2011

Cloud Nine? An Integrative Risk Management Framework for Cloud Computing

Indrit Troshani
University of Adelaide, Australia, indrit.troshani@adelaide.edu.au

Giselle Rampersad
Flinders University, Australia, giselle.rampersad@flinders.edu.au

Nilmini Wickramasinghe
RMIT University, Australia, nilmini.wickramasinghe@rmit.edu.au

24th Bled eConference
eFuture:
Creating Solutions for the Individual, Organisations and Society
June 12 - 15, 2011; Bled, Slovenia

On Cloud Nine?
An Integrative Risk Management Framework for Cloud Computing

Indrit Troshani
University of Adelaide, Australia
indrit.troshani@adelaide.edu.au

Giselle Rampersad
Flinders University, Australia
giselle.rampersad@flinders.edu.au

Nilmini Wickramasinghe
RMIT University, Australia
nilmini.wickramasinghe@rmit.edu.au

Abstract
Cloud computing is heralded to be one of the most significant information technology developments in recent years. There is widespread agreement that the adoption of cloud resources and capabilities is poised for strong growth into the future. Nevertheless, there is paucity of research concerning the perceived risks that affect the adoption intentions of prospective organisational adopters. In attempts to contribute to the existing body of knowledge, this study draws on qualitative evidence to explore perceived cloud computing risks. It culminates with an integrative risk management framework for the adoption of cloud computing.

Keywords*:* cloud computing, innovation adoption, risk, risk management.

1 Introduction

Cloud computing is a new information technology (IT) delivery paradigm that is increasingly recognised as one of the most significant developments in recent years (Gilbert, 2010; Julisch & Hall, 2010). Many firms are seeking to get 'on cloud nine' in attempts to take advantage of the value propositions of cloud computing including low cost, increased flexibility, and shorter time-to-market. Cloud computing has the potential to transform the IT industry in many ways including changing the ways in which IT software and hardware are designed and used in modern businesses (Armbrust et al., 2010; Julisch & Hall, 2010).

There is widespread agreement in both academia and industry that cloud services are poised for strong growth into the future. For example, a recent IDC survey finds that 12

percent of the worldwide software market is expected to move to the cloud by 2013 (Clavister, 2009; Gens, Mahowald, & Villars, 2009; IDC, 2008; Subashini & Kavitha, 2011), whereas Gartner predicts that cloud services revenue is expected to reach US$148.8 billion through 2014 with financial and manufacturing industries being the largest early adopters (DeFelice, 2010). Also, according to Gartner, by 2012 at least a third of business application software spending will be on cloud applications (Plummer et al., 2008).

Given these trends, there are calls in the literature for further research concerning cloud computing. However, while existing analyses on cloud computing have been undertaken from the service-providers' perspective, there is need for further research that focuses on the organisational users' perspective (Clarke, 2010; Svantesson & Clarke, 2010). While cloud computing is an emerging phenomenon, there is paucity of research concerning the perceived risks that affect the adoption intentions of prospective organisational adopters. In attempts to address these shortcomings and to add to the existing cloud computing literature, with this paper we aim to address the research question, 'what are the perceived cloud computing risks in organisational adopters'? The study culminates with an integrative risk management framework concerning the adoption of cloud computing. This framework contributes to the exiting body of knowledge by informing prospective organisational cloud adopters for technological, organisational, and environmental risks which need to be both managed and mitigated before the adoption of cloud computing can succeed (Farrell, 2010).

To address our aim, first we provide an overview of cloud computing before discussing the notions of risk, risk management, and the organising framework. The manner in which data was collected is explained before the framework is elaborated. The paper is concluded with a discussion and managerial relevance.

