cloud computing. Section 2.2 provides a definition for cloud computing, followed by Section 2.3 which summarises the main characteristics of cloud computing in order to provide insight into those services which could possibly be classified as cloud computing services. Section 2.4 continues by describing the main deployment models of cloud computing, followed by Section 2.5 which lists the main service models. Lastly, Section 2.6 concludes the section on the definition of cloud computing by providing examples from the marketplace of cloud computing service providers and their services.

2.2 - Definition

For the purposes of this study, cloud computing will be defined by combining two current authoritative definitions. These two definitions encompass the main characteristics of cloud computing.

Cloud computing is "a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using Internet technologies", as defined by Gartner

Research (Plummer *et al.* 2009). These IT-enabled capabilities entail "ubiquitous, convenient, on-demand network access to a shared pool of configurable computer resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction", as defined by the National Institute of Standards and Technology of the United States of America (Mell & Grance 2011).

2.3 - Main characteristics of cloud computing

It may be helpful to explain the concept of cloud computing in terms of its outcome: A cloud service consumer enterprise that fully adopts cloud computing for all IT-enabled capabilities would not need to purchase (capital expenditure) or maintain (operational expenditure) its own IT resources (except a network accessing device or thin client device and possibly other output-related resources, such as a printer) in order to acquire IT-enabled capabilities relating to the services purchased. It can decide to utilise the IT resources of a cloud service provider through a network and pay only for the usage required by that consumer of these resources. These services are accessed via the Internet or other wide area network. However, most consumer enterprises currently adopt cloud computing only for certain IT capabilities and retain other functions in-house (Smith 2011).

The cornerstone of cloud computing is the delivery of IT-enabled capabilities as services. These services are referred to as cloud services (Plummer *et al.* 2009; ISACA 2009; Mell & Grance 2011). The main characteristics which a service should display in order to qualify as a cloud service, as drawn from the definition in Section 2.2, are presented in Table 2.1.

Table 2.1 - Main cloud computing characteristics

Characteristic	Description
On-demand self-service **(1)** / Scalable **(2)**	A consumer of the cloud services should have the capability to automatically provision the IT-enabled capabilities and the scale of usage of such capabilities (i.e. increase or decrease network storage etc.), due to automation on the part of the provider.
Broad network access **(1)** / Internet technologies **(2)**	The cloud service should be readily available, independent of the physical location of the *consumer* and independent of which type of standard network accessing device (such as computer, smart phone etc.) is used (i.e. it should be available using technologies developed around Internet usage).
Resource pooling **(1)** / Shared pool of resources **(2)**	The cloud services are provided to multiple consumers by using/sharing the same IT resources of the cloud service provider to achieve economies of scale (often referred to as the multi-tenant model). This also entails that the services are independent of the physical location of the resources of the *provider*.
Rapid elasticity **(1)** / Elastic **(2)**	These IT-enabling capabilities should be elastically scalable with the minimum, if any, time lag. The consumer must be able to rapidly scale up or down the level of IT capabilities required. This usually creates the impression with the consumer that the information technology resources are unlimited.
Measured service **(1)** / Metered by use **(2)**	The provider should have an accounting system in place that keeps record of resource usage in order to provide for billing of usage, relevant to the IT capabilities used by each consumer. This equates computing resources to commonly known utilities, such as electricity and telephone services. However the actual billing plans may take on different forms (e.g. pay-as-you-use, prepaid, fixed plans etc.)

(1) Characteristics according to USA National Institute of Standards and Technology (Mell & Grance 2011).

(2) Attributes according to research firm Gartner (Plummer *et al.* 2009).

If IT services exhibit these characteristics, it can be classified as cloud services. These cloud computing services will be deployed, using one of the deployment models discussed in the following section.

2.4 - Main deployment models of cloud computing

As stated earlier, cloud computing remains an evolving paradigm, resulting in the broadening of deployment models as it evolves. Plummer *et al*. (2009), on behalf of Gartner, indicated two deployment models, namely public cloud computing (or public cloud) and private cloud computing (or private cloud).

ISACA (2009), previously known as the Information Systems Audit and Control Association, expanded the deployment models to include community and hybrid cloud computing, as presented in Table 2.2.

Table 2.2 - Main cloud computing deployment models

Deployment model	Description
Public cloud	The cloud infrastructure is made available to the general public or a large industry group (i.e. the cloud service consumers) and is owned by a cloud service provider, which sells these cloud services.
Private cloud	The cloud infrastructure is operated solely for a single cloud service consumer enterprise. It may be managed by the enterprise or a third party and may exist on or off the consumer premises.
Community cloud	The cloud infrastructure is shared by several cloud service consumer enterprises and supports a specific community that has shared concerns (e.g. mission, security requirements, policy,

	and compliance considerations). It may be managed by the enterprises or a third party and may exist on or off the community premises.
Hybrid cloud	The cloud infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

Source: ISACA 2009 (amended)

This study approaches the incremental risks associated with cloud services from the perspective of a public cloud. Because a private cloud is operated solely for a specific enterprise, fewer security risks regarding multi-tenancy exist and the consumer enterprise would normally have more control over the services developed for it. Risks relating to these areas are therefore also decreased (Blandford 2011). This study can, however, be adjusted to apply to a private cloud computing deployment model by eliminating or decreasing those risks listed in Section 5 that relate to the above mentioned areas. An example of a risk that increases for private cloud services is compatibility issues when considering a change from one cloud service provider to another (i.e. becoming locked in with one service provider as systems already developed are not compatible with those of other providers).

Different IT capabilities can be delivered using these deployment models. The next section will explore the main service models into which these IT capabilities are divided.

2.5 - Main service models of cloud computing

The three main service models are derived from the IT capabilities that are provided in each case. These can be provided either alone or, most often, in combination. The service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Mell & Grance 2011). Certain literature refers to these service models as cloud service 'layers' (Jensen, Schwenk, Gruschka & Iacono 2009), as these services can indeed be, and often are, layered upon each other in implementation (Winkler 2011a). Table 2.3 elucidates the three main service models.

Table 2.3 - Main cloud computing service models

Service model	Description
Cloud infrastructure as a Service (IaaS)	The IT capability provided is that of processing, storage, network and other computer hardware-related capabilities. The consumer can run their own software (including operating system) on the computer hardware-related capability.
Cloud platform as a Service (PaaS)	The IT capability provided is that of a computing platform on which to run the software of the consumer, which was created using the programming languages and protocols supported by the specific platform.
Cloud software as a Service (SaaS)	The IT capability provided is that of software applications for use by the consumer. The software would be run on cloud infrastructure (either that of the SaaS provider or possibly that of another IaaS and/or PaaS provider), and be accessible by means of a network accessing device.

Source: ISACA 2009 (amended)

It should be noted that the consumer does not own the underlying cloud infrastructure in any of the cases above. This study encompasses all three service models and may be adjusted if utilisation of only one or two of the service models is contemplated.

2.6 - Examples from the marketplace of cloud service providers

In order to provide an overview of how providers of cloud services implement these deployment models and service models in practice, examples of cloud service providers and the related services that they offer are presented in Tables 2.4 to 2.6.

Table 2.4 summarises the services provided by some of the key cloud service providers.

Table 2.4 - Key cloud service providers

Provider	Description of service
Amazon	Amazon offers its Amazon Web Services, a suite of several services which includes the Elastic Compute Cloud (EC2), for computing capacity, and the Simple Storage Service (S3), for on-demand storage capacity. In addition to these core offerings, Amazon offers the SimpleDB (a database web service), the CloudFront (a web service for content delivery) and the Simple Queue Service (a hosted service for storing messages as they travel between nodes).
Apple	Apple introduced its cloud offering, 'iCloud', in 2011, as a central repository for applications, media files, documents, backups, settings and other items. Apple allows consumers to synchronise their data from their computers and mobile devices to a personalised central repository. The central repository on the Internet subsequently synchronises all of the data and media files back down to all of the consumer's devices, so that all devices have the same data (Hiner 2011).
AT&T	AT&T provides two cloud services: Synaptic Hosting, which enables consumers to store Windows serve, Linux client server applications and web applications on AT&T's cloud; and Synaptic Storage, enabling consumers to store their data on AT&T's cloud. AT&T provides one key component of the requisite infrastructure — the network backbone, and has experience in billing for it (i.e. they have an established revenue model). AT&T is currently adding data services to its offering.
Enomaly	Enomaly's Elastic Computing Platform (ECP) integrates enterprise data centres with commercial cloud computing offerings, allowing IT professionals to manage and govern both internal and external resources from a single console, while making it easy to move virtual machines from one data centre to another.
Google	Google's App Engine offers consumers access to Google's cloud-based platform, which provides tools to build and host web applications. Its premier SaaS offering is Google Apps, a set of online office productivity tools, including e-mail, calendaring, word processing and a simple website creation tool. Its acquisition of Postini, which offers a set of e-mail and web security services, makes it a credible provider in the area of electronic corporate communications.

