UNIVERSITY OF OREGON

APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary
Studies Program:
Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners

CAPSTONE REPORT

Thomas J. Betcher
Sr. Disaster Recovery Coordinator

University of Oregon
Applied Information
Management
Program

February 2010

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

____

Dr. Linda F. Ettinger
Academic Director, AIM Program

Running Head: CLOUD COMPUTING RISKS

Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners

Thomas J. Betcher

Abstract

Although the benefits of cloud computing are well known, safety concerns have received less attention (Rash, 2009). This review of selected literature, published between 2007 and 2009, identifies key IT-related cloud computing risks that should be considered by security practitioners. Three types of cloud computing risks are examined: policy and organizational, technical, and legal. Risk mitigation strategies are also explored, and include audit controls, policies and procedures, service level agreements, and other forms of governance.

Table of Contents

List of Figures

Introduction

Problem Area/Significance

Cloud computing is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2009, p. 1). Applications of cloud computing broadly span three areas known as 'cloud service delivery models': (a) Infrastructure as a Service (IaaS), (b) Platform as a Service (PaaS), and (c) Software as a Service (SaaS) (Cloud Security Alliance, 2009, p. 6).

As suggested by Levitt (2009), cloud computing frees organizations from the need to buy and maintain their own hardware and software infrastructure (p. 17). Erdogmus (2009) reports that there are two key business drivers to consider in relation to cloud computing: (a) economics, and (b) simplification of software delivery (p. 4). Leavitt (2009) suggests that cloud computing offers additional technical benefits including high availability and easy scalability (p. 15), providing faster, more direct access to IT resources (Ryan, 2008, p. 32).

However, while there is much "buzz" on the benefits of cloud computing, fewer questions have been raised with respect to whether cloud computing is safe (Rash, 2009, p. 8). Hayes (2009) raises concerns about privacy, security, and reliability (p. 11). With respect to privacy, there is the possibility that cloud computing may lead to "commingling of information assets with other cloud customers, including competitors" (ISACA, 2009a, p. 7). With respect to security, Viega (2009) foresees that data and code residing in cloud computing environments will become more tempting targets to hackers (p. 108). With respect to reliability, Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, et al. (2009) argue that few non-cloud IT infrastructures are as robust as cloud computing service offerings, but organizations are still concerned about availability in light of recent outages from Amazon and Google (p. 14).

Gatewood (2009) suggests that cloud computing vendors' ideas "may not be fully developed or include records management rules-based control" (p. 33). The Cloud Security Alliance (2009) eschews the notion that cloud computing should be viewed as a black box (p. 5). The Information Systems Audit and Control Association (ISACA) (2009a) recommends that organizations need to conduct business impact analyses and risk assessments as part of a major cloud computing governance initiative (p. 10). As noted by Leavitt (2009), organizations are now evaluating both the risks and rewards of cloud computing (p. 18). The assumption underlying this study is that this is essential, especially in light of the statement by Nelson (2009a) that "it is feasible that within the next 5 years, more than 80% of the world's computing and data storage could occur 'in the Cloud'" (p. 1656). Likewise, International Data Corporation (IDC) (2009a) estimates that worldwide IT cloud services revenue will increase at an annual rate of 26% from $17.4 billion in 2009 to $44.2 billion in 2013.

Purpose

The purpose of this study is to describe and identify key public cloud computing "IT-related risks" (Stoneburner, Hayden, & Feringa, 2004, p. A-2) as reported in selected literature. IT-related risk is defined in this study as "the net mission/business impact considering … the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability" (Stoneburner, et al., 2004, p. A-2). The study is designed as a literature review of relevant research between 2007 and 2009. The study addresses the following research question:

"What are the key IT-related risks that should be considered by security practitioners when evaluating cloud computing service providers?"

Audience

The target audience for the study is primarily security practitioners who evaluate, recommend, and lead the implementation of cloud computing services on behalf of their respective organizations. The Cloud Security Alliance (2009) acknowledges that cloud computing is an "unstoppable force" and that security practitioners need to be proactive in leading its secure adoption (p. 5). Security practitioners face a daunting challenge, as "many of the leading cloud service providers accept no responsibility for the data being stored in their infrastructure" (Cloud Security Alliance, 2009, p. 26). In addition, security practitioners must address the possibility that business users can now bypass IT and engage directly with cloud computing service providers (ISACA, 2009a, p. 8).

Outcome

The intended outcome of this study is an explicated set of cloud computing IT-related risks, along with a review of potential mitigation strategies. The most common and severe IT-related cloud computing risks reported in the selected literature are identified to provide critical areas of focus for security practitioners. IT-related risks are collected and organized into "risk categories," as documented in the Disaster Recovery Journal (Risk categories, n.d.). A pre-selected set of categories is pulled from a glossary developed jointly by the editorial advisory board of the Disaster Recovery Journal and the DRII Certification Commission and includes: reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, outsourcing, people, technology and knowledge (Risk categories, n.d.). Once identified, the IT-related cloud computing risks are classified into three overarching risk categories (policy and organizational, technical, and legal) that serve as a useful reference to security practitioners as they evaluate cloud computing service providers. Each of these risk categories apply to the three cloud service delivery models associated with cloud computing (IaaS, PaaS, and SaaS), although the specific IT-related risks within each of these three delivery models varies.

