African Journal of Business Management Vol.6 (37), pp. 10185-10194, 19 September, 2012
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM12.679
ISSN 1993-8233 ©2012 Academic Journals

Full Length Research Paper

Cloud computing adoption: Control objectives for information and related technology (COBIT) - mapped risks and risk mitigating controls

Zacharias Enslin

Department of Accounting, Stellenbosch University, Private Bag X1, Matieland, 7602, South Africa.
E-mail: zenslin@sun.ac.za. Tel: 021 808 3085. Fax: 021 886 4176.

Accepted 3 September, 2012

Cloud computing has emerged as one of the most hyped information technology topics of the decade. 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. The aim of this study is to inform enterprise managers, who possess business knowledge and who may also be knowledgeable on the main aspects of COBIT, about the significant incremental risks this new technological advancement may expose the enterprise to if the proposals of possible controls are implemented by the prospective consumer enterprises to mitigate the incremental risks of cloud computing. An IT governance control framework was used to systematically identify and categorise the significant incremental risks and to assist in identifying the possible risk mitigating controls. It was discovered that the major risks of cloud computing adoption would be outsourcing of IT function (possibly across judicial borders) and the use of internet or wide area access technologies.

Key words: Cloud computing, information technology (IT), control objectives for information and related technology (COBIT), IT governance, IT related risk.

INTRODUCTION

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 et al., 2009). Consequently, by using cloud computing services a consumer enterprise will become critically reliant on a number of outside parties (internet service provider (ISP) or virtual private network (VPN) provider and cloud service provider (CSP) with regard to its IT functionality and data security.

The adoption of cloud computing offers important benefits to a cloud service consumer (CSC) 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 (ISACA, 2009; Knipp, 2011; Pring, 2010; Subashini and Kavitha, 2011). Furthermore, the management of the CSC 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 (Knipp, 2011; Pring, 2010; Subashini and Kavitha, 2011).

Recently “cloud failures” have occurred at some high level CSP’s, 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 aforementioned “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.

Definition of cloud computing

Gartner research firm’s definition was provided in the aforementioned area. This subarea serves to briefly further elucidate the definition of cloud computing.

The cornerstone of cloud computing is the delivery of IT-enabled capabilities as services which are referred to as cloud services (Plummer et al., 2009; ISACA, 2009; Mell and Grance, 2011). These services entail "ubiquitous, convenient, on-demand network access (internet, virtual private network or wide area network based)[1] 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 and Grance, 2011).

Most CSC enterprises currently adopt cloud computing only for certain IT capabilities and retain other functions in-house (Smith, 2011).

For guidance on the main characteristics, deployment models and service models are given in ISACA (2009) and Plummer et al. (2009).

Research problem

Cloud computing has emerged as one of the most hyped topics in computing (Smith, 2010). However there is a shortage of research literature aimed at guiding prospective CSC enterprises (including business) in the adoption of cloud computing (Marston et al., 2011).

Business professionals and enterprise managers are expected to increasingly take control of the enterprise's IT function (Plummer et al., 2011), although they are not specifically educated to handle the very specific risks associated with an emerging IT paradigm such as cloud computing.

Research objectives

This study assists in fulfilling the need for consumer guidance by identifying significant 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 focus is specifically on incremental risk, thus additional risk that the adoption of cloud computing may expose a prospective CSC enterprise to.

RESEARCH METHODOLOGY

Significant incremental risks associated with the adoption of cloud computing by a prospective CSC enterprise were identified by using a recognised IT control framework. The control framework then assisted in identifying risk mitigating controls.

Identified significant incremental risks and selected risk mitigating controls were confirmed and supplemented, by a literature study on cloud computing related literature. A prospective CSC enterprise can thus refer to the literature if further detail on a specific issue is required.

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 CSC enterprise, fewer security risks regarding multi-tenancy exist and the CSC enterprise would normally have more control over the services developed for it. Risks relating to these areas are therefore also decreased (Blandford, 2011).