IBM	IBM's cloud computing service, known as Blue Cloud, offers consumer enterprises access to tools that allow them to manage large scale applications and databases via IBM's cloud. The company offers consulting services to help companies integrate their infrastructure into the cloud.
Microsoft	Windows Azure, the "cloud operating system" PaaS appeared in early 2010. Additionally, they are creating the Azure Services Platform to run on the Windows Azure operating systems, giving consumer enterprises access to several online Microsoft services like Live, .Net, SQL, SharePoint and Microsoft's Dynamic CRM. Developers of cloud applications can potentially mix and match the building block services (e.g., SQL services, .NET services, Live services, etc.) that will run on the base Azure "operating system". Microsoft intends to offer its own cloud applications (e.g. Exchange Online) that will run off the Azure platform.
SalesForce.com	SalesForce.com is the first well-known and successful SaaS application. It has also introduced Force.com, an integrated set of tools and application services that independent software vendors and corporate IT departments can use to build any business application and run it on the same infrastructure that delivers the Salesforce CRM applications. It includes the company's Apex programming language.

Source: Marston *et al*. 2011 (amended)

It can be seen that well known and successful IT organisations are experimenting with different cloud service offerings. This serves as a convincing indicator of the way IT services are developing and that these large organisations see cloud computing as a worthwhile direction to pursue.

As the services offered are currently so diverse, various needs exist to ensure the technology is available to support these services. Table 2.5 lists service providers that provide technology that enables and complements the provision of cloud services by cloud service providers.

Table 2.5 - Key cloud computing technology providers

Provider	Description of service
Apache	Apache's Hadoop is an open-source software framework that has inspired the development of database and programming tools for cloud computing.
Cisco	Cisco is actively working on a set of standards that will allow portability across providers. One crucial aspect of this task is ensuring workload portability from one autonomous system to another, which includes the consistent execution of the workload on the new system (i.e. the execution of the complete IT policy associated with that workload).
EMC	EMC provides two key components in cloud computing — storage and virtualisation software (thanks to its acquisition of VMWare). EMC is also offering specialised storage solutions for cloud applications. The company has also introduced their vCloud initiative, which allows consumer enterprises to run their in-house applications on a cloud and be interoperable with other cloud services from other providers within the vCloud ecosystem.

Source: Marston *et al*. 2011 (amended)

Table 2.5 also illustrates the evolving nature of cloud computing. Cisco's planned portability standards, when finalised, would go far to lower the risk for consumer enterprises of becoming "locked-in" at one service provider.

Another gap that is exploited by IT organisations is to provide support service to cloud computing consumer enterprises. Table 2.6 lists a few cloud service support providers in order to further illustrate the resilience of the market with regard to cloud computing and related services.

Table 2.6 - Key cloud computing service support providers

Provider	Description of service
CapGemini	CapGemini is the first major professional services firm to pursue a partnership on Google Apps Premier Edition (GAPE) for consumer enterprises. It uses Google's software as a service initiative to seize opportunities among large consumer enterprises. CapGemini's GAPE service offerings reside within its well-established and mature Desktop Outsourcing Services practice.

RightScale	The RightScale Platform is an SaaS platform that helps consumer enterprises to manage the IT processes they have outsourced to cloud providers. It deploys new virtual servers and applications, performs load balancing in response to changing needs, automates storage backups, and offers monitoring and error reporting.
Vordel	Vordel offers several hardware and software products that help consumer enterprises to deploy cloud-based applications. Vordel provides the governance, performance, interoperability and security framework to enable consumer enterprises to exploit cloud computing.

Source: Marston *et al*. 2011 (amended)

The adoption of cloud computing by an prospective consumer enterprise may thus involve enlisting the services of several providers of cloud related services.

To better comprehend the possible benefits and incremental risk, an IT control framework was adopted to identify and categorise these benefits and incremental risks. The next section explains which framework was selected.

Section 3 - Control framework applied to cloud computing

It is of the utmost importance that the management of an enterprise comprehensively addresses the risks facing the enterprise. The Committee of Sponsoring Organisations of the Treadway Commission (COSO), an initiative to provide thought leadership on enterprise risk management (COSO 2010), strongly suggests the usage of a relevant and accredited control framework to address such risks. A generally accepted framework to supplement COSO in order to manage IT-related risks is Control Objectives for Information and related Technology (COBIT) (Tuttle & Vandervelde 2007).

COBIT is specifically designed to align IT management and governance with business requirements (COBIT 2007). This is achieved as COBIT has the following focus areas, namely; strategic alignment, value delivery, resource management, risk management and performance measurement. It is therefore specifically suited to this study which focuses on informing enterprise (including business) managers on the paradigm of cloud computing.

Tuttle & Vandervelde (2007) provide assurance that COBIT is not merely a valuable tool to guide management in IT governance, but that it is also an appropriate audit framework to use in an IT setting. This presents a strong case for its risk control properties.

COBIT is periodically updated to ensure its relevance in the ever-changing IT environment. Version 4.1 (the current version) was used in this study. Version 5 is currently in development, but is only expected to be finalised during 2012 (ISACA 2011). Furthermore, enterprise managers are expected to have built up a degree of knowledge on the current version of COBIT (4.1) and, accordingly, the presentation of this study in the version 4.1 format should make the study more user-friendly at the present stage.

COBIT 4.1 is divided into four domains, which are further subdivided into a total of 34 processes. All 34 processes were considered for this study to ensure completeness, but only the processes which could be linked to significant benefits or significant incremental risk are presented in the research findings tables in Sections 4 and 5.

Section 4 - Significant benefits of cloud computing adoption

4.1 - Significant benefits to consumer enterprise

This section focusses on the significant benefits of the adoption of a cloud computing approach by a consumer enterprise. These benefits were identified and categorised using COBIT's applicable processes. The research findings regarding these significant benefits are presented in Table 4.1. The left-hand column of this table represents the COBIT process for which a significant incremental benefit(s) was identified accompanying the adoption of a cloud computing approach while the right-hand column contains a description of the identified benefit(s).

Most of the significant benefits identified are supported by authoritative publications and earlier research, as indicated by numerals in brackets that correspond to the numbered list of these references listed below Table 4.1. References were only indicated where publications and research dealt with the benefit in relative detail. As a result, a specific reference may also briefly name some of the other benefits. However, these weren't necessarily referenced to it. References include: ISACA (2009), Cloud security alliance (2009), Jensen *et al*. (2009), Hill & Humphrey (2010), Marston *et al*. (2011), Subashini & Kavitha (2011), Sanders (2010), Hayes (2008), Feiman (2010), Mingay & Govekar (2010), Heiser (2009 & 2010), Knipp (2011), Pescatore (2010), Pring (2010) and Winkler (2011a & 2011b).

As discussed in Section 3, COBIT is divided into four domains which are further sub-divided into 34 processes. The processes are numbered in the following manner:

- Firstly, the relevant domain is stated in an abbreviated fashion, being either PO for 'Plan and Organise' domain, AI for 'Acquire and Implement' domain, DS for 'Delivery and Support' domain and ME for 'Monitor and Evaluate' domain; and
- Secondly, the processes in each domain are numbered.

The abbreviation 'CS' is used in the table to refer to 'cloud service' or 'cloud services'.

A short descriptive summary of the main benefits identified from the research findings is provided at the end of this section.