2 Background

2.1 An Overview of Cloud Computing

Although the definition of cloud computing is still expected to evolve overtime, it is generally widely accepted that cloud computing is an arrangement that enables the convenient provisioning of configurable software capabilities and underlying hardware resources across numerous host computers that are connected via a network (Mell & Grance, 2010; Svantesson & Clarke, 2010). There are five essential characteristics that characterise cloud computing (Mell & Grance, 2010):

- On-demand self-service whereby consumers can obtain computing capabilities or resources (e.g. network storage or server time) without necessarily requiring service provider interaction;
- Broad network access whereby computing capabilities or resources can be accessed ubiquitously using any device (e.g. mobile phones, laptops);
- Resource pooling whereby location-independent computing resources and capabilities are assigned dynamically to consumers according to demand;
- Rapid elasticity whereby computing capabilities and resources are rapidly scalable and can be purchased by consumers at any time in any quantity; and,

- Measured service whereby resource usage can be metered providing transparency to both service providers and consumers.

Cloud computing capabilities and resources include various applications and services, storage, processing power, memory, network bandwidth, virtual machines which are classified into three broad categories (Julisch & Hall, 2010; Mell & Grance, 2010):

- Software as a Service (SaaS) which includes software applications controlled by providers that consumers can access and run through thin client interfaces (e.g. web-browsers). Examples include web-based mail services such as gmail.
- Platform as a Service (PaaS) which includes provider-controlled platforms comprising development tools and run time environments which cloud consumers can use to develop their own software applications. Examples of PaaS include Google Apps, Microsoft Azure.
- Infrastructure as a Service (IaaS) which includes provider-controlled fundamental computing resources such as virtual machines, storage, networks where consumers can run arbitrary applications including operating systems. Examples include Amazon's Elastic Compute Cloud (Amazon EC2).

Cloud computing is a type of traditional IT outsourcing (Cullen & Willcocks, 2003). However, unlike traditional IT outsourcing whereby providers offer unique and customised services according to the client's exact terms and specification, cloud computing services offered are highly standardised which providers can offer inexpensively in a commoditized "one-size-fits-all" fashion by spreading costs across large consumer bases (Brunette & Mogull, 2009; Datamonitor, 2009; Julisch & Hall, 2010). Thus, while cloud computing providers can offer low-cost, short time-to-market, on-demand services, the shared underlying cloud computing infrastructure across numerous clients "destroys any client's ability to afford the same level of control known from classic IT outsourcing." (Julisch and Hall, 2010, p. 300). Nevertheless, like classic outsourcing, with cloud computing, the contractual terms detailing the cooperation agreement between service cloud providers and consumers are specified in Service Level Agreements (SLAs) which can provide clients with some control concerning the extent to which cloud computing capabilities and resources can be customised to their needs (Cullen & Willcocks, 2003; Julisch & Hall, 2010). The extent to which control is maintained on the cloud by clients or ceded to cloud providers can create uncertainty or risk for clients concerning the various ways in which their core competencies or supporting functions are perceived to be affected in cloud environments.

2.2 Risk and Risk Management

Risk is defined as the possible impact of an event on an organisation's assets and the corresponding expected and unexpected consequences that occur as a result (Levin & Schneider, 1997; Stoneburner, Goguen, & Feringa, 2002). In measurable terms, risk is a statistical measure that encapsulates the consequence of a loss by the chance of its occurrence (Crouhy, Galai, & Mark, 2006). Various disciplines define risk in different ways. For example, medical science adopts the perspective of risk as a probability function (Kobs, 1998). In finance, risk represents the variance of distribution of outcomes (Levine, 2000; Schirripa & Tecotzky, 2000), whereas casualty insurance views risk as expected loss (Bowers, Gerber, Hickman, Jones, & Nesbit, 1986). A

managerial perspective of risk in IT outsourcing associates risks with "danger or hazard" perceptions that can result in negative outcomes (March & Shapira, 1987). In this study we adopt the managerial perspective of risk. This choice is a useful proposition, particularly given the emerging nature of cloud computing and its pertinence to managers.