Delimitations

Time frame. Although its origins go back several years, there has recently been significant interest in cloud computing (Youseff, Butrico, & Da Silva, D., 2008, p. 1). Major cloud computing providers include Amazon AWS and Google Apps, both initiated in 2006, and Salesforce.com, initiated in 1999 (Leavitt, 2009). And although Salesforce.com entered the cloud computing services industry in 1999 (Service Cloud, n.d., p. 2), the term “cloud computing” itself was not widely used in tech circles until early 2007 (Lasica, 2009, p. 5). Sources published prior to 2007 that are related directly to cloud computing are not included in this literature review due to the newness of the subject. The only sources published prior to 2007 are not specific to cloud computing and address the NIST definition for IT-Related risks (Stoneburner, et al., 2004, p. A-2), research methodology (Leedy & Ormond, 2005) and literature reviews (Obenzinger, 2005).

Selection criteria. This study attempts to locate literature meeting criteria that Leedy and Ormond (2005) and Smith, T. (2009) say should be considered when evaluating research by others. This study gives preference to scholarly (or academic or expert) research, as "most academic work will favor scholarly sources over popular ones" (Smith, T., 2009). However, literature is also obtained from reputable trade journals and professional organizations, as there does not appear to be an established number of academic literature reviews of cloud computing. With respect to non-scholarly works using the descriptions delineated by Smith, T. (2009), strong preference is given to articles, written by experts in the field (as opposed to journalists and freelance writers), cited with a bibliography and/or references, and non-commercial in nature. Preference is also generally given to sources that have a clear focus, are organized and easy to follow (Leedy & Ormond, 2005, pp. 9-10), and relevant to public cloud computing IT-related risks.

Audience. This literature review is intended for security practitioners at organizations evaluating or using cloud computing service providers. The audience should be familiar with their respective organizations' IT infrastructures with which cloud computing service providers will integrate or replace on their behalf. This literature review is not intended to benefit audiences unfamiliar with basic IT security best practices.

Topic definition. The Cloud Security Alliance (2009) states that "the ability to govern and measure enterprise risk within a company owned data center is difficult and surprisingly still in the stages of maturation in most organizations. Cloud computing brings new unknowns to governance and enterprise risk" (p. 26). Risks pertaining to public cloud computing are reviewed using the definition for IT-related risks provided by Stoneburner, et al. (2004, p. A-2). The public cloud computing IT-related risks are organized and presented by their potential to align with three primary risk categories as identified by the European Network and Information

Security Agency (ENISA) which are: (a) policy and organizational risks, (b) technical risks, and (c) legal risks (ENISA, 2009, p. 23). The foregoing risks categories are selected from ENISA because they offer the most comprehensive ontology available at this time, with respect to classifying cloud computing IT-related risks.

Focus (included). IT-related risks pertaining to public cloud computing are the subject of this literature review. Armbrust, et al. (2009) describe cloud computing as the sum of Software as a Service and utility computing, but not private clouds (p. 1). IT-related risks pertaining to the three areas known as ‘cloud service delivery models’: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Cloud Security Alliance, 2009, p. 6) are explored.

Focus (not included). Private clouds are not included in this study because they are generally considered to be internal data centers, rather than external data centers operated and managed by public cloud computing service providers (Armbrust et al., 2009, p. 1).

Vaquero, Rodero-Merino, Caceres, and Lindner (2009) state that a source of confusion about cloud computing is its relationship with grid computing (p. 51). Wang, von Laszewski, Kunze, and Tao (2008) distinguish cloud computing from other computing paradigms (including grid computing) in that cloud computing provides: User-centric interfaces, on-demand service provisioning, QoS guaranteed offer, autonomous system, and scalability and flexibility (pp. 5-6). Grid computing is not explicitly excluded from search patterns because there are multiple articles that describe both cloud computing and grid computing. However, articles focused exclusively on grid computing are not included in this literature review.

Ryan (2008) notes cloud computing is a rebranded form of utility computing (p. 31). However, despite its close relation to cloud computing, utility computing is not the focus of this literature review, as utility computing does not include Software as a Service (Armbrust, et al., 2009).

Data Analysis Plan Preview

This study is intended to provide a meaningful overview of public cloud computing IT-related risks. The research is designed as a literature review, and places the topic "within the universe of already existing research" (Obenzinger, 2005, p. 1). The goal is to pull together "diverse perspectives and research results … into a cohesive whole" (Leedy & Ormond, 2005, p. 79). In order to reach this goal, the approach to data analysis selected for use in this study is conceptual analysis, as the process is described by Busch, De Maret, Flynn, Kellum, Le, and Meyers (2005).

Busch, et al. (2005) recommend beginning the conceptual analysis with the identification of research questions and choosing sample literature. Then, the coding process of "selection reduction" (Busch, et al., 2005) is utilized where the text from the selected literature is categorized by keywords that allow for effective content analysis. The keywords in this study are chosen and aligned with the category of IT-related risks related to utilizing public cloud computing service providers. Coding process details are provided in the Research Parameters section of this paper.

Writing Plan Preview

This study searches for key rhetorical patterns within the results of the data analysis process, that determine the scope and content of literature that is reviewed (Obenzinger, 2005, p.

4). Because cloud computing is a new computing technology with a limited history (Wang, et al, 2008, p. 1), a thematic review of cloud computing literature is employed rather than time progression (Literature review, 2007). The public cloud computing IT-related risks are organized and presented by their potential to align with three primary risk categories as identified by the European Network and Information Security Agency (ENISA) which are: (a) policy and organizational risks, (b) technical risks, and (c) legal risks (ENISA, 2009, p. 23).