Table 4.1 - Mapping of significant benefits of cloud computing to COBIT

COBIT process	Possible benefit
PO1 Define a strategic IT plan	• Cloud services add a new dynamic to strategic IT planning as the outsourcing of capital expenditure in hardware, operating platform and software as all become viable options. **(1) (15)** • New enterprises will incur significantly less IT-related start-up costs to establish IT capabilities. **(5) (6) (15)**
PO3 Determine technological direction	• Cloud computing should support business opportunities, such as expansion of business (e.g. opening new branches), as it enables expansion of IT capabilities with minimal capital outlay in terms of IT infrastructure. **(1) (13) (15) (16)** • The economies of scale of cloud computing also have a positive environmental impact. The adoption of cloud computing may lower a CS consumer enterprise's carbon footprint ('greener' business practice). **(10)**
PO5 Manage IT investment	• Cloud computing enables the realisation of economies of scale by CS providers, due to the multi-tenant principle, that each CS consumer enterprise would not be able to realise on its own. In order to be competitive in the future cloud computing market, the CS provider would have to pass some of the benefits of these economies of scale through to the CS consumers. This should enable a CS consumer enterprise to achieve a better return on IT investment. **(1) (5) (13) (15) (16)**
PO7 Manage IT human resources	• The number of IT staff members required by a CS consumer enterprise is likely to decrease with the adoption of cloud computing, thereby ensuring a savings in operational expenditure relating to a decrease in human resources. **(9)**

COBIT process	Possible benefit
PO8 Manage quality	• Most aspects of quality management are outsourced to the CS provider. The CS consumer enterprise should benefit from economies of scale of the CS provider relating to the cost and employment of specialised IT professionals to ensure adequate controls. The CS provider's reputation depends on the adequacy of controls. **(13) (16)**
PO9 Assess and manage IT risks	• Certain IT risks, previously managed solely by the CS consumer enterprise, are now part of the outsourced services, enabling the enterprise to possibly benefit from the CS provider's superior ability to attract and employ specialised IT risk mitigating professionals, due to the CS provider's increased economies of scale. **(13) (15) (16)**
AI1 Identify automated solutions	• Cloud services provide automated solutions to satisfy infrastructure (hardware) requirements that could not traditionally be satisfied by automated solutions (specifically Iaas and Paas). **(12) (16)** • Saas and PaaS are also subject to greater automation than traditionally possible. **(12)** • A CS consumer enterprise can experiment with a larger array of different innovative IT capabilities and technologies than it would have been able to afford if it had to purchase such technologies before experimenting with them.**(5)** • The usage of Internet technologies also enables access, irrespective of location, as an option. **(5) (16)**
AI2 Acquire and maintain software	• Patching and version upgrades of software accessed as a cloud service by a CS consumer enterprise, should be up to date if a trustworthy CS provider (consider including this in a service level agreement (SLA)) is used who will benefit from economies of scale regarding such upgrading or patching. This can be achieved without the usual capital expenditure required on the CS consumer enterprise's side. **(15) (16)**

COBIT process	Possible benefit
AI3 Acquire and maintain technology infrastructure	• Technology infrastructure accessed as a cloud service by a CS consumer enterprise, should be up to date if a trustworthy CS provider (consider including this in an SLA) is used who will benefit from economies of scale regarding such upgrading of infrastructure. This can be achieved without the usual capital expenditure required on the CS consumer enterprise's side. **(1) (13) (15) (16)**
AI4 Enable operation and use	• Cloud computing is characterised by a multi-tenant model. Thus, the CS provider should have standardised user manuals and/or training available to all CS consumers (tenants).
AI6 Manage changes	• Most cloud services-related changes, such as patching and/or upgrading of infrastructure, are done by the CS provider, significantly reducing the workload regarding the management of changes on the CS consumer enterprise's side. **(15)** • The level of IT capabilities required by the CS consumer can be scaled up or down through a self-service process. This significantly decreases the number of controls which were traditionally needed, where changes to IT capabilities required major changes such as the installation of a new server, etc. **(1) (7)**
DS3 Manage performance and capacity	• Cloud services are characterised by rapid elasticity on-demand, ensuring that IT resource capacity can be rapidly scaled up or down to meet the CS consumer enterprise's changing requirements at all times. **(1) (5) (13) (15) (16)**
DS4 Ensure continuous service	• Most aspects of ensuring continued IT services are transferred to the CS provider. The CS provider will be inclined to ensure adequate controls relating to continuity of services due to the fact that a significant number of the CS provider's CS customers may be affected by downtime as a shared pool of resources is used to provide services to all of the CS provider's CS customers. Any interruption of services will have a major impact on the CS provider's reputation. **(1) (5) (13)**

COBIT process	Possible benefit
	• As cloud services are provided using broad network access (Internet technologies), continuation of service is not dependent on the location of the CS consumer enterprise's users. This means the CS consumer enterprise can easily access the IT capabilities from different locations (enhanced mobility). **(5) (16)** • As cloud services are provided using broad network access (Internet technologies), continuation of service is not necessarily dependent on a specific access route to a network or the Internet (.i.e. if the ADSL line is not functioning, 3.5G wireless access could, for example, be used to continue service in the interim). This could translate into fewer single points of failure ('SPOF') risk than in the case of leased VPN lines, for example. • Also refer to PO9.
DS5 Ensure systems security	• Most aspects of ensuring system security relating to IT services are transferred to the CS provider who will be inclined to ensure adequate controls relating to security due to the fact that a security breach relating to inadequate controls on the CS provider's side will have a major impact on the CS provider's reputation. **(1) (5)** • Also refer to PO9.
DS6 Identify and allocate cost	• One of the defining characteristics of cloud services is that the service is measured or metered by use. The CS provider would therefore already have such an accounting/metering system in place. This system could possibly meter use by individual groups within the CS consumer enterprise, making the allocation of IT-related costs to different segments of the CS consumer enterprise a vastly simpler task.
DS7 Educate and train users	• Refer to AI4.

COBIT process	Possible benefit
DS8 Manage service desk and incidents	• Most aspects of the IT service desk management are outsourced to the CS provider who would be required by all its CS consumer enterprise clients to have an adequate service desk to resolve user queries and incidents. The adequacy of this service will influence the CS provider's reputation.
DS9 Manage configuration	• Most aspects of configuration management are outsourced to the CS provider. The CS provider should benefit from economies of scale relating to the cost and employment of specialised IT professionals to ensure adequate controls. The CS provider's reputation depends on the adequacy of controls. **(16)**
DS10 Manage problems	• Most aspects of problem management are outsourced to the CS provider. The CS provider should benefit from economies of scale relating to the cost and employment of specialised IT professionals to ensure adequate controls. The CS provider's reputation depends on the adequacy of controls. **(16)**
DS11 Manage data	• Most aspects of data management are outsourced to the CS provider. The CS provider should benefit from economies of scale relating to the cost and employment of specialised IT professionals to ensure adequate controls. The CS provider's reputation depends on the adequacy of controls. **(16)** • Also refer to DS5.
DS12 Manage the physical environment	• Most aspects of managing the physical environment are outsourced to the CS provider. The CS provider should benefit from economies of scale relating to the cost and employment of specialised IT professionals, securing the physical environment and ensuring off-site backup (distributed data centres) to ensure adequate controls. The CS provider's reputation depends on the adequacy of controls. **(16)**
DS13 Manage operations	• Most aspects of operations management are outsourced to the CS provider. The CS provider should benefit from economies of scale relating to the cost and employment of specialised IT professionals to ensure adequate controls. The CS provider's reputation depends on the adequacy of controls. **(16)**

Numbered list of references:

(1) ISACA 2009.

(2) Cloud security alliance 2009.

(3) Jensen *et al*. 2009.

(4) Hill & Humphrey 2010.

(5) Marston *et al*. 2011.

(6) Subashini & Kavitha 2011.

(7) Sanders 2010.

(8) Hayes 2008.

(9) Feiman 2010.

(10) Mingay & Govekar 2010.

(11) Heiser 2009.

(12) Heiser 2010.

(13) Knipp 2011.

(14) Pescatore 2010.

(15) Pring 2010.

(16) Winkler 2011a.

(17) Winkler 2011b.

4.2 - Summary of main benefits to consumer enterprise

The majority of the benefits listed above relate to the scale benefits that are gained by the cloud service provider by having a significantly larger scale IT operation than any single consumer enterprise would reasonably be able to attain on its own. These benefits include the ability to attract and employ more highly skilled IT professionals, implement better continuation and security controls, diversifying physical location of data and back-up centres, providing better support as well as the ability and need to continually upgrade the hardware and software which is utilised to provide the IT capabilities. These benefits are subsequently passed on to the consumer enterprise in terms of a better IT service than the consumer could have provided for itself. A portion of the cost benefits is also passed on to the consumer enterprise.