There is widespread agreement in the literature that even in established relationships between organisations, risks might exists on whether partners have the intention or will to, in fact, act appropriately as specified in IT outsourcing SLAs (Cullen & Willcocks, 2003; Liang, et al., 2005). These risks can erode relationships and potentially increase costs for both providers and their clients (Rousseau, et al., 1998) and may operate in cloud computing contexts as well (Paquette, Jaeger, & Wilson, 2010). In an emerging area such as cloud computing, prospective adopting organisations may find it challenging to easily and clearly associate risk with well-understood or widely-accepted cost structures (Paquette et al., 2010).

Closely related to risk is the notion of risk management. In cloud settings, risk management is the process of developing risk-adjusted strategies that attempt to balance opportunities that cloud computing offers with likely positive and negative consequences of taking advantage of them (Crouhy et al., 2006; Straub & Welke, 1998). That is, risk management can help deal with the consequences of "modification, destruction, theft, or lack of availability of computer assets such as hardware, software data and services" (Straub and Welke, 1998, p. 442) that are likely to occur in cloud settings.

In cloud computing contexts where sensitive data is held and operations are carried out outside organisational boundaries, risk can increase substantially as client organisations can expose themselves to failure risk or opportunism from their cloud providers (McCutcheon & Stuart, 2000). Examples include computer misuse, disaster, violation of access privileges and restrictions, intellectual property theft, data loss or damage (Paquette et al., 2010). Consequently, clients may want strong guarantees that cloud providers will not opportunistically share their data with others or that the computing resources that the providers offer will be reliable and impenetrable to illicit hacking activities from both outsiders or even cloud co-tenants.

As cloud computing is a type of outsourcing, if one is to understand risks associated with it "it is essential to identify the array of potential undesirable outcomes that could occur with respect to the outsourcing [or cloud] arrangement" (Aubert, Patry, and Rivard, 2005, p. 12). Therefore, understanding and undertaking risk management relevant to cloud computing settings is of paramount importance for organisations that intend to take advantage of cloud computing resources and capabilities. While risk management can be complex and ensuing outcomes or consequences not necessarily precise, identifying cloud computing risks is the first step that can allow these risks to be managed and mitigated (Paquette et al., 2010).

2.3 Organising Framework

In this paper we consider cloud computing as an innovation which various organisations are considering to adopt. One of the most established approaches in studying the adoption of innovations entails identifying contingency factors that can affect adoption decisions in organisations (Fichman, 2004). Also known as "innovation configuration"

(Fichman, 2004, p. 320) these factors can jointly explain adoption outcomes in organisations, and are commonly classified into three broad contextual categories, namely, technology, organisation, and environment (TOE) (DePietro, Wiarda, & Fleischer, 1990; Tornatzky & Klein, 1982). The TOE models can be useful for the systematic and structured analysis of innovation adoption in organisations, in that, it helps distinguish between the intrinsic characteristics of innovations, organisational capabilities and motivations, and broader environmental dimensions that impact on adopters (Dedrick & West, 2004).

First, the technology context focuses on the manner in which technology characteristics or associated risks can influence adoption (DePietro et al., 1990; Yang, Lee, & Lee, 2007). The context emphasis relates to the operationalisation and potential realisation of benefits or risks and the existing organisational adoption capability (Chong & Ooi, 2008; Pedroso, Zwicker, & de Souza, 2009; Tan, Chong, Lin, & Eze, 2009). Second, the organisational context describes the nature of the characteristics of the organisations that may facilitate or inhibit adoption. Third, the environmental context represents the arena where adopting organisations conduct their business, and includes industry characteristics, government regulation, and supporting infrastructure (Chong & Ooi, 2008; DePietro et al., 1990; Oliveira & Martins, 2010). These factors can both present opportunities to encourage organisations to, or inhibit them from adopting innovations including cloud computing.