Definitions

Erdogmus (2009) acknowledges disagreement among subject matter experts in defining the term “cloud computing” (p. 4). Vaquero, et al. (2009) observed over 20 different definitions for cloud computing (p. 50). There is disagreement in the definitions of related terms as well. In the context of this literature review, preference is given to definitions provided by the National Institute of Standards and Technology, a non-regulatory federal agency within the United States (U.S.) Department of Commerce (Mell & Grance, 2009, pp. 1-2). Definitions are also included from business and academic sources where there is some agreement as to their meaning. Citations are noted in each case.

Cloud computing – “Is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, 2009, p. 1).

IDC – Known less by the name “International Data Corporation,” IDC is a market research and analysis firm that provides market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets (IDC, 2009b).

ENISA – The “European Network and Information Security Agency,” (ENISA), is a European Union agency that provides advice and best practices in network and information security (ENISA, 2009).

ISACA – Formerly known as the "Information Systems Audit and Control Association," ISACA is a global organization serving information governance, control, security and audit professionals (ISACA, 2009b).

Grid computing – "Interconnected computer systems where the machines utilize the same resources collectively. Grid computing usually consists of one main computer that distributes information and tasks to a group of networked computers to accomplish a common goal. Grid computing is often used to complete complicated or tedious mathematical or scientific calculations" (Grid computing, n.d.).

Hybrid cloud – Two or more clouds (private, public, etc.) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (Mell & Grance, 2009, p. 1).

Infrastructure as a Service (IaaS) – "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)" (Mell & Grance, 2009, p. 2). Amazon's AWS Elastic Compute Cloud (EC2) is an example of an IaaS offering (Cloud Security Alliance, 2009, p. 22).

IT-Related Risk – "The net mission/business impact considering 1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability, and 2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to: Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information; non-malicious errors and omissions; IT disruptions due to natural or man-made disasters; and failure to exercise due care and diligence in the implementation and operation of the IT" (Stoneburner, et al., 2004, p. A-2)

Managed Cloud – An arrangement whereby the "physical infrastructure is owned by and/or physically located in the organization's datacenters with an extension of management and security control planes controlled by the designated service provider" (Cloud Security Alliance, 2009, p. 19).

Platform as a Service (PaaS) – "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations" (Mell & Grance, 2009, p. 2). Google's AppEngine is an example of a PaaS offering (Cloud Security Alliance, 2009, p. 22).

Private cloud – Consists of "internal data centers of a business or other organization that are not made available to the public" (Armbrust et al., 2009, p. 1). They "may be managed by the organization or a third party and may exist on premise or off premise" (Mell & Grance, 2009, p. 2).

Public cloud – Is "provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment (Cloud Security Alliance, 2009, p. 19).

Risk categories – Risks of similar types that are grouped together under key headings. Categories include reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, outsourcing, people, technology and knowledge (Risk Categories, n.d.). For the purposes of this study, (a) policy and organizational risks, (b) technical risks, and (c) legal risks are the three primary IT-related risk categories pertaining to cloud computing.

Selective reduction – "The central idea of content analysis. Text is reduced to categories consisting of a word, set of words or phrases, on which the researcher can focus. Specific words or patterns are indicative of the research question and determine levels of analysis and generalization" (Busch, et al., 2005).

Software as a Service (Saas) – "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings" (Mell & Grance, 2009, p. 2). SalesForce.com is an example of a SaaS offering (Cloud Security Alliance, 2009, p. 22).

Utility computing – "Is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate. The utility model seeks to maximize the efficient use of resources and/or minimize associated costs" (Stolvoort, 2007, p. 3).

Research Parameters

This section explains the methods used to frame and conduct this literature review. There are five parts to this section, which consist of the following: (a) research question and sub-questions, (b) search strategy, (c) evaluation criteria, (d) data analysis plan, and (e) writing plan. Based on the research question and sub-questions, a search strategy is followed to locate relevant literature. Evaluation criteria determine what to include and exclude from this literature review. A data analysis plan determines how to process the key concepts from the sampled literature, while the writing plan explains how the Review of the Literature section of the paper is organized and written.

Research Question and Sub-questions

Main question. What are the key reported IT-related risks, as defined by Stoneburner, et al. (2004, p. A-2), that should be considered by security practitioners when evaluating public cloud computing service providers?

Sub-questions.

- What is the likelihood that a cloud computing threat source will exploit, or trigger, a particular information system vulnerability?
- What is the resulting impact, legal liability or mission/business loss due to, but not limited to:
  - Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information?
  - Non-malicious errors and omissions?
  - IT disruptions due to natural or man-made disasters?

    - Failure to exercise due care and diligence in the implementation and operation of the IT?
- How can cloud computing customers mitigate identified IT-related risks?

Search Strategy

Search terms. References for the literature review are collected using the search terms and controlled vocabularies listed below. The search terms are mined from the analysis of literature found during initial searches (see the search report in Appendix A). Cloud computing and related definitions from Mell and Grance (2009, pp. 1-2) and the Cloud Security Alliance (2009, pp. 15-24) are mined for additional search terms. Key search terms include:

- Cloud Computing
- Cloud Computing Business Risks
- Cloud Computing Legal Risks
- Cloud Computing Risk Mitigation
- Cloud Computing Risks
- Cloud Computing Security
- Cloud Computing Security Risks
- Cloud Computing Technical Risks
- Infrastructure as a Service
- Managed Cloud
- Platform as a Service
- Public Cloud
- Software as a Service

Literature Resources. Using the keywords above, literature is collected using the following tools, which consist of search engines, databases, and other resources. Google Scholar and Yahoo are the primary search engines utilized to locate cloud computing literature. Both search engines are valuable in locating articles not found in other academic database and index searches. Administratively, Google Scholar is more useful than Yahoo because of its ability to export citations into the EndNote bibliographic manager format.