The fact that cloud computing enables a cloud service consumer enterprise to exchange the traditional capital expenditure required to expand an enterprise's IT capacity for operational expenditure, in terms of a pay-as-you-use model, also represents a major benefit. As a result, an enterprise requires significantly less capital to start up or to expand, as it need not purchase an extensive IT system, but can scale its IT capabilities from cloud service providers, and connect from new locations to the cloud at pay-as-you-use rates.

Another advantage that is often overlooked is the fact that a consumer enterprise may indeed lower its negative impact on the environment by changing to cloud computing. According to a study by Mingay & Govekar (2010), the economies of scale achieved by the shared pool of resources which is utilised by the cloud service provider to provide the cloud services, also apply to environmental impact. For example, the cloud service provider is in a better position, due to the scale of its IT operations, to ensure that large data centres are run on an energy efficient basis. This would have the additional benefit of saving the service provider energy-related costs.

However, all these benefits must be considered in the context of the risks discussed in the following section. This holistic view should then be compared to the main business imperatives of each enterprise in order to decide whether cloud computing is an appropriate IT direction for the enterprise to pursue. This will also inform decisions on the level of implementation of cloud computing in the enterprise, versus the retention of certain functions in-house.

Section 5 - Significant incremental risks arising from cloud computing adoption, and controls addressing these risks

5.1 - Significant risks and controls relating to consumer enterprise

This section focusses on the significant incremental risks arising as a result of the adoption of cloud computing by a consumer enterprise, as well as risk mitigating controls to address these risks. The focus is specifically on incremental risk, thus additional risk that the adoption of cloud computing may expose a prospective cloud service consumer enterprise to.

These risks and controls were once again identified and categorised using COBIT's applicable processes. The research findings are presented in a Table 5.1. Please refer to Section 4 for an explanation of the table presentation, abbreviations usage and numeral referencing as they also apply to Table 5.1.

However, the column set-up of Table 5.1 differs from that of Table 4.1. Table 5.1 consists of three columns. The left-hand column represents the COBIT process for which a significant incremental risk(s) was identified. The middle column contains a description of the risk(s) identified and the right-hand column contains a possible risk mitigating control(s).

A short descriptive summary of the main risks and controls identified from the research findings is presented at the end of this section.

Table 5.1 - Mapping of significant incremental risk and risk mitigating controls relating to cloud computing to COBIT

COBIT process	Possible risk	Possible control
PO1 Define a strategic IT plan	• The hype around cloud computing may encourage the adoption thereof without careful and objective consideration of the advantages and disadvantages (including risks) with respect to each CS consumer enterprise's unique characteristics and requirements. This may lead to an incorrect decision to incorporate cloud computing into the prospective CS consumer enterprise's strategic IT plan. **(1) (15) (16)** Cloud computing may not be the best solution, as it may not align with business imperatives of the CS consumer enterprise (e.g. their strategy may be not to outsource, or utmost security over information may be a main business imperative). **(1)** • As cloud computing is still an evolving paradigm, the possibility exists that risks and threats that are not yet defined, may subsequently be discovered.	• Proper planning and investigation, as introduced by this study, should be done to ensure cloud services are the correct solution to a prospective CS consumer enterprise's IT requirements. **(1) (15)** • A definite incorporation of cloud computing into a prospective CS consumer enterprise's IT plan should be considered with great care, with reference to the CS consumer enterprise's unique situation, by a high level team of IT and business management and professionals. All stakeholders of the CS consumer enterprise should be consulted. **(1) (5) (15)**

COBIT process	Possible risk	Possible control
PO2 Define information architecture	• The outdated information architecture model of the CS consumer enterprise may allow the creation of data elements that are incompatible with the CS provider's platform. **(1)**	• Ensure that the information architecture model does not only account for the CS consumer enterprise's own architecture, but also for the CS provider's specific architecture (including platform). **(1) (2)** • Also refer to DS2.
PO3 Determine technological direction	• The IT plan of the CS consumer enterprise may not align IT investment with the characteristics of cloud computing, as is needed to ensure value and benefit realisation. For example, the IT plan should support IT investment in thin client devices when cloud computing is adopted, rather than over-investing in server infrastructure. • Major disinvestment in IT architecture by the CS consumer enterprise to realise benefits of cloud computing may lead to major future capital expenditure if the technological direction of the CS consumer enterprise were to change back to an in-house model in the future. • Cloud computing may not be the correct technological direction for a CS consumer	• Ensure that the IT plan of the CS consumer enterprise as a whole aligns with the characteristics of cloud computing to ensure full realisation of the benefits. **(1) (2)** • Develop the correct approach to implement cloud computing to ensure that the CS consumer enterprise's adoption of cloud computing is at the correct level for the particular enterprise, i.e. the relevant critical functions should be retained in-house where necessary. **(5) (14)** • A phased approach to the adoption of cloud computing, by not immediately disposing of all major redundant IT architecture, may decrease the risk of major financial loss if a change back to an in-house model is required. **(12) (15)**

COBIT process	Possible risk	Possible control
	enterprise located in geographical regions with underdeveloped Internet infrastructure to support efficient use of cloud computing, causing latency problems, for example. **(13)**	• Evaluate the adequacy of the speed and reliability of Internet offerings in the CS consumer enterprise's geographical region, before adopting cloud computing. **(13)** • Also refer to DS3.
PO4 Define the IT processes, organisation and relationships	• Refer to PO1 and PO2.	• Refer to PO1 and PO2.
PO5 Manage IT investment	• Prospective CS consumer enterprises with an established, up-to-date IT infrastructure (e.g. wide area network) may incorrectly assume that cloud computing would increase return on investment in IT infrastructure. Established infrastructure represents a sunk cost that may not be recoverable by the sale of this infrastructure. **(1) (13) (16)** • The most reliable public CS providers are currently located in a limited number of larger countries. They may, therefore, require payment in foreign currencies if the CS consumer enterprise is not located in the same country as	• IT investment should be managed by taking only future cash flows into consideration. For example, the net present value calculation method should be used to compare the cloud computing model's cash flows to that of the current IT model in use by the enterprise. **(13)** • Refer to DS2.

COBIT process	Possible risk	Possible control
	the CS provider. This will expose the CS consuming enterprise to additional foreign currency risk. **(13)**	
PO7 Manage IT human resources	• Some IT staff of the CS consumer enterprise may become redundant if cloud computing is adopted. **(9)** Labour laws may make the termination of their services challenging. • As a result of the abovementioned risk, a suggestion to consider cloud computing as an alternative may be greeted with opposition from some IT staff of the prospective CS consumer enterprise, who may be concerned about their job security. **(5)** **(9)** This may also lower the morale of IT staff. **(13)**	• Conduct proper IT staff planning and projections, and take the cost of the termination of redundant staff into consideration when deciding on cloud computing as a possible technological direction. • Clear communication should take place between management and IT staff to ensure that each staff member knows where he/she fits into the abovementioned planning and projections. **(9)**
PO8 Manage Quality	• Most aspects of quality management are outsourced to the CS provider. The risk exists that the CS provider's quality of service will not be adequate.	• Refer to DS2.

COBIT process	Possible risk	Possible control
PO9 Assess and manage IT risks	• Some aspects of risk assessment and management are outsourced to the CS provider. The risk exists that the CS provider's controls will not be adequate. **(1) (2) (11)** • There is increased exposure to IT-related risks for the CS consumer enterprise due to the incremental risks of cloud computing not being properly understood or not being properly incorporated into the risk management framework. **(1) (2)**	• Refer to DS2. • Ensure that a proper combination of skilled professional staff forms part of the risk assessment and management team of the CS consumer enterprise. **(1) (7)** • Ensure that the CS consumer enterprise's risk management framework incorporates the incremental risks associated with cloud computing into the risk management process. **(1) (2) (17)** • Refer to relevant literature (including this study and its references) to ensure that cloud computing-associated risk is understood and mitigated to an acceptable level.