Because risks are factors that can impact on an organisation's assets when their corresponding expected and unexpected consequences eventuate (Levin & Schneider, 1997; Stoneburner et al., 2002), we argue that risks can affect the adoption of innovations, in general, and cloud computing, in particular. Therefore, using the TOE framework as a starting point for identifying cloud computing risks, and subsequently developing a risk management framework is not unreasonable.

3 Data Collection

The research reported in this paper is exploratory and employs qualitative evidence. Given that the adoption of cloud computing is still at an emerging stage, a better understanding of the potential risks that are associated with it can be obtained by examining qualitative interpretations of the relevant stakeholders as they are affected by the potential adoption of cloud computing (Van de Ven & Rogers, 1988; Wolfe, 1994). We used focus groups to collect qualitative data (Krueger & Casey, 2000; Malhotra, Hall, Shaw, & Crisp, 1996). The aim of focus groups is to elicit participants' attitudes, perceptions and feelings about new topics. This was consistent with our aim of eliciting risks in cloud computing settings. Focus groups are suitable for exploratory research where the field of study is relatively new.

The focus group technique was used to provide a quick and cost-effective way for collecting rich data in relatively new domains such as cloud computing. It enables focus group participants to openly express their views while interacting with others in the group. It also provides opportunities for clarification and expansion on arguments to be made. Consequently, we found the focus group technique to be an invaluable tool not only for investigating the participants' thoughts but also for understanding how expressed views evolve as participants justify them to others in the group. Additionally, we found that new ideas were being generated as participants could build on arguments

based on each others' responses. This enabled the generation of insights that might have not otherwise been identified using alternative techniques such as in-depth interviews and surveys.

The aim of the focus group was to explore the perceived risks concerning the adoption of cloud-computing SaaS capabilities at an Australian educational organisation. The focus group was comprised of representatives of various functional areas of the organisation in question. The representatives were individuals who were considered knowledgeable on the relevant topics in their respective areas. The focus group met in four separate sessions which were organised by the same moderator. Each session lasted approximately 90 minutes. In the first session, the moderator prompted participants with some general topics and issues recognised as relevant in extant literature. The objective of each session was to refine and elaborate the topics and issues identified in previous sessions and even identify new ones as applied to the various functional areas at the organisation in question. This stepwise refinement was repeated until all issues were exhausted and agreement concerning respective clarifications were reached or until disagreements were explained and resolved. The contents of the collected data were analysed thematically. Codes were developed which provided the basis for analysis and helped identify and analyse emerging patterns of themes (Carson, et al., 2001).

4 Technology, Organisation, and Environment Risks

In this section we classify the identified risks into three broad categories, namely, technology, organisation, and environment as guided by the organising framework discussed in section two. The specific risks that have been identified in relation to cloud computing have been summarised in Figure 1. These risks have been discussed in further detail in the sections that follow.