The following databases were searched to find relevant literature pertaining to cloud computing. Results varied among the databases.

• Academic Search Premier: The EBSCO Host search mode “Find all my search terms” is used and provided effective results by finding many cloud computing articles while eliminating most unrelated meteorological studies.

• ACM Digital Library: The ACM Digital Library yielded fair results. It is difficult to quickly ascertain the quality of the search results, as the database generated many non-descriptive titles, requiring the need to drilldown to abstracts residing on separate web pages. Large published compilations of articles often resulted in false positive search results.

• Business Source Premier: The EBSCO Host search mode “Find all my search terms” is also used and provided good results. There is a fair amount of overlap in results between Academic Search Premier and Business Source Premier, but Business Source Premier located more articles relevant to cloud computing.

• IEEE Xplore: The IEEE Xplore database generated a high proportion of articles related to cloud computing, although the total number of articles was low.

• WorldCat: Not many search results were produced where electronic sources were readily available.

The following additional literature resources are also examined:

Professional organization websites.

Information Security and Governance

- CERT http://www.cert.org
- ISACA http://www.isaca.org

Security Assurance within Cloud Computing

- Cloud Security Alliance http://www.cloudsecurityalliance.org

Evaluation Criteria

Academic and trade publications are reviewed to collect references relevant to security practitioners who evaluate public cloud computing service providers. As cloud computing is still evolving (Wang, et al., 2008, p. 3), an evaluation of both scholarly and non-scholarly literature sources is necessary for this review.

Keyword searches against academic, business, and technical indices yield articles on cloud computing and IT-related risks. Boolean searches using the terms “cloud” and “computing” generate positive results. To reduce the number of irrelevant search results, weather-related terms such as “meteorology” and “meteorological” are explicitly excluded from key search terms. However, the word “weather” is not an exclusionary search term, as its inclusion in common phases such as “weather the storm” might potentially omit otherwise useful and relevant articles.

Literature relevant to public cloud computing is restricted to articles published during or after 2007. Although Salesforce.com was founded 1999 (Service Cloud, n.d., p. 2), stalwarts Amazon AWS and Google Apps did not enter the cloud computing services industry until 2006, and the term “cloud computing” was not widely known until early 2007 (Lasica, 2009, p. 5). By restricting literature results to not precede 2007, search results for similar but importantly different computing service paradigms, such as grid computing and utility computing, are minimized.

To determine the credibility of research content for this study, each article is evaluated using pre-specified criteria. This study gives preference to scholarly (or academic or expert) over non-scholarly (or popular) research sources” (Smith, T., 2009), but non-scholarly works are included if they are determined to embody important characteristics that are otherwise considered scholarly.

To be considered scholarly, the intended audience for articles written on cloud computing IT-related risks should be comprised of security “practitioners” (Smith, T., 2009), not individuals unfamiliar with IT in general or cloud computing in particular. Conversely, the credentials of each author are also reviewed with the expectation that they too are “experts in the field” (Smith, T., 2009) of cloud computing and/or IT security, not just journalists or freelance writers. Credentials demonstrating the author’s expertise, which are typically either at the beginning or ending of each article, are also reviewed. Articles are also evaluated by the presence and level of citation that is accompanied by a “bibliography, references, notes and/or works cited section” (Smith, T., 2009), and given preference over articles that rarely include footnotes.

Another quality indicator for articles used in this study is determined by whether an article has been subject to editorial “peer review” by a board of outside scholars, as opposed to editors of the publisher (Smith, T., 2009). Of the journal articles examined for potential use in this study, those that are “juried” (judged by respected colleagues in the author’s field) are preferred over “nonjuried” articles (appears in a journal without first being screened by one or more experts) (Leedy & Ormond, 2005, p. 9).

Data Analysis Plan

In this study, selected literature from many different sources is analyzed to identify the IT-related risks of cloud computing. Several relevant articles pertain to one or more of three distinct cloud computing IT-related risk categories: (a) policy and organizational, (b) technical, and (c) legal, all of which provide the organizational foundation upon which this literature review is based.

To ensure that the literature in this study is synthesized properly (Leedy & Ormond, 2005, p. 79), procedures established by subject matter experts in the field of data analysis are followed. To analyze literature in an objective, reliable, and valid manner, this study employs the content analysis methodology (also known as conceptual analysis), described by Busch, et al. (2005). They describe content analysis as the processing and coding of text from selected literature through eight steps described below, reducing it into manageable content categories.

The “level of analysis” (Busch, et al., 2005) applied to coding literature content is at the key phrase level. For example, although the words “cloud” and “computing” are not useful by themselves, using the phrase “cloud computing” provides more precision for the relevant codifying of text, and, for the purposes of this literature review, must be located within each literature sample.