It should be noted that cloud computing is an evolving paradigm (Smith, 2010; Mell and Grance, 2011) with new risks certain to develop as the computing paradigm matures.

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 enterprise 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 and Vandervelde, 2007).

Accordingly, this study identified significant incremental risks related to the adoption of cloud computing by a prospective CSC enterprise, using COBIT and its 34 IT control processes (COBIT, 2007) as framework. Significant incremental risks were identified by analysing the effects that the characteristics of cloud computing (ISACA, 2009; Plummer et al., 2009) would have on each relevant IT control process. Risks were confirmed and additional incremental risks were identified by means of a literature study of cloud computing related literature.

Tuttle and 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.

Consequent to the identification of the incremental risks, COBIT's control processes were used to identify and select risk mitigating controls. Again, the selected risk mitigating controls were confirmed and supplemented by means of a further literature study of cloud computing related literature.

SIGNIFICANT RISKS AND CONTROLS RELATING TO CONSUMER ENTERPRISE

The research regarding the significant incremental risk and possible risk mitigating controls are presented in Table 1 which 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).

COBIT 4.1 is divided into four domains, which are further subdivided into a total of 34 processes (COBIT, 2007). The processes are numbered in the following manner:

1. 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
2. Secondly, the processes in each domain are numbered.

[1] Author's own addition between brackets

Table 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	Hype around cloud computing may encourage the adoption thereof without careful and objective consideration of advantages and disadvantages (including risks) with respect to each CSC enterprise's unique characteristics and requirements. This may lead to an incorrect decision to incorporate cloud computing into the prospective CSC enterprise's strategic IT plan (7) (13) (16).	1. Proper planning and investigation, as introduced by this study in the whole of table 1, should be done to ensure cloud services are the correct solution to a prospective CSC enterprise's IT requirements (7) (13). 2. A definite incorporation of cloud computing into a prospective CSC enterprise's IT plan should be considered with reference to the CSC enterprise's unique situation (for example, if confidentiality and security of information is a dominant business imperative, adoption of cloud computing may not be desirable), by a high level team of IT, business management and legal professionals. All stakeholders of the CSC enterprise should be consulted (7) (10) (13).
PO2 Define information architecture	The outdated information architecture model of the CSC enterprise may allow the creation of data elements that are incompatible with the CSP's platform (7).	1. Ensure that the information architecture model does not only account for the CSC enterprise's own architecture, but also for the CSP's specific architecture (including platform) (1) (7). 2. Also refer to DS2.
PO3 Determine technological direction	1. The IT plan of the CSC 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. 2. Major disinvestment in IT architecture by the CSC enterprise to realise benefits of cloud computing may lead to major future capital expenditure if the technological direction of the CSC enterprise were to change back to an in-house model in the future. 3. Cloud computing may not be the correct technological direction for a CSC enterprise located in geographical regions with underdeveloped Internet infrastructure to support efficient use of cloud computing, causing latency problems, for example (especially relevant in developing countries) (9). 4. As cloud computing is still an evolving paradigm, the possibility exists that risks and threats that are not yet defined may subsequently be discovered.	1. Ensure that the IT plan of the CSC enterprise as a whole aligns with the characteristics of cloud computing to ensure full realisation of the benefits (1) (7). Examples include that the IT plan specifically state that thin client devices are desirable and that server investment is not allowed without the highest level of authorisation (if at all). 2. Develop the correct approach to implement cloud computing to ensure that the CSC 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 (10) (12). 3. 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 (5) (13). 4. Evaluate the adequacy of the speed and reliability of Internet offerings in the CSC enterprise's geographical region, before adopting cloud computing (9). 5. Also refer to DS4.
PO4 Define the IT processes, organisation and relationships	Refer to PO1 and PO2.	Refer to PO1 and PO2.
PO5 Manage IT investment	1. Prospective CSC 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 (7) (9) (16). 2. The most reliable public CSPs are currently located in a limited number of larger countries. They may, therefore, require payment in foreign currencies if the CSC enterprise is not located in the same country as the CSP. This will expose the CSC enterprise to additional foreign currency risk (9).	1. 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 (9). 2. Refer to DS2.
PO7 Manage IT human resources	1. Some IT staff of the CSC enterprise may become redundant if cloud computing is adopted (2). Labour laws may make the termination of their services challenging.	1. Conduct proper IT staff planning and projections, which also take the cost of the termination of redundant staff into consideration when deciding on cloud computing as a possible technological direction.