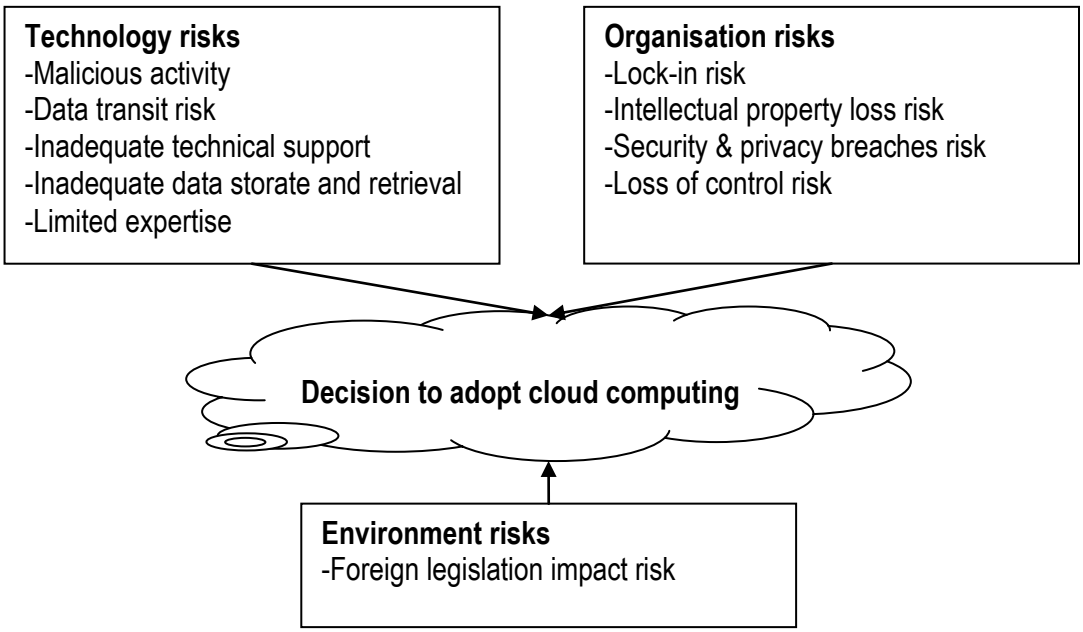

Figure 1: Cloud computing risk management framework

4.1 Technology Risks

Malicious activity Cloud resources can be susceptible to malicious activity by i) cloud provider insiders, and ii) outsiders or hackers. The first type of malicious activity concerns situations whereby individuals can abuse their high privilege roles in their capacity as cloud provider employees. For example, roles such as system administrators, security providers that analyse intrusion detection, auditors, etc. constitute high privilege roles within cloud providers. The second type of malicious activity concerns hacking by outsiders on cloud resources that attempt threats, such as, malicious probes, scans, and network mapping. Malicious activities can potentially lead to loss of data integrity, confidentiality, and availability, potentially leading to economic loss, diminished customer trust, and damaged organisational reputation.

Data transit risk Due to their distributed nature, at any given time in cloud computing architectures larger amounts of data are likely to be in transit than in traditional architectures. Data transfers will occur between the cloud provider infrastructure and remote web clients for synchronisation, storage or processing purposes. This, however, may increase exposure to eavesdropping threats including sniffing, email wiretaps, and spoofing. While data transit risk can have serious consequences for cloud computing clients it can be mitigated using available encryption technologies.

Inadequate technical support Evidence suggests that current cloud providers operate self-service type support and provide administrative functions enabling cloud clients to apply self-fixes. However, this level of support may be perceived to be inadequate, particularly because traditional infrastructures operate helpdesk type support which is generally perceived to be efficient and effective. Inadequate helpdesk support is perceived to adversely impact the productivity of cloud users. This risk could be mitigated by either providing helpdesk type support that is effective, efficient and that operates in the client's time zone.

Inadequate data storage and retrieval In order to ensure that business continuity is at least maintained (if not improved), cloud clients need to be able to store and retrieve their data both in a timely and cost-effective manner and in accordance with their business requirements. Consequently, cloud providers need to ensure that their underlying infrastructure offers adequate bandwidth and capacity to meet existing business needs of their clients with flexibility as businesses grow in response to changing environments and business requirements. Cloud clients can mitigate risks of this nature by including relevant clauses in SLAs with cloud providers concerning both critical levels of functional specifications and reasonable fees that may be charged by providers.

Limited expertise While cloud providers can offer various computing capabilities and resources, clients also require adequately skilled human resources that can manage the interface between themselves and their cloud providers. There was agreement in the focus group that there is currently limited expertise available including knowledge, experience, and skills, in managing cloud provider relationships. While this risk can adversely affect the experience of cloud users, it can be mitigated by way of training and recruitment.