Although Busch, et al. (2005) give researchers a choice between “pre-defined” or “interactive” categories, a combination of both pre-defined and interactive sets of IT-related cloud computing risk categories is utilized. Major risk categories (policy and organizational, technical, and legal) are pre-defined and by definition do not change. However, as there are different types of IT-related cloud computing risks that are included within each major risk category (ENISA, 2009, pp. 22-51), flexibility is employed to allow "new, important material to be incorporated into the coding process that could have significant bearings on one's results" (Busch, et al., 2005). Each individually identified IT-related risk within the above risk categories pertains to one, two, or all three of the cloud service delivery models (IaaS, PaaS, and SaaS), depending on the risk.

Considered a key decision in the coding process (Busch, et al., 2005), this literature review codes for the "existence" of key phrases rather than the "frequency" of them, as the number of times an IT-related risk pertaining to cloud computing is mentioned is not positively correlated to the quality or depth of research being conducted.

As Leedy and Ormond (2005) state that literature reviews put together "diverse perspectives and research results … into a cohesive whole" (p. 79), a "level of generalization" (Busch, et al., 2005) is used that accommodates for subtle differences in the naming of IT-related risks. For example, with respect to the term "lock-in" (ENISA, 2009, pp. 24-27) that falls within the "policy and organizational" risk category, the terms "data lock-in" (Armbrust, et al., 2009, pp. 14-15) and "vendor lock-in" (Brandel, 2009, p. 23) are also included and coded as similar but distinct terms. To ensure such phrases are coded within the correct risk category, "translation rules" are used (Busch, et al., 2005), but phrases that are not relevant to IT-related cloud computing risks are disregarded.

Although irrelevant phrases are not recorded in the coding process, information is initially viewed as relevant and important and used "to reexamine, reassess and perhaps even alter the … coding scheme" (Busch, et al., 2005). By extending the potential scope of coding phrases, the intention is to “define them with increasing precision to produce narrower terms” (Hewitt, 2002, p. 17) that enables more relevant coding throughout the entire body of literature.

Text is coded manually but with the use of electronic tools. For example, an electronic spreadsheet is used to keep track of coded text, including the coded phrase itself, the source of the text (author, title, and page number), the IT-related risk category (policy and organizational, technical, and/or legal), and the IT-related risk. Automated content analysis programs are not used, as “when coding is done manually, a researcher can recognize errors far more easily” (Busch, et al., 2005).

After coding of the selected literature is completed, results are analyzed and conclusions are drawn from the results (Busch, et al., 2005). It is during this final step of content analysis that cloud computing IT-related risks are identified, classified, and better understood within their overall context. Details are provided below, in the Writing Plan. With properly coded results, this study is able to proceed with evaluating, organizing, and synthesizing “what others have done” (Leedy & Ormond, 2005, p. 77).

Writing Plan

Subject matter relating to IT-related cloud computing risks is obtained from literature using the content analysis methodology (Busch, et al., 2005) described in the foregoing Data Analysis section. Wang, et al. (2008) describe cloud computing as a “new paradigm” (p. 1), and there has not been significant “discussion or analysis of contemplation of implications or anticipation of further research” (Obenzinger, 2005). Due to the short history of cloud computing, a thematic presentation of the results of the data analysis process frames the development of the Review of the Literature section of the paper. The thematic approach is utilized because it is "organized around a topic or issue, rather than the progression of time" (Literature review, 2007).

The primary goal of this literature review is to describe the IT-related risks of cloud computing and how such risks can be mitigated. Using the definition for "IT-related risk" by Mell and Grance (2009), cloud computing IT-related risks within each risk category are described in terms of probability, impact, and/or vulnerability (p. 1-2).

The following two larger themes are anticipated – risks are presented in the order of perceived overall highest risk to lowest risk as presented by ENISA (2009, pp. 9-10).

Theme 1: Risk Categories - ENISA (2009) has identified three risk categories that are specific to cloud computing (p. 23) that are used as an initial overarching thematic framework for describing the numerous cloud computing IT-related risks.

• **Policy and Organizational Risks**: IT-related risks falling within this risk category are not technical per se, but include risks that are ranked high by ENISA (2009, pp. 24-28).

• **Technical Risks**: IT-related risks falling within this risk category are technical in nature.

• **Legal Risks**: IT-related risks falling within this category are legal in nature and include risks that are ranked high by ENISA (2009, pp. 44-45). There are numerous IT-related risks in this category, as the Cloud Security Alliance (2009) states that "numerous United States laws require public and private organizations to protect the security of their information and computer systems" (p. 30).

Theme 2: Mitigation Strategies - Mitigation strategies for reducing IT-related cloud computing risks in the above three risk categories are also described in this study.

• **Audit controls**: This mitigation strategy pertains not only to the organizations using cloud computing services, but to the cloud computing service providers as well.

• **Policies and procedures**: This mitigation strategy pertains to the development and maintenance of a myriad of documents used to ensure policies are enforced in conjunction with cloud computing services.

• **Other forms of corporate governance**: There are several other methods and tools available for organizations to use that are also important, as cloud computing "brings new unknowns to governance and enterprise risk" (Cloud Security Alliance, 2009, p. 26).