Table 1. Contd.

	2. 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 CSC enterprise, who may be concerned about their job security (2) (10). This may also lower the morale of IT staff (9).	2. 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 (2).
PO8 Manage Quality	Most aspects of quality management are outsourced to the CSP. The risk exists that the CSP's quality of service will not be adequate.	Refer to DS2.
PO9 Assess and manage IT risks	1. Some aspects of risk assessment and management are outsourced to the CSP. The risk exists that the CSP's controls will not be adequate (1) (4) (7). 2. There is increased exposure to IT-related risks for the CSC enterprise due to the incremental risks of cloud computing not being properly understood or not being properly incorporated into the risk management framework (1) (7).	1. Refer to DS2. 2. Ensure that a proper combination of skilled professional staff forms part of the risk assessment and management team of the CS consumer enterprise (7) (14). The team should, for example, include professionals knowledgeable on cloud computing, as well as legal professionals knowledgeable on cross jurisdiction trade. 3. Ensure that the CSC enterprise's risk management framework incorporates the incremental risks associated with cloud computing into the risk management process (1) (7) (17). The second column in this table lists the most significant of those risks. 4. 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.
AI2 Acquire and maintain application software	1. Current software of the CSC enterprise, or the acquisition of new software by the CSC enterprise, may not be compatible with the CSP's platform (relating to Platform as a Service (PaaS)) (6) (10). 2. The CSP's software maintenance may be lacking (relating to Software as a Service (SaaS)) in terms of keeping up with patches and upgrading versions (1).	1. Refer to PO2. 2. Refer to DS2.
AI3 Acquire and maintain technology infrastructure	1. The current infrastructure of the CSC enterprise, or the acquisition of infrastructure (e.g. thin client device) by the CSC enterprise, may not be compatible with the CSP's Internet technologies/network access. 2. The CSP's infrastructure maintenance may be lacking (relating to Infrastructure as a Service (IaaS) and PaaS) in terms of keeping up with new infrastructure technology (that is, faster processors) and upgrading versions of platforms (1).	1. Refer to PO2. 2. Refer to DS2.
AI4 Enable operation and use	Standardised user manuals and/or training of the CSP may not consider the specific CSC enterprise's circumstances, as they are written or conducted for the 'standard' CSC.	If the CSC enterprise's circumstances differ from that of the 'standard' CSC (examples include extensive travelling in developing countries by CSC employees, where internet connectivity is limited, or if the CSC is highly specialised), the CSC enterprise may need to consult with the CSP on possible specialised training (refer to DS2), or conduct such training itself.
AI5 Procure IT resources	1. The contract and/or Service Level Agreement (SLA) with the CSP may not be enforceable. Cloud services are provisioned to consumers independent of the location of the CSP. Cloud services are available across juristic borders (that is, globally), making it difficult to ascertain under which country's jurisdiction a contract and/or SLA may fall (1) (7) (9). 2. Also refer to DS2.	Cloud contracts which could possibly span juristic borders should be reviewed by legal advisors knowledgeable in international law (1).

Table 1. Contd.