4.2 Organisation Risks

Lock-in risk. This risk may emerge to become a serious threat on client operations if or when service or delivery performance in the cloud deteriorates overtime. Additionally, potentially disastrous business failure can result in situations when cloud providers face bankruptcy, terminate their services, or are acquired by other cloud providers. In these scenarios clients may have to migrate from one cloud provider to another which may result in disruption of core business functions. This risk may be mitigated by ensuring that optimal performance indicators are prescribed in SLAs and that cloud providers offer adequate tools, procedures, and standards that can guarantee seamless data and capability portability.

Intellectual property (IP) loss risk. This risk concerns perceptions that IP may be lost as commercial and confidential type of information concerning research and development is transferred to and stored in cloud environments. Exposure of such information may increase legal liability of clients. Focus group informants were consistent in pointing out that IP loss risk can be mitigated in various ways. For example, clients can specify clauses in contractual agreements that using cloud capabilities and resources does not cede IP rights to cloud providers. Additionally, clients can select cloud providers that operate in national jurisdictions which protect IP in ways that are similar to what is afforded by Australian legislation.

Security & privacy breaches risk. This risk is related to perceptions amongst client users that security with existing in-house traditional architectures is higher than in cloud architectures. However, there was agreement amongst informants that these perceptions are incorrect and not justified, and that security in cloud architectures can, in fact, be higher than in traditional in-house IT environments. Additionally, privacy breach risk is considered to be important particularly in cases where confidentiality breaches are not reported to clients by their cloud providers. Both security and privacy breaches can result in serious economic loss due to potential disruptions of core operations, litigation due to loss of commercially-sensitive or personal data. This risk can be mitigated by providing awareness sessions to reassure users concerning security levels that cloud environments can offer.

Loss of control risk. Migration to cloud environments entails ceding control of computing capabilities and resources to cloud providers. There are negative perceptions associated with this amongst client users as loss of control is seen as dependency on cloud providers which can adversely affect clients' ability to control service delivery and quality including contingency procedures, such as, disaster recovery, backup and restore functions. For example, cloud providers may outsource specialised functions which can extend client dependency to third parties thereby potentially complicating both coordination chains and recourse to remedies in cases of non-compliance with SLA specifications. Additionally, clients may have less bargaining power with larger and reputable cloud providers while contract enforcement can be costly and difficult particularly if cloud providers are outside Australia which is quite likely. This was unanimously considered to be a high risk, but which could be mitigated by way of contract negotiation and specification of legally binding terms and conditions in SLAs.

4.3 Environment Risks

Foreign legislation impact risk. It is expected that cloud providers operate their capability and resource offerings outside Australia. Cloud services used by clients will, as a consequence, be subject to the host countries' legislation. This was considered to be highly risky, particularly when host countries' legislation changes frequently, is unpredictable, is not enforced consistently, is inconsistent with or does not adhere by international agreements. Corollary issues include scenarios whereby cloud providers are subpoenaed by law enforcement organisations where hardware can be confiscated for e-discovery purposes. These situations can potentially result in confidentiality breaches, data leakage, and economic losses for cloud clients. Although this was considered to be a high risk with potentially serious consequences, it can be mitigated by way of contract negotiation. That is, including clauses requiring full disclosure and negotiation concerning data storage locations.

5 Discussion and Conclusion

We have identified three different risk management perspectives and integrated them into a single framework which can improve current understanding of emerging and complex phenomena concerning the adoption of cloud computing while also adding to existing embryonic cloud computing literature. We have discussed some of the possible impacts of these risks and possible ways in which they can be mitigated. While our analysis of cloud computing risks is not meant to be exhaustive, rather a starting point for further investigations, it is consistent with and responds to calls in extant research for considering cloud computing risks from the user's perspective. We have adopted an integrative view of these risks by adapting the well-known TOE framework in cloud computing settings. Adopting an integrative view can provide practitioners with a holistic and unified tool for explaining the complex phenomenon of cloud computing risk management.