Annotated Bibliography

The annotated references in this study have been obtained from several different types of sources and provide the literature most significant to the development of this study on IT-related cloud computing risks. Abstracts are included, which provide a "summary of an article or research study" (Leedy & Ormond, 2005) and the original literature source. Comments attesting to the credibility and relevancy of each literature source are also included for the 21 key references below, as well as an explanation of the way each reference is used to support this study.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. (2009). *Above the Clouds: A Berkeley view of cloud computing.* Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

Abstract. Provided certain obstacles are overcome, we believe Cloud Computing has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new interactive Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get their results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. The economies of scale of very large-scale datacenters combined with ``pay-as-you-go" resource usage has heralded the rise of Cloud Computing. It is now attractive to deploy an innovative new Internet service on a third party's Internet Datacenter rather than your own infrastructure, and to gracefully scale its resources as it grows or declines in popularity and revenue. Expanding and shrinking daily in response to normal diurnal patterns could lower costs even further. Cloud Computing transfers the risks of over-provisioning or under-provisioning to the Cloud Computing provider, who mitigates that risk by statistical multiplexing over a much larger set of users and who offers relatively low prices due better utilization and from the economy of purchasing at a larger scale. We define terms, present an economic model that quantifies the key buy vs. pay-as-you-go decision, offer a spectrum to classify Cloud Computing providers, and give our view of the top 10 obstacles and opportunities to the growth of Cloud Computing.

Comments. This report provides a technical and economic overview of cloud computing. The top ten obstacles and opportunities associated with cloud computing are explored, which pertain to the technical obstacles to the adoption of cloud computing, technical obstacles to the growth of cloud computing, and policy and business obstacles to the adoption of cloud computing. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Signficance, Delimitations, and Review of the Literature sections of this study. The authors consist of computer science faculty members and graduate students affiliated with the Reliable Adaptive Distributed (RAD) System Lab at the University of California at Berkeley.

Brandel, M. (2009). Exit strategy. (Cover story). *Computerworld*, *43*(13), 22-26. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=37614378&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article focuses on how high technology industries in the U.S. escape from the hassles brought about by locking-in into cloud computing. It notes that cloud computing is a computer architecture wherein companies consume technologies resources as an Internet service rather than as an owned system. According to John Willis, a systems management consultant who blogs about information technology (IT) management and cloud computing, much of the fear of lock-in is caused by misconceptions.

Comments. Vendor lock-in is the primary IT-related cloud computing risk described in this article. The article explores and describes the potential for vendor lock-in within the different cloud service delivery models (including Saas, PaaS, and IaaS), along with guidance to minimize risk. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature sections of this study. This article is considered credible as it comes from a magazine that provides information to technology managers and is published in many countries around the world. The author has written extensively on IT-related topics.

Cachin, C., Keidar, I., & Shraer, A. (2009). Trusting the cloud. *SIGACT News*, *40*(2), 81-86. doi: http://doi.acm.org/10.1145/1556154.1556173

Abstract. More and more users store data in "clouds" that are accessed remotely over the Internet. We survey well-known cryptographic tools for providing integrity and consistency for data stored in clouds and discuss recent research in cryptography and distributed computing addressing these problems.

Comments. This article addresses data privacy, availability, integrity, and other risks as they relate to cloud computing. Cryptographic tools that address these risks are surveyed and described. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. The authors, which include an IBM researcher, Professor of Computer Science, and doctoral student, have several published journal and conference papers in the areas of distributed computing, cryptology, and distributed storage.

Cloud Security Alliance. (2009). *Security guidance for critical areas of focus in cloud computing*. Retrieved from http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

Abstract. The report focuses on outlining initial areas of concern and guidance for organizations adopting cloud computing. The intention is to provide security practitioners with a comprehensive roadmap for being proactive in developing positive and secure relationships with cloud providers.

Comments. This report provides security practitioners with a guide to focus on IT-related cloud computing risks and mitigation strategies. In the report, there are fifteen domains, each described in depth, that collectively span all three IT-related risk categories that are described in this study. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance, Audience, Delimitations, Search Strategy, Writing Plan, and Review of the Literature sections of this study. The resource is considered credible in that there are 17 primary authors and 26 contributing reviewers from several well-known and reputable organizations that provided input into the report.

Creeger, M. (2009). CTO roundtable: Cloud computing. *Communications of the ACM, 52* (8), 50-56. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=43479961&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article presents a discussion of topics in computer science related to cloud computing, featuring the opinions of high-ranking technology executives from several major corporations. Participants in the discussion include Werner Vogles, the chief technical officer (CTO) at Amazon.com, Greg Olsen, CTO of Coghead, and Lew Tucker, CTO of cloud computing at Sun Microsysterms. Topics addressed include the usefulness of cloud computing for various types of business models in terms of capitalization, cost effectiveness and economic flexibility.

Comments. This article is based on a roundtable discussion of subject matter experts who describe cloud computing and the business drivers behind it. Although much of the article describes the benefits of cloud computing, IT-related risks, including scalability, are discussed. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. This article is considered credible as it appears within a peer-reviewed journal and the roundtable participants are all experts in cloud computing services.

ENISA. (2009). *Cloud computing: benefits, risks and recommendations for information security*. Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Abstract. The paper provides an assessment of the security risks and benefits of using cloud computing.

Comments. This paper provides security guidance for potential and existing users of cloud computing. Twenty-four risks are described in the policy and organizational, technical, and legal risk categories. For each risk, the probability, impact, vulnerability, affected assets, and risk rating are identified and described. Research and legal recommendations to mitigate such risks are also included. The reference is included in the data set for coding, and supports ideas presented in the Delimitations, Writing Plan Preview, and Review of the Literature sections of this study. Over twenty individuals from several private and governmental organizations contributed to the paper. The resource is considered credible due in part to ENISA's personnel assuming editorial responsibilities.