AI6 Manage changes	1. Some aspects of change management are outsourced to the CSP. The risk exists that the CSP's control over changes may not be adequate (5). 2. Changing from one CSP to another may be an onerous process, as the different CSPs have their own platforms, which may result in compatibility issues when changing from one CSP to another (1) (6) (10). 3. Implementing cloud computing may result in the loss of data or IT capabilities of the CSC enterprise due to incompatibility issues or other failure (4). 4. 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 CSC enterprise (1) (7).	1. The CSP 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 CSP to another. If possible, select a CSP that has a reputation as a reliable supplier of IT products and service and which uses generally established standards to ensure provider portability (1). 2. Develop and implement compensating change-related controls (i.e. back-up, contingency plans etc.) before implementing cloud computing (1) (4) or before changing from one CSP to another. 3. 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 CSC enterprise (1) (14). 4. Also refer to DS2 and DS4. 5. 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) (7). 6. Controls (both automated and manual) should be introduced to ensure adherence to the abovementioned policy regarding scaling of services.
DS1 Define and manage service levels	Due to the resulting smaller IT department within the CSC 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.	1. Management of the CSC enterprise should pay due attention to drawing up a documented framework of all the IT services required, in line with business requirements (7). A multidisciplinary team should be established for this purpose (IT, business and legal professionals). 2. A portion of the savings obtained by the CSC enterprise from the utilisation of cloud services should be invested in monitoring service levels of the CSP, especially in monitoring security-related controls (1).
DS2 Manage third-party services	1. There may be insufficient SLAs and other contracts with the CSP to ensure that effective and efficient IT capability is provided, as well as to ensure that confidentiality and integrity of the CSC enterprise's data is preserved by the CSP. 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 CSC enterprise's ability to conduct business (1) (7) (13). 2. Also refer to AI5.	1. Draw up proper and enforceable (both legally and logistically) SLAs and other contracts with the CSP, which include remedial and penalty-related agreements (1) (7). 2. A team of IT, business and legal professionals should inspect/draw up the SLAs and other contracts relating to cloud services (1) (4) (10) (14). 3. 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) (7). 4. A CSP 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) (7) (14). 5. Third party enterprises who audit the adequacy of CSPs' controls against a pre-set checklist and provide certification of accreditation based on the audit outcome (1) (4), are in the process of evolving. A prospective CSC enterprise will soon be able to (and critically must then) check a CSP's level of certification or accreditation in order to determine the relevant level of controls implemented by the provider (17). 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?) (5).

Table 1. Contd.

DS3 Manage performance and capacity	1. The performance of IT resources provided as cloud services by the CSP may be poor (1). 2. There may be a delay in the scaling of cloud services or limitations on the scaling of such services (16). 3. Also refer to PO3.	Refer to DS2.
DS4 Ensure continuous service	1. As cloud services are provided using broad network infrastructure and Internet technologies, the CSC 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 (8). 2. Single point of failure (SPOF) risk, including the risk described above in relation to the CSC enterprise, may also exist on the CSP's side, causing interruption of services to the CSC enterprise (16). 3. The CSP my not implement sufficient alternate continuation controls, such as off-site backup etc., thereby substantially affecting the CSC enterprise in the event of failure (1) (7). 4. Bankruptcy of the CSP could cause the loss of IT capability and/or data of the CSC enterprise (1) (10).	1. The CSC enterprise should consider upgrading SLAs with their ISP, or other network infrastructure provider (7) to ensure higher reliability and better security. 2. The CSC enterprise should develop a proper continuity plan to ensure continued access to network infrastructure and Internet technologies (for example, wireless access as a continuity option for fixed line downtime) (1) (7). 3. It may be wise to have a list of pre-authorised 'alternative' CSPs, to ensure continuation of IT capabilities if a CSP is suddenly unable to deliver the capability. 4. The CSC enterprise could make regular data extraction back-ups of critical data in a format that is generally compatible (1). 5. As these risks, along with security risks (refer to DS5), are so critical, it may be wise for the CSC enterprise to take out insurance covering the effects of such service failures. 6. Also refer to DS2.
DS5 Ensure systems security	1. Data is transferred to the CSP (for processing and/or storage) over a broad network (possibly the Internet). The security of data could be compromised during transfer (1) (7) (8) (15). 2. Data is transferred to the CSP (for processing and/or storage), which means that the CSC enterprise becomes reliant on the security controls of the CSP with relation to its data. The CSP's controls may be inadequate (1) (5) (7) (15). 3. 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 stage (1). 4. The CSP 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 CSC enterprise and the CSP may differ (7) (15). 5. Due to the multi-tenant characteristic of cloud computing, many CSCs' data would be processed and/or stored by a single CSP. If insufficient controls exist at the CSP, or if systems failure occurs, one tenant (consumer) may accidentally or intentionally gain access to another tenant's data ('comingling of data') (1) (7) (8) (5) (15) (16). 6. Cloud computing services are dynamically scalable, 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 management therefore becomes much more complex and any failure may have an increased effect on the CSC enterprise (1).	1. Data transfer controls should be implemented, such as encryption and the use of a proper VPN (1) (7). 2. A Web Systems Security (WS-Security) specification should be adopted as part of the security policy by both the CSC enterprise and the CSP (8). 3. Data that is stored on a CSP's resources should be in an encrypted format (15). 4. CSPs should guarantee (and demonstrate) comprehensive compartmentalisation of resources and data belonging to CSCs to limit the possibility of CSCs accidentally or maliciously gaining access to other CSCs' data (1). 5. As these risks are so critical, it may be wise for the CSC enterprise to take out insurance covering the effects of such service failures. 6. Also refer to DS2 and AI5. 7. Refer to DS2 – specifically: the CSP should guarantee very reliable identity and access management controls (authentication etc.) (1). 8. The CSC enterprise should also develop appropriate identity and access management policies and controls to control risks on its own side (examples include resource scaling only allowed if done by high level manager, combined with username and password, and possibly biometric, based access to resource scaling), as it would be able to scale users on-demand by itself (1).
DS6 Identify and allocate cost	If the CSP's accounting system does not provide for the measurement of usage by different groups within the CSC enterprise, the task of allocating such costs may become very onerous.	Refer to DS2.