While using a focus group to isolate potential risks associated with cloud computing, we appreciate that a limitation is that the risks examined are based on only one focus group the members of which are part of the same organisation, thereby providing potentially limited insights for generalising to the wider population of prospective cloud computing adopters across Australia and more broadly worldwide. However, given the exploratory nature of this study, generalisation was not an objective. We accept that the extent to which our findings are useful in practice can be deemed to be tentative without further research investigating cloud computing adoption risks from other perspectives in both Australian and non-Australian organisations.

Nevertheless, given the rich nature of collected data, managerial implications can be derived which can provide insights concerning managerial implications in relation to cloud computing adoption risks. First, it can offer managers in organisations that are seeking to get 'on cloud nine' by contemplating to adopt cloud computing resources or capabilities, improved insights in balancing specific decisions concerning potential risks. Second, given its integrative approach the proposed framework may be better positioned to help organisations with cloud computing adoption ambitions carry out in-depth analyses of the cloud computing resources and capabilities that they might be considering to adopt. In doing so, organisations can analyse their strengths or

weaknesses and the manner in which the adopted capabilities can help enhance or minimise them in strengthening their competitive positions. Third, managers need to become cognisant of the relevant legislation in their host country where cloud computing operations will be based which may be different to the rules under which they may used to operate. A deep understanding of host countries' institutional contexts may be critical for risk minimisation.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010). A vew of cloud computing. Communications of the ACM, *53*(4), 50-58.

Bowers, L. N., Gerber, U. H., Hickman, C. J., Jones, A. D., & Nesbit, J. C. (1986). Actuarial Mathematics. Itasca: The Society of Actuaries.

Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2.1. Available: http://www.cloudsecurityalliance.org/csaguide.pdf. Accessed on 8 January 2010: Cloud Security Alliance.

Carson, D., Gilmore, A., Gronhaug, K., & Perry, C. (2001). Qualitative Research in Marketing. London: Sage.

Chong, A. Y.-L., & Ooi, K.-B. (2008). Adoption of interorganizational system standards in supply chains: an empirical analysis of RosettaNet standards. Industrial Management & Data Systems, *108*(4), 529-547.

Clarke, R. (2010). Computing clouds on the horizon? Benefits and risks from the user's perspective. Paper presented at the 23rd Bled eConference, Bled, Slovenia, June 20-23.

Clavister. (2009). Security in the Cloud. Clavister White Paper. Available: http://www.it-wire.nu/members/cla69/attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdf. Accessed on 7 January 2011.: Clavister.

Crouhy, M., Galai, D., & Mark, R. (2006). The Essentials of Risk Management. Toronto, Ontario: McGraw-Hill.

Cullen, S., & Willcocks, L. P. (2003). Intelligent IT outsourcing: Eight Building Blocks to Success. London: Butterworth-Heinemann.

Datamonitor. (2009). Can Cloud Computing Help Enterprises Weather the Economic Storm? Gauging the disruptive potential of a new model of IT consumption. Report DMTC2267: Datamonitor.

Dedrick, J., & West, J. (2004). An exploratory study into open source platform adoption. Paper presented at the 37th Hawaii International Conference on System Sciences, Hawaii.

DeFelice, A. (2010). Cloud computing: What accountants need to know. Also available at: http://www.journalofaccountancy.com/Issues/2010/Oct/20102519.htm. Journal of Accountancy, *October*, 50-55.

DePietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: organization, technology, environment. In L. G. Tornatzky & M. Fleischer (Eds.), The Process of Technological Innovation (pp. 151-175). Lexington, MA: Lexington Books.

Farrell, R. (2010). Securing the cloud-governance, risk, and compliance issues reign supreme. Information Security Journal: A Global Perspective, *19*(6), 310-319.

Fichman, R. G. (2004). Going beyond the dominant paradigm for information technology innovation research. Journal of the Association for Information Systems, *5*(8), 314-355.