COBIT process	Possible risk	Possible control
AI2 Acquire and maintain application software	• Current software of the CS consumer enterprise, or the acquisition of new software by the CS consumer enterprise, may not be compatible with the CS provider's platform (relating to PaaS). **(4) (5)** • The CS provider's software maintenance may be lacking (relating to SaaS) in terms of keeping up with patches and upgrading versions. **(2)**	• Refer to PO2. • Refer to DS2.
AI3 Acquire and maintain technology infrastructure	• The current infrastructure of the CS consumer enterprise, or the acquisition of infrastructure (e.g. thin client device) by the CS consumer enterprise, may not be compatible with the CS provider's Internet technologies/network access. • The CS provider's infrastructure maintenance may be lacking (relating to IaaS and PaaS) in terms of keeping up with new infrastructure technology (i.e. faster processors) and upgrading versions of platforms. **(2)**	• Refer to PO2. • Refer to DS2.

COBIT process	Possible risk	Possible control
AI4 Enable operation and use	• Standardised user manuals and/or training of the CS provider may not consider the specific CS consumer enterprise's circumstances, as they are written or conducted for the 'standard' CS consumer.	• If the CS consumer enterprise's circumstances differ from that of the 'standard' CS consumer, the CS consumer enterprise may need to consult with the CS provider on possible specialised training (refer to DS2), or conduct such training itself.
AI5 Procure IT resources	• The contract and/or SLA with the CS provider may not be enforceable. Cloud services are provisioned to consumers independent of the location of the CS provider. Cloud services are available across juristic borders (i.e. globally), making it difficult to ascertain under which country's jurisdiction a contract and/or SLA may fall. **(1) (2) (13)** • Also refer to DS2.	• Cloud contracts which could possibly span juristic borders should be reviewed by legal advisors knowledgeable in international law. **(2)**
AI6 Manage changes	• Some aspects of change management are outsourced to the CS provider. The risk exists that the CS provider's control over changes may not be adequate. **(12)** • Changing from one CS provider to another may be an onerous process (at this stage in time), as	• The CS provider should be selected with great care, using a meticulous selection and approval process, to minimise the possibility of the enterprise wishing to change from one provider to another. If possible, select a CS provider that uses generally established standards to ensure provider portability. **(2)**

COBIT process	Possible risk	Possible control
	the different providers have their own platforms, which may result in compatibility issues when changing from one CS provider to another. **(2) (4) (5)** • Implementing cloud computing may result in the loss of data or IT capabilities of the CS consumer enterprise due to incompatibility issues or other failure. **(11)** • The self-service automated scaling of resources may allow unauthorised scaling of services by individuals or even programs, for example, resulting in an unauthorised increase in expenditure for the CS consumer enterprise. **(1) (2)**	• Develop and implement compensating change-related controls (i.e. back-up, contingency plans etc.) before implementing cloud computing. **(2) (11)** • The change to cloud computing should be approached as a large project, including the utilisation of project control frameworks (such as Prince II) by the prospective CS consumer enterprise. **(2) (7)** • Also refer to DS2 and DS4. • A clear policy should be adopted and implemented regarding who authorises the scaling of services and on which grounds. This policy must be communicated to all relevant stakeholders. **(1) (2)** • Controls (both automated and manual) should be introduced to ensure adherence to the abovementioned policy regarding scaling of services.

COBIT process	Possible risk	Possible control
DS1 Define and manage service levels	• Due to the resulting smaller IT department within the CS consumer enterprise, too little attention may be given to drawing up, monitoring and maintaining a comprehensive internal IT service level framework that aligns internal IT policies and services with business requirements.	• Management of the CS consumer enterprise should pay due attention to drawing up a documented framework of all the IT services required, in line with business requirements. **(1)** • A portion of the savings obtained by the CS consumer enterprise from the utilisation of cloud services should be invested in monitoring service levels of the CS provider, especially monitoring security-related controls. **(2)**
DS2 Manage third-party services	• There may be insufficient service level agreements (SLAs) and other contracts with the CS provider to ensure that effective and efficient IT capability is provided, as well as to ensure that confidentiality and integrity of the CS consumer enterprise's data is preserved by the CS provider. The availability and reliability of IT resources are also crucial. Due to the scale of outsourcing of IT resources, insufficiencies in the SLAs – leading to limited/no recourse with regard to poor or insufficient service – could severely hamper the	• Draw up proper and enforceable (both legally and logistically) SLAs and other contracts with the CS provider, which include remedial and penalty-related agreements. **(1) (2)** • A team of IT, business and legal professionals should inspect/draw up the SLAs and other contracts relating to cloud services. **(2) (5) (7) (11)** • As a minimum, all the risks for which controls were referred to this section (i.e. 'Refer to DS2') should be considered in drawing up the agreements and contracts. **(1) (2)**

COBIT process	Possible risk	Possible control
	CS enterprise's ability to conduct business. **(1) (2) (15)** • Also refer to AI5.	• A CS provider should be selected with great care, using a meticulous selection and approval process. This should include checking of the references and reputation of the CS provider. **(1) (2) (7)** • Third party enterprises who audit the adequacy of CS providers' controls against a pre-set checklist **(2) (11)** and provide certification of accreditation based on the audit outcome, are likely to become increasingly important. A prospective CS consumer enterprise will then be able to check a CS provider's level of certification or accreditation in order to determine the relevant level of controls implemented by the provider. Such checking of certification or accreditation by a prospective CS consumer enterprise will be essential. **(17)** As with cloud computing, the evolvement of such third party certifications are still relatively immature and should only be relied upon after thorough evaluation of the written certification report (i.e. does it address all 'Refer to DS2' issues?). **(12)**

COBIT process	Possible risk	Possible control
DS3 Manage performance and capacity	• The performance of IT resources provided as cloud services by the CS provider may be poor. **(2)** • There may be a delay in the scaling of cloud services or limitations on the scaling of such services. **(16)** • Also refer to PO3.	• Refer to DS2.
DS4 Ensure continuous service	• As cloud services are provided using broad network infrastructure and Internet technologies, the CS consumer enterprise will become critically reliant on this network or Internet access. If access to the network or internet is unavailable (e.g. denial of service attacks) there may be no IT capability available relating to the cloud services subscribed to. **(3)** • Single point of failure (SPOF) risk, including the risk described above in relation to the CS consumer enterprise, may also exist on the CS provider's side, causing interruption of services to the CS consumer enterprise. **(16)** • The CS provider my not implement sufficient	• The CS consumer enterprise should consider upgrading SLAs with their Internet service provider (ISP), or other network infrastructure provider. **(1)** • The CS consumer enterprise should develop a proper continuity plan to ensure continued access to network infrastructure and Internet technologies (e.g. wireless access as a continuity option for fixed line downtime). **(1) (2)** • It may be wise to have a list of pre-authorised 'alternative' CS providers, to ensure continuation of IT capabilities if a CS provider is suddenly unable to deliver the capability. • The CS consumer enterprise could make regular data extraction back-ups of critical data in a format that is

COBIT process	Possible risk	Possible control
	alternate continuation controls, such as off-site backup etc., thereby substantially affecting the CS consumer enterprise in the event of failure. **(1) (2)** • Bankruptcy of the CS provider could cause the loss of IT capability and/or data of the CS consumer enterprise. **(2) (5)**	generally compatible. **(2)** • As these risks, along with security risks (refer to DS5), are so critical, it may be wise for the CS consumer enterprise to take out insurance covering the effects of such service failures. • Also refer to DS2.
DS5 Ensure systems security	• Data is transferred to the CS provider (for processing and/or storage) over a broad network (possibly the Internet). The security of data could be compromised during transfer. **(1) (2) (3) (6)** • Data is transferred to the CS provider (for processing and/or storage), which means that the CS consumer enterprise becomes reliant on the security controls of the CS provider with relation to its data. The CS provider's controls may be inadequate. **(1) (2) (6) (12)** • Currently, data needs to be decrypted for it to be processed (IaaS), making it extremely vulnerable to theft and/or loss of confidentiality during this	• Data transfer controls should be implemented, such as encryption and the use of a proper VPN. **(1) (2)** • A Web Systems Security (WS-Security) specification should be adopted as part of the security policy by both the CS consumer enterprise and the CS provider. **(3)** • Data that is stored on a CS provider's resources should be in an encrypted format. **(6)** • CS providers should guarantee (and demonstrate) comprehensive compartmentalisation of resources and data belonging to CS consumers to limit the possibility of CS consumers accidentally or maliciously gaining access to other CS consumers'