Table 1. Contd.

DS7 Educate and train users	Refer to AI4.	Refer to AI4.
DS8 Manage service desk and incidents	1. Inadequate service desk services may be provided by the CSP. 2. The CS provider's service desk processes, tools and hours may be incompatible with the processes and hours of the CSC enterprise (e.g. disparate time zones) (1).	Refer to DS2.
DS9 Manage the configuration	Most aspects of configuration management are outsourced to the CSP. The risk exists that the CSP's controls will not be adequate (1).	Refer to DS2.
DS10 Manage problems	Most aspects of problem management are outsourced to the CSP. The risk exists that the CSP's controls will not be adequate (5) (7).	Refer to DS2.
DS11 Manage data	1. Refer to DS5 and PO2. 2. The dynamic nature of cloud computing services (for example, a CSP may use multiple locations and devices for storage) can cause uncertainty relating to where the data of the CSC 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 (7) (10) (15). 3. Upon termination of a contract with a CSP, the data of the CSC enterprise which is left on the CSP's infrastructure, may not be properly deleted or may even be maliciously disclosed by the CSP. The data may possibly also be withheld by the CSP until full payment for services is received (or even for other reasons) (1) (3).	1. Refer to DS5 and PO2. 2. Refer to DS2.
DS12 Manage the physical environment	Most aspects of managing the physical environment are outsourced to the CSP. The risk exists that the CSP's controls will not be adequate (1) (7).	Refer to DS2.
DS13 Manage operations	1. Most aspects of operations management are outsourced to the CSP. The risk exists that the CSP's controls will not be adequate (1) (7). 2. Refer to DS5.	1. Refer to DS2. 2. Refer to DS5.
ME2 Monitor and evaluate internal control	1. 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 CSP storing data of various smaller and larger CSC 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 (15). The risk of a smaller CSC enterprises therefore increases (from being unappealing for attack, to being appealing due to the amalgamation with other enterprises' data at the CSP). 2. There is a risk of non-compliance of the CSC enterprise and/or its data with the laws and regulations governing the CSP (if they are under different jurisdiction) and *vice versa*, causing liability (7). 3. There is a risk of insufficient internal controls at the CSP (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 CSC enterprise) (1) (4) (7) (10) (15).	1. Refer to DS2 and AI5. 2. Clear policies must be developed, communicated and enforced by the CSC enterprise regarding sensitive data which should possibly not be allowed to be processed/stored using cloud services, and other less sensitive data.