Gens, F., Mahowald, R. P., & Villars, R. L. (2009). Cloud Computing 2010 - An IDC Update. Sep 29, 2009 - Doc # IDC_P20476. Framingham, MA United States IDC.

Gilbert, F. (2010). Cloud service contracts may be fluffy: selected legal issues to consider before taking off. journal of Internet Law, *14*(6), 17-30.

IDC. (2008). IT Cloud Services User Survey, pt.2: Top Benefits & Challenges. Framingham, MA: International Data Corporation (IDC).

Julisch, K., & Hall, M. (2010). Security and control in the cloud. Information Security Journal: A Global Perspective, *19*(6), 299-309.

Kobs, A. (1998). Sentinel events - A moment in time, a lifetime to forget. Nursing Management, *29*(2), 10-13.

Krueger, R. A., & Casey, M. A. (2000). Focus Groups: A Practical Guide for Applied Research. Thousand Oaks, California: Sage.

Levin, M., & Schneider, M. (1997). Making the disctinction: risk management, risk exposure. Risk Management, *44*(8), 36-42.

Levine, E. (2000). Defining risks. CA Magazine, *133*(3), 45-46.

Liang, H., Xue, Y., Laosethakul, K., & Lloyd, S. J. (2005). Information systems and healthcare-I: trust, uncertainty, and online prescription filling. Communications of the Association for Information Systems, *15*, 41-60.

Malhotra, N. K., Hall, J., Shaw, M., & Crisp, M. (1996). Marketing Research: An Applied Orientation. Sydney: Prentice-Hall.

March, J., & Shapira, Z. (1987). Managerial perspectives on risk and risk-taking. Management Science, *33*(11), 1404-1418.

McCutcheon, D., & Stuart, F. I. (2000). Issues in choice of supplier alliance partners. Journal of Operations Management, *18*(3), 279-302.

Mell, P., & Grance, T. (2010). The NIST definition of cloud computing. Communications of the ACM, *53*(6), 50.

Oliveira, T., & Martins, M. F. (2010). Understanding e-business adoption across industries in European countries. Industrial Management & Data Systems, *110*(9).

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly, *27*(3), 245-253.

Pedroso, M. C., Zwicker, R., & de Souza, C. A. (2009). RFID adoption: framework and survey in large Brazilian companies. Industrial Management & Data Systems, *109*(7), 877-897.

Plummer, D. C., Smulders, C., Fiering, L., Natis, Y. V., Mingay, S., Driver, M., et al. (2008). Gartner's Top Predictions for IT Organizations and Users, 2008 and Beyond: Going Green and Self-Healing. Available: http://www.gartner.com/DisplayDocument?id=578409. Stamford, CT: Gartner.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: a cross discipline view of trust. Academy of Management Review, *23*(3), 393-404.

Schirripa, F., & Tecotzky, N. (2000). An optimal frontier. The Journal of Protfolio Management, *26*(4), 29-40.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology. Available: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf, Accessed on 8 January 2011. Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST).

Straub, D., & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly, *22*(4), 441-469.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, *14*(1), 1-11.

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, *26*(4), 391-397.

Tan, K. S., Chong, S. C., Lin, B., & Eze, U. C. (2009). Internet-based ICT adoption: evidence from Malaysian SMEs. Industrial Management & Data Systems, *109*(2), 224-244.

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption implementation: a meta-analysis of findings. IEEE Transactions on Engineering Management, *EM-29*(1), 28-45.

Van de Ven, A. H., & Rogers, E. M. (1988). Innovation and organisations: critical perspectives. Communication Research, *15*, 632-651.

Wolfe, R. A. (1994). Organisational innovation: review, critique and suggested research directions. Journal of Management Studies, *31*(3), 405-431.

Yang, K. H., Lee, S. M., & Lee, S.-G. (2007). Adoption of information and communication technology: impact of technology types, organizational resources and management style. Industrial Management & Data Systems, *107*(9), 1257-1275.