COBIT process	Possible risk	Possible control
	stage. **(2)** • The CS provider could have access to the data transferred and could be forced to disclose information relating to the data. This is especially relevant as jurisdictions governing the CS consumer enterprise and the CS provider may be different. **(1) (6)** • Due to the multi-tenant characteristic of cloud computing, many consumers' data would be processed and/or stored by a single CS provider. If insufficient controls exist at the CS provider, or if systems failure occurs, one tenant (consumer) may accidentally or intentionally gain access to another tenant's data ('comingling of data'). **(1) (2) (3) (6) (12) (16)** • Cloud computing services are dynamically scaleable, allowing the addition of users, and, additionally, are accessible from anywhere (any Internet-enabled device or thin client device, irrespective of location). Identity and access	data. **(2)** • As these risks are so critical, it may be wise for the CS consumer enterprise to take out insurance covering the effects of such service failures. • Also refer to DS2 and AI5. • Refer to DS2 – specifically: the CS provider should guarantee very reliable identity and access management controls (authentication etc.). **(2)** • The CS consumer enterprise should also develop appropriate identity and access management policies and controls to control risks on its own side, as it would be able to scale users on-demand by itself. **(2)**

COBIT process	Possible risk	Possible control
	management therefore becomes much more complex and any failure may have an increased effect on the CS consumer enterprise. **(2)**	
DS6 Identify and allocate cost	• If the CS provider's accounting system does not provide for the measurement of usage by different groups within the CS consumer enterprise, the task of allocating such costs may become very onerous.	• Refer to DS2.
DS7 Educate and train users	• Refer to AI4.	• Refer to AI4.
DS8 Manage service desk and incidents	• Inadequate service desk services may be provided by the CS provider. • The CS provider's service desk processes, tools and hours may be incompatible with the processes and hours of the CS consumer enterprise (e.g. disparate time zones). **(2)**	• Refer to DS2.
DS9 Manage the configuration	• Most aspects of configuration management are outsourced to the CS provider. The risk exists that the CS provider's controls will not be adequate. **(2)**	• Refer to DS2.

COBIT process	Possible risk	Possible control
DS10 Manage problems	• Most aspects of problem management are outsourced to the CS provider. The risk exists that the CS provider's controls will not be adequate. **(1) (12)**	• Refer to DS2.
DS11 Manage data	• Refer to DS5 and PO2. • The dynamic nature of cloud computing services (e.g. a CS provider may use multiple locations and devices for storage) can cause uncertainty relating to where the data of the CS consumer enterprise actually resides. This may cause time delays in the recovery of data, as well as legal implications regarding the jurisdiction under which the data resides. **(1) (5) (6)** • Upon termination of a contract with a CS provider, the data of the CS consumer enterprise which is left on the CS provider's infrastructure, may not be properly deleted or may even be maliciously disclosed by the CS provider. The data may possibly also be withheld by the CS provider until full payment for services is received	• Refer to DS5 and PO2. • Refer to DS2.

COBIT process	Possible risk	Possible control
	(or even for other reasons). **(2) (8)**	
DS12 Manage the physical environment	• Most aspects of managing the physical environment are outsourced to the CS provider. The risk exists that the CS provider's controls will not be adequate. **(1) (2)**	• Refer to DS2.
DS13 Manage operations	• Most aspects of operations management are outsourced to the CS provider. The risk exists that the CS provider's controls will not be adequate. **(1) (2)** • Refer to DS5.	• Refer to DS2. • Refer to DS5.
ME2 Monitor and evaluate internal control	• Smaller enterprises' data are usually not attacked at regular intervals, as they (data or enterprise) are of too low a value to cyber terrorists. The CS provider storing data of various smaller and larger CS consumer enterprises does, however, represent a high value target for a potential attack, as a shared pool of data will be subject to such an attack. **(6)** The risk of a smaller CS consumer enterprises therefore increases (from being unappealing for attack, to being appealing	

COBIT process	Possible risk	Possible control
	due to the amalgamation with other enterprises' data at the CS provider). • There is a risk of non-compliance of the CS consumer enterprise and/or its data with the laws and regulations governing the CS provider (if they are under different jurisdiction) and *vice versa*, causing liability **(1)**. • There is a risk of insufficient internal controls at the CS provider (these could be in general, or in the case of tighter controls being required by the consumer enterprise – due to different jurisdictions or simply better governance at the CS consumer enterprise). **(1) (2) (5) (6) (11)** • There could be non-adherence by users inside the CS consumer enterprise to security policies regarding which data may be processed/stored using the cloud services (IaaS, PaaS and SaaS) and which are too sensitive for cloud services. **(12)**	• Refer to DS2 and AI5. • Clear policies must be developed, communicated and enforced by the CS consumer enterprise regarding sensitive data which should possibly not be allowed to be processed/stored using cloud services, and other less sensitive data.
ME3 Ensure compliance with external requirements	• Refer to ME2.	• Refer to ME2.

Numbered list of references:

(1) ISACA 2009.

(2) Cloud security alliance 2009.

(3) Jensen *et al*. 2009.

(4) Hill & Humphrey 2010.

(5) Marston *et al*. 2011.

(6) Subashini & Kavitha 2011.

(7) Sanders 2010.

(8) Hayes 2008.

(9) Feiman 2010.

(10) Mingay & Govekar 2010.

(11) Heiser 2009.

(12) Heiser 2010.

(13) Knipp 2011.

(14) Pescatore 2010.

(15) Pring 2010.

(16) Winkler 2011a.

(17) Winkler 2011b.

5.2 - Summary of main risks for consumer enterprise

Cloud computing's main risks, as perceived from the point of view of a consumer of cloud services, hinge on two characteristics of the service offering, namely outsourcing and the use of Internet technologies or wide network access to deliver these services.

Outsourcing results in the loss of a level of control by becoming dependent on another party to fulfil the enterprise's needs and to provide adequate controls. Use of Internet technologies or wide area network access to access IT capabilities and data creates dependency on these possibly more vulnerable access paths. The main risks arising from these dependencies and vulnerabilities are risks relating to continuity issues and security of information. Continuity is complicated by the fact that downtime of Internet or network access, or downtime at the cloud service provider, could translate into unavailability of all IT capabilities outsourced by the consumer enterprise. Security is complicated as the cloud service provider utilises a multi-tenant model and therefore stores various enterprises' data at any one physical location, creating the risk of the leakage of data belonging to one consumer to another, or to unauthorised third parties. In addition, the fact that all data relating to the IT capabilities which are outsourced travels on the Internet or network in order to be accessed or processed, creates the risk of unauthorised access to, or manipulation or corruption of data.

A few of the main secondary risks identified are that of non-compliance with laws and regulations due to the fact that the cloud service consumer enterprise and the cloud service provider reside in different jurisdictions, as well as the risk of not being able to switch from one cloud provider to another (non-portability issues).

5.3 - Summary of main controls for consumer enterprise

The best controls that a prospective cloud consuming enterprise can implement to mitigate risks relate to the selection of an appropriate cloud service provider(s). No time and consultation should be spared in selecting the appropriate and most reliable cloud service provider that fits the specific enterprise's need and risk profile.

One of the main sources of risk in the cloud computing environment, as discussed in Section 5.2, is that of the outsourcing of the provision of IT capabilities. In this case, the importance of the service level agreement (SLA) with the cloud service provider becomes critical. This can be deduced from Table 5.1, by taking into consideration all the risk mitigating controls which refer to the Delivery and Support process 2 (DS2).

Two approaches are suggested to ensure that reliance can be placed on a cloud service provider's undertakings in the SLA. The first is based on the Cloud Security Alliance's (2009) publication termed 'Security Guidance for Critical Areas of Focus in Cloud Computing V2.1'. This approach is based on the inspection and auditing of the controls of the cloud service provider as if it were the consumer enterprise's own controls. This entails that the cloud service provider would have to allow the consumer full access to its internal policy documents as well as access to physically inspect the implementation of these policies. In addition, this would negate the cost advantage that the consumer enterprise could have gained by placing reliance on a provider's controls. In fact, the auditing of these controls may be very expensive for the consumer enterprise due to the different locations of the cloud service provider's operations and the need to cooperate with the cloud service provider in terms of access provision for the performance of these audits.