Table 1. Contd.

	4. There could be non-adherence by users inside the CSC 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 (5).	
ME3 Ensure compliance with external requirements	Refer to ME2.	Refer to ME2.

Numbered list of references: (1) Cloud security alliance (2009); (2) Feiman (2010); (3) Hayes (2008); (4) Heiser (2009); (5) Heiser (2010); (6) Hill and Humphrey (2010); (7) ISACA (2009); (8) Jensen et al. (2009); (9) Knipp (2011); (10) Marston et al. (2011); (11) Mingay and Govekar (2010); (12) Pescatore (2010); (13) Pring (2010); (14) Sanders (2010); (15) Subashini and Kavitha (2011); (16) Winkler (2011a); (17) Winkler (2011b).

All 34 processes were considered for this study to ensure completeness, but only the processes which could be linked to significant incremental risk are presented in the research table.

Most of the significant risks and controls 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 in Table 1. References were only indicated where publications and research dealt with the risk or control in relative detail.

DISCUSSION

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 (CSC), 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 (or parties) 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 CSC 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 along the Internet or other wide 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 CSC enterprise and the CSP reside in different jurisdictions, as well as the risk of not being able to switch from one CSP to another (non-portability issues).

Summary of main controls for consumer enterprise

The best control that a prospective CSC enterprise can implement is to mitigate risks, relate to the selection of an appropriate CSP(s). The appropriate and most reliable CSP that fits the specific CSC enterprise's need and risk profile should be selected, mainly by applying the approach summarised, in the rest of this subarea.

One of the main sources of risk in the cloud computing environment, as discussed in the previous area, is that of the outsourcing of the provision of IT capabilities. In this case, the importance of the service level agreement (SLA) with the CSP becomes critical. This can be deduced from Table 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 CSP'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 CSP as if it were the CSC enterprise's own controls. This entails that the CSP would have to allow the CSC 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 CSC enterprise could have gained by placing reliance on a CSP's controls. In fact, the auditing of these controls may be very expensive for the CSC enterprise due to the different locations of the CSP's operations and the need to cooperate with the CSP in terms of access provision for the performance of these audits.

The second approach is the certification of CSPs by third party certification bodies or enterprises that assess and rate the CSPs' risk mitigating controls on behalf of all CSC enterprises (Heiser, 2009; Winkler, 2011a). This certification and rating should be used by prospective CSCs to select a CSP with the appropriate certified rating for the level of controls and security required by the relevant prospective CSC enterprise. It logically follows that the cost of cloud services provided by higher rated CSPs 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 CSC enterprise should inspect certification reports to ensure that, at the very least all issues referred to at DS2 in Table 1 are indeed dealt with in the certification report.

To mitigate the risks relating to the use of Internet technologies and network access, the CSC enterprise should update its SLAs with the provider of these technologies (ISP). 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. Examples include, changing from a VPN option that is located on the internet (World Wide Web) to a VPN located on a private network. Although these would probably be more expensive options, the increased cost will be negated by the savings achieved by utilising cloud services.

Controls suggested to mitigate some of the secondary risks mentioned, include firstly consultation with legal professionals on cross jurisdiction and intangible asset issues, before concluding agreements with CSPs. To secondly address the risk arising from non-portability, the careful selection of a CSP, as outlined in the paragraphs earlier mentioned, reduces the risk of wanting to switch from one CSP to another. Additionally, Cisco is working on creating standards for cloud computing services which would ensure that CSPs that apply these standards afford their CSCs the ability to switch to other CSPs that also apply these standards (Marston et al., 2011). Thus, selecting a CSP that applies these standards would be a strong control, once these standards are finalised.

Conclusion

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

A prospective CSC enterprise may gain a competitive advantage from the adoption of cloud computing, but should pay due attention to the issues raised in this study. These issues include the outsourcing of the provision of IT capabilities which results in extreme reliance being placed on a third party, namely the CSP, to implement proper controls to satisfy the CSC 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.