Erdogmus, H. (2009). Cloud Computing: Does nirvana hide behind the nebula? *IEEE Software*, *26*(2), 4-6. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04786942

Abstract. The article focuses on cloud computing, a new method of using software through the Internet and doing away with software on individual desktops. The technology shifts the focus of software development from pure Software as a Service (SaaS) to software infrastructure as a service as a result of advances in virtualization technologies and a realization of the financial burden involved in maintaining proprietary information technology infrastructure.

Comments. The article takes a holistic view of cloud computing by exploring the definition of cloud computing, performance limitations, software development opportunities, platform independency, and challenges associated with capacity and operational management. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance, Definitions, and Review of the Literature sections of this study. The resource is considered credible in that the author holds a Ph.D. degree in Telecommunications and is the Editor in Chief of IEEE Software, which is peer-reviewed.

Finnie, S. (2008, October 6). Peering behind the cloud. *Computerworld*, p. 22. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=34703832&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The author reflects on the development of cloud computing. He asserts that cloud computing is already a minefield in the computer world with potentials to cut costs as shown by most chief information officers (CIOs) and information technology (IT) organizations. He argues that IT organizations are not yet ready to take a big chance on a technology that is not fully mature. He suggests that organizations must build vendor relationships to understand the potential capacity of technology service.

Comments. This article recommends and justifies that organizations should consider experimenting with cloud computing services sooner rather than later to become more knowledgeable of the associated IT-related risks. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. This article is considered credible as it comes from a magazine that provides information to technology managers and is published in many countries around the world. The author is Editor in Chief at and has written on IT-related subject matter for 25 years.

Gatewood, B. (2009). Clouds on the information horizon: How to avoid the storm. *Information Management (15352897)*, *43*(4), 32-36. Retrieved from Academic Search Premier database:

http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=43659227&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article presents the cloud-based solutions in the U.S. It states that communications are a natural fit for cloud computing solutions because they are uniformly relying on the basic infrastructure which is the Internet. Another is the disaster recovery and business continuity because utilizing the cloud infrastructure for storing or managing business-critical information makes sense if the proper controls are in place. Despite the advantages of the solutions, the records and information management, information technology and legal staff must also understand the disadvantages in order to identify possible risk and minimize them.

Comments. The article describes the typical applications available from cloud computing service providers. In addition, IT-related risk issues related to electronic discovery, privacy concerns, and compliance difficulties are described in detail. A checklist for evaluating cloud-based initiatives is also provided and serves as a guide to writing better contracts, ensuring adequate audit controls, implementing acceptable policies and procedures. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance and Review of the Literature sections of this study. The author is a Certified Records Manager, has worked in records management for over a decade, and is a local and national speaker on records management and related topics.

Hayes, B. (2008). Cloud computing. *Communications of the ACM*, *51*(7), 9-11. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=34059107&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article discusses cloud computing, examining the shift in computing that is occurring in 2008 from locally installed programs to the computer cloud. The term computer cloud, also known as "Internet as platform," infers that the locus of computation occurs at data centers connected through the Internet, in places near and far from the user. Topics include the surrender of control of computing resources to third-party service providers, the client-server model of the 1980's, and the hub-and-spoke model of time-sharing systems.

Comments. This article describes the shift from customer controlled computing to cloud service provider controlled computing. Cloud computing IT-related risks including privacy, security, scalability, and reliability are also discussed. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance and Review of the Literature sections of this study. This article is judged to be credible as submissions are reviewed by a communications editorial board and editor-in-chief and the author has written over one hundred articles on computing science.

ISACA. (2009). *Cloud Computing: Business benefits with security, governance and assurance perspectives*. Retrieved from http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=53044

Abstract. Globalization and recent economic pressures have resulted in increased requirements for the availability, scalability and efficiency of enterprise information technology (IT) solutions. A broad base of business leaders has become increasingly interested in the costs and the underlying technology used to deliver such solutions because of their growing impact on the bottom line. Many parties claim that "cloud computing" can help enterprises meet the increased requirements of lower total cost of ownership (TCO), higher return on investment (ROI), increased efficiency, dynamic provisioning and utility-like pay-as-you-go services. However, many IT professionals are citing the increased risks associated with trusting information assets to the cloud as something that must be clearly understood and managed by relevant stakeholders. This paper clarifies what cloud computing is, identifies the services offered in the cloud, and also examines potential business benefits, risks and assurance considerations.

Comments. This article addresses what cloud computing is and why it is becoming so popular. In addition, the benefits of cloud computing are briefly described, followed by an overview of risks and security concerns, which include choosing the right provider, proper information handling, confidentiality, commingling of information assets, and disaster recovery and business continuity. Service level agreements and other governance and change issues are provided as examples to mitigate IT-related cloud computing risks. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance, Audience, and Review of the Literature sections of this study. The source is considered credible, as it was published by a global organization serving information governance, control, security and audit professionals.

Kaufman, L. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE, 7*(4). doi: http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2009.87

Abstract. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. In this new world of computing, users are universally required to accept the underlying premise of trust. Within the cloud computing world, the virtual environment lets users access computing power that exceeds that contained within their own physical worlds. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs. The data you can find in a cloud ranges from public source, which has minimal security concerns, to private data containing highly sensitive information (such as social security numbers, medical records, or shipping manifests for hazardous material). Does using a cloud environment alleviate the business entities of their responsibility to ensure that proper security measures are in place for both their data and applications, or do they share joint responsibility with service providers? The answers to this and other questions lie within the realm of yet-to-be-written law. As with most technological advances, regulators are typically in a "catch-up" mode to identify policy, governance, and law. Cloud computing presents an extension of problems heretofore experienced with the Internet. To ensure that such decisions are informed and appropriate for the cloud computing environment, the industry itself should establish coherent and effective policy and governance to identify and implement proper security methods.