The second approach is the certification of cloud service providers by third party certification bodies or enterprises that assess and rate the cloud service providers' risk mitigating controls on behalf of all cloud service consumer enterprises (Heiser 2009, Winkler 2011a). This certification and rating should be used by prospective cloud service consumers to select a cloud service provider with the appropriate certified rating for the level of controls and security required by the relevant prospective consumer enterprise. It logically follows that the cost of cloud services provided by higher rated cloud service providers would also be higher due to the cost of implementing the higher level of control.

However, Heiser (2009) states that it may take some time for the certifications to mature and provide advanced reliability. To combat the immaturity issue of the certifications, a prospective consumer enterprise should inspect certification reports to ensure that, at the very least, all issues referred to at DS2 in Table 5.1 are indeed dealt with in the report.

To mitigate the risks relating to the use of Internet technologies and network access, the enterprise should update its SLAs with the provider of these technologies (e.g. Internet service provider). This may entail switching to higher level options (in terms of continuity and security) available from these service providers to ensure adequate continuity of service as well as security. Although these would probably be more expensive options, the increased cost will be negated by the savings achieved by utilising cloud services.

Section 6 - Conclusion

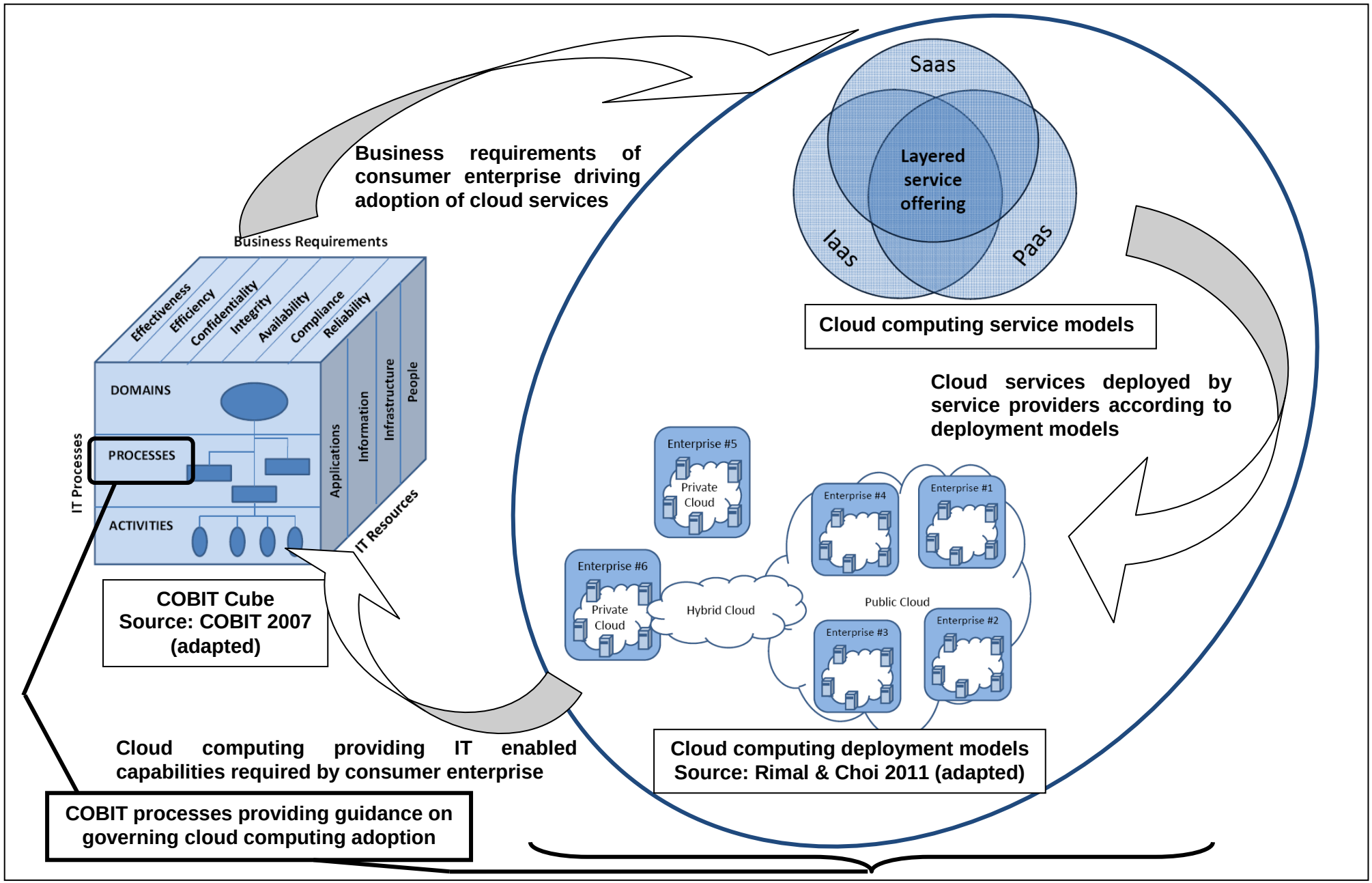
A very simple manner of identifying and interpreting the benefits and risks of cloud computing would be to view them as a return to the mostly archaic concept of the mainframe supercomputer. The first difference being that the "mainframe computer" is not owned or managed by the enterprise, but by a provider of cloud services. Secondly, the "mainframe computer" is usually used by the service provider to provide services to various enterprises at the same time (public or hybrid cloud). Thirdly, the "mainframe computer" is accessed using Internet technologies or wide network access.

The adoption of cloud computing offers important benefits to a consumer enterprise, most notably possible cost savings due to heavily reduced capital expenditure on IT capabilities and the ability to rapidly scale IT capabilities according to each period's specific requirements. Furthermore, the management of the enterprise can focus on the enterprise's core objectives as much of the IT controls which previously may have required continual management focus are now outsourced.

However, the outsourcing of the provision of IT capabilities results in extreme reliance being placed on a third party, namely the cloud service provider, to implement proper controls to satisfy the consumer enterprise's security needs. Furthermore, as is customary for evolving IT paradigms, new or amended risks evolve for which previous paradigms' controls will be insufficient.

Figure 6.1 provides an overview of how the COBIT framework can assist a prospective consumer enterprise on the adoption of cloud computing.

Figure 6.1 - Cloud computing and COBIT Cube



The following can be derived from Figure 6.1:

- The business requirements and imperatives of a prospective cloud services consumer enterprise drives the decision of whether or not to adopt cloud computing;
- Cloud computing services which may be adopted can either be Infrastructure as a Service (hardware related), Platform as a Service (platform related) or Software as a Service (software related), or these services may be layered upon each other as a combined service, or even be sourced from various providers;
- These cloud computing services may be deployed by the provider as public, private, community (for a specific community) or hybrid cloud services;
- A prospective consumer enterprise can select the appropriate deployment model, again based on its business requirements and imperatives;
- Cloud computing thus provides the IT enabled capabilities required by the consumer enterprise as IT resources, and lastly;
- As illustrated in Sections 4 and 5 of this study, COBIT's IT processes can be used to provide guidance on governance of cloud computing adoption.

A consumer enterprise may gain a competitive advantage from the adoption of cloud computing, but should evaluate each offering termed as a cloud or related offering with care and pay due attention to the issues raised in this study.

The business imperatives of each prospecting cloud service consumer enterprise may very well determine whether or not the enterprise should become an early adopter of a cloud computing IT approach. If one of the business's imperatives is strict confidentiality of most data, for example, cloud computing may not be a preferred approach at this stage. On the other hand, if efficiency, rapid scalability and mobility are critical business imperatives (separately or in combination), early adoption of cloud computing may offer significant advantages.

It is envisaged that, as the evolution of the cloud computing paradigm reaches maturity, so will the associated risk mitigating controls, which should effectively lower the risk associated with the adoption of cloud computing, making it viable for more and more consumer enterprises (Smith 2011).