At this early stage in the evolution of cloud computing it will be wise to select a CSP that has a reputation of being one of the world leaders in the provision of IT related products and services, as they are likely to apply the best controls in order to protect their reputation.

The business imperatives of each prospective CSC 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 (except possibly a private cloud) 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).

Abbreviations: **COBIT,** Control objectives for information and related technology; **CSC,** cloud service consumer; **CSP,** cloud service provider, **IaaS,** infrastructure as a service; **ISP,** internet service provider; **SaaS,** software as a service; **SLA,** service level agreement(s); **VPN,** virtual private network **PaaS**, Platform as a Service.

REFERENCES

Amazon Web Services (2011). Summary of the Amazon EC2 and Amazon RDS service disruption in the US East Region. Media release. [Online]. http://aws.amazon.com/message/65648/ (Accessed 25 May 2011).

Blandford R (2011). Information security in the cloud. Netw. Secur. 2011(4):15-17.

Cloud Security Alliance (2009). Security guidance for critical areas of focus in cloud computing V2.1. Cloud security alliance. [Online]. 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. [Online]. 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. [Online]. http://my.gartner.com/resources/206000/206018/how_to_keep_your_job_from_di_206018.pdf (Accessed 12 July 2011).

Hayes B (2008). Cloud computing. Comm. ACM, 51(7):9-11.

Heiser J (2009). What you need to know about cloud computing security compliance. Gartner. Research report, 13 July 2009. [Online]. 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. [Online]. 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.

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

Jensen M, Schwenk J, Gruschka N, Iacono LL (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. [Online]. http://my.gartner.com/resources/209300/209391/cloud_computing_and_emerging_209391.pdf (Accessed 11 July 2011).

Marston S, Li Z, Bandyopadhyay S, Ghalsasi A (2011). Cloud computing – the business perspective. Decis. Support Syst. 51:176-189.

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. [Online]. 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. [Online]. http://my.gartner.com/resources/206000/206019/securing_and_managing_privat_206019.pdf (Accessed 11 July 2011).

Plummer DC, Smith DM, Bittman TJ, Cearley DW, Cappuccio DJ, Scott D, Kumar R, Robertson B (2009). Five refining attributes of public and private cloud computing. Gartner. Research report, 5 May 2009. [Online]. http://my.gartner.com/resources/167100/167182/five_refining_attributes_of__167182.pdf (Accessed 25 May 2011).

Plummer D, Prentice S, Da Rold C, Feiman J, Pescatore J, Clark W, Cain MW, Prentice B, Notardonato S, Dominy M, Tay G (2011). Gartner's top predictions for IT organizations and users, 2012 and beyond: Control slips away. Gartner. Research report, 23 November 2011. [Online]. http://my.gartner.com/resources/226700/226767/gartners_top_predictions_for_226767.pdf (Accessed 9 February 2012).

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

Sanders A (2010). A Phased Approach to Reviewing Cloud Computing Risks. ISSA J., October 2010; pp. 24-27.

Smith DM (2010). Hype cycle for cloud computing, 2010. Gartner. Research report, 27 July 2010. [Online]. http://my.gartner.com/resources/201500/201557/hype_cycle_for_cloud_computi_201557.pdf (Accessed 14 July 2011).

Smith DM (2011). Hype cycle for cloud computing, 2011. Gartner. Research report, 27 July 2011. [Online]. 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.[Online]. 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. J. Netw. Comput. Appl. 34(1):1-11.

Tuttle B, Vandervelde SD (2007). An empirical examination of COBIT as an internal control framework for information technology. Int. J. Account. Inform. Syst. 8(2007):240-263.

Winkler JR (2011a). Chapter 1 - Introduction to Cloud Computing and Security. Securing the Cloud. Syngress, Boston, pp. 1-27.

Winkler JR (2011b). Chapter 6 - Key Strategies and Best Practices. Securing the Cloud. Syngress, Boston, pp. 153-185.