This study is presented in business and control terms, but does not cover the technical discussions on the risks and technical implementation techniques and procedures needed to activate the identified controls. Further research could consist of mapping possible technical control techniques and procedures to the identified controls. This may be especially valuable, as business management who are responsible for governance of the enterprise, including IT governance, often lack in-depth technical IT knowledge to communicate the controls required effectively to IT professionals within the cloud service provider. Conversely, the IT professionals often do not comprehend the governance controls required by the consumer enterprise's management and how they link to the technical procedures, if they are only expressed in business terminology. Additionally, further research may also separate incremental benefits and risks per type of cloud service model.

Lastly, a research area of interest, which may be worthwhile for a prospective cloud services consumer to take note of as a possible solution to many of the risks of cloud computing, is that of 'fully homomorphic encryption' (Anthes 2010). The concept behind this research is to encrypt data in such a manner that operations can be performed on the data without decrypting it in order to do so. The effect with reference to infrastructure as a service, for example, would be that the decryption of data would not be required in order for operations using the cloud service provider's processing capacity to be performed on that data. The result is that no access to data can be gained during transmission or the execution of operations on the data, as it remains in an encrypted format. However, this had not yet been developed to the level of a feasible solution at the time this study was performed.

References:

Abraham, K.G. & Taylor, S.K. 1993, "Firms' use of outside contractors: Theory and evidence", Working Paper #4468, *NBER Working Paper Series*, National Bureau of Economic Research, Cambridge, USA.

Amazon Web Services 2011, "*Summary of the Amazon EC2 and Amazon RDS service disruption in the US East Region*", Media release, http://aws.amazon.com/message/65648/ Accessed 25 May 2011.

Anthes, G. 2010, "Security in the cloud", *Communications of the ACM,* vol. 53, no. 11, pp. 16-18.

Blandford, R. 2011, "Information security in the cloud", *Network Security,* vol. 2011, no. 4, pp. 15-17.

Cloud security alliance 2009, "Security guidance for critical areas of focus in cloud computing V2.1", *Cloud security alliance,* http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf Accessed 12 July 2011.

COBIT 2007, "*COBIT 4.1.*", COBIT Steering Committee, IT Governance Institute, Rolling Meadows, Illinois, USA.

COSO 2010, "*COSO announces project to modernize internal control - integrated framework*", Committee of Sponsoring Organisations of the Treadway Commission, News release, 18 November 2010, http://www.coso.org/documents/COSOReleaseNov2010.pdf Accessed 8 August 2011.

Feiman, J. 2010, "How to keep your job from disappearing into the cloud", *Gartner,* Research report, 26 August 2010, http://my.gartner.com/resources/206000/206018/how_to_keep_your_job_from_di_206018.pdf Accessed 12 July 2011.

Giglia, N. & De Orlov, L.L. 2011, "*The last cloud computing definition you'll ever need*", TechTarget, http://searchcloudcomputing.techtarget.com/feature/The-last-cloud-computing-definition-youll-ever-need Accessed 4 July 2011.

Hayes, B. 2008, "Cloud computing", *Communications of the ACM,* vol. 51, no. 7, pp. 9-11.

Heiser, J. 2009, "What you need to know about cloud computing security compliance", *Gartner*, Research report, 13 July 2009, http://my.gartner.com/resources/168300/168345/what_you_need_to_know_about__168345.pdf Accessed 11 July 2011

Heiser, J. 2010, "Analyzing risk dimensions of cloud and SaaS computing", *Gartner,* Research report, 17 March 2010, http://my.gartner.com/resources/174800/174873/analyzing_the_risk_dimension_174873.pdf Accessed 12 July 2011.

Hill, Z. & Humphrey, M. 2010, "CSAL: A cloud storage abstraction layer to enable portable cloud applications", *Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*, pp. 504-511.

Hiner, J. 2011, "Apple cloud vs. Google cloud: the philosophical differences", *TechRepublic*, Blog, Posted 8 June 2011, http://www.techrepublic.com/blog/hiner/apple-cloud-vs-google-cloud-the-philosophical-differences/8492?tag=nl.e098 Accessed 14 July 2011.

ISACA 2009, "Cloud computing: Business benefits with security, governance and assurance perspectives", *ISACA Emerging technology white paper,* Rolling Meadows, Illinois, USA, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx Accessed 22 March 2011.

ISACA 2011, "*COBIT 5 Initiative—Status Update*", Media release, http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx Accessed 13 March 2011.

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L.L. 2009, "On technical security issues in cloud computing", *CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing*, pp. 109-116.

Knipp, E. 2011, "Cloud computing and emerging economies: a mixed opportunity", *Gartner,* Research report, 1 February 2011, http://my.gartner.com/resources/209300/209391/cloud_computing_and_emerging_209391.pdf Accessed 11 July 2011.

Kushida, K.E., Murray, J. & Zysman, J. 2011, "Diffusing the Cloud: Cloud Computing and Implications for Public policy", *Journal of Industry, Competition and Trade,* vol. 11, no. 3, pp. 209-237.

Marston, S., Li, Z., Bandyopadhyay, S. & Ghalsasi, A. 2011, "Cloud computing – the business perspective", *Decision support systems,* vol. 51, pp. 176-189.

Mell, P. & Grance, T. 2011, "The NIST definition of cloud computing", *Special Publication 800-145*, National Institute of Standards and Technology, Maryland, USA.

Mingay, S. & Govekar, M. 2010, "Does cloud computing have a 'green' lining?", *Gartner,* Research report, 14 October 2010, http://my.gartner.com/resources/206900/206983/does_cloud_computing_have_a__206983.pdf Accessed: 24 May 2011.

Pescatore, J. 2010, "Securing and managing private and public cloud computing", *Gartner,* Research report, 2 September 2010, http://my.gartner.com/resources/206000/206019/securing_and_managing_privat_206019.pdf Accessed 11 July 2011

Plummer, D.C., Smith, D.M., Bittman, T.J., Cearley, D.W., Cappuccio, D.J., Scott, D., Kumar, R. & Robertson, B. 2009, "Five refining attributes of public and private cloud computing", *Gartner*, Research report, 5 May 2009, http://my.gartner.com/resources/167100/167182/five_refining_attributes_of__167182.pdf Accessed 25 May 2011.

Pring, B. 2010, "Cloud computing: the next generation of outsourcing", *Gartner,* Research report, 1 November 2010, http://my.gartner.com/resources/207200/207255/cloud_computing_the_next_gen_207255.pdf Accessed 24 May 2011.

Rimal, B.P. & Choi, E. 2011, "A service-oriented taxonomical spectrum, cloudy challenges and opportunities of cloud computing", *International journal of communication systems,* May 2011, pp. 1099-1131.

Sanders, A. 2010, "A Phased Approach to Reviewing Cloud Computing Risks", *ISSA Journal*, October 2010, p.24-27.

Smith, D.M. 2010, "Hype cycle for cloud computing, 2010", *Gartner,* Research report, 27 July 2010, http://my.gartner.com/resources/201500/201557/hype_cycle_for_cloud_computi_201557.pdf Accessed 14 July 2011.

Smith, D. M. 2011, "Hype cycle for cloud computing, 2011", *Gartner*, Research report, 27 July 2011, http://my.gartner.com/resources/214900/214915/hype_cycle_for_cloud_computi_214915.pdf Accessed 21 September 2011.

Sony Online Entertainment 2011, "*Sony Online Entertainment announces theft of data from its systems*", Media release, 3 May 2011, http://www.sony.net/SonyInfo/News/Press/201105/11-0503E/index.html Access 26 May 2011.

Subashini, S. & Kavitha, V. 2011, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications,* vol. 34, no. 1, pp. 1-11.

Tuttle, B. & Vandervelde, S.D. 2007, "An empirical examination of COBIT as an internal control framework for information technology", *International Journal of Accounting Information Systems,* vol. 8, 2007, pp. 240-263.

Vaquero, L. M., Rodero-Meniro, L., Caceres, J. & Lindner, M. 2009, "A Break in the clouds: towards a cloud definition", *Communication Review,* vol.3 9, no. 1, pp. 50-55.

Winkler. J.R. 2011a, "Chapter 1 - Introduction to Cloud Computing and Security" in *Securing the Cloud,* Syngress, Boston, pp. 1-27.

Winkler, J.R. 2011b, "Chapter 6 - Key Strategies and Best Practices" in *Securing the Cloud,* Syngress, Boston, pp. 153-185.