Comments. This paper examines security issues and associated regulatory and legal concerns as they relate to cloud computing. A background of cloud computing is described, followed by concerns relating to data confidentiality, integrity, and availability. Cloud computing is described as a tempting target for cybercriminals that raises regulatory questions and calls for proactive measures to ensure security. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. This article is judged to be credible because it appears in a peer-reviewed journal and is written by an author who has a Ph.D. in Electrical Engineering and has research interests including cyber security, software assurance, and biometrics.

Leavitt, N. (2009). Is cloud computing really ready for prime time? *Computer*, *42* (1), 15-25. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04755149

Abstract. Even though the technology faces several significant challenges, many vendors and industry observers predict a bright future for cloud computing.

Comments. This articles describes what cloud computing is, how much it is expected to grow, along with the advantages and disadvantages with using cloud computing service providers. Several IT-related cloud computing risks are described and include vendor lock-in and system performance, latency, and reliability. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance, Delimitations, and Review of the Literature sections of this study. This article is judged to be credible because it appears in a peer-reviewed journal and the author is regular contributor to a number of technology and interactive marketing publications.

Nelson, M. (2009). The cloud, the crowd, and public policy. *Issues in Science & Technology*, *25*(4), 71-76. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=43278297&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article focuses on the phase of computing called Cloud computing which includes activities like Web 2.0, Web services, and the Grid. According to the article, expectations from leading technologists depicts that within 5 to 10 years, 80% or 90% of the world's computing and data storage will occur in the Cloud. It is stated that the pace of development and implementation of the Cloud relies on various factors. It mentions that the factors include the speed of a basic technology's maturation, the speed of computer and telecommunications industries to agree on standards, and the aggressiveness of companies to invest in the needed infrastructure.

Comments. This article includes discussion on a number of challenges and risks that need to be addressed for cloud computing. Three different future scenarios for cloud computing are reviewed that range from closed solutions based on proprietary standards and government policies to open solutions based on open standards, open interfaces, and open-source software. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance and Review of the Literature sections of this study. This article is judged to be credible because it appears in a peer-reviewed journal and the author has a Ph.D. in Geophysics and teaches courses and conducts research on the future of the Internet, cyber-policy, technology policy, innovation policy, and e-government.

Rai, S., & Chukwuma, P. (2009). Security in a cloud. *Internal Auditor*, *66*(4), 21-23. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=43703716&loginpage=Login.asp&site=ehost-live&scope=site

Abstract. The article discusses how auditors can address individually the separate environments of the identity and access management (IAM) solutions namely the client environment, the service provider's environment and the Internet cloud as part of a single strategy. An elaboration on how organizations have utilized IAM solutions to meet security administration functions and meet compliance and regulatory requirements is presented. The various risks that auditors need to assess in the three IAM elements are identified.

Comments. This article describes the mitigation strategies that auditors and security practitioners must follow when IT security administration is outsourced to cloud computing service providers. To mitigate IT-related cloud computing risks such as insecure data or intercepting data in transit, a three-pronged audit strategy is presented that addresses the key areas of concern. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. This article is judged credible as it is intended for internal audit professionals and was evaluated by an editorial policy review board. The authors have over 50 years of combined experience in information technology and both hold the Certified Information Systems Security Professional (CISSP) certification.

Rash, W. (2009). Is cloud computing secure? Prove it. *eWeek, 26*(16), 8-10. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=44601453&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article examines the security of cloud computing and its future in the information technology (IT) industry. It states that its security is still questionable as the public cloud providers do not have the capability to meet regulatory requirements and the means to meet the compliance issues related to security. It states that the deployment of a private cloud is one way to balance security with its efficiency.

Comments. This article describes the challenges that customers may face with respect to mitigating IT-related cloud computing risks. For organizations that face stringent government or industry compliance rules, using public cloud computing service providers may not currently be a viable option, as compliance audit failures would be likely. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance and Review of the Literature sections of this study. This

article is judged to be credible as the author has written about and tested computer and network products for over 30 years.

Ryan, V. (2008). A place in the cloud. *CFO*, *24*(8), 31-35. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=34514238&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article discusses the implication of cloud computing which refers to a concept that takes outsourcing, software as a service, and similar rent-don't-own trends to their logical conclusion. Despite the claims of some executives that cloud computing is the best model for running information technology (IT) system, issues on its risks are in debate. Major Horton, chief financial officer (CFO) of Nirvanix Inc., explained that companies are still struggling with the use of cloud computing.

Comments. This article provides an overview of cloud computing and IT-related risks, including the possibility that non-IT personnel could violate governance policies and government regulations. Mitigation strategies are also described and include using metrics-driven technologies. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance, Delimitations, and Review of the Literature sections of this study. This article is considered credible as it is a requested controlled circulation title magazine with registered readers who are senior level financial decision makers.

Smith, J. (2009). Fighting physics: A tough battle. *Communications of the ACM*, *52*(7), 60-65. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=43019152&loginpage=login.asp&site=ehost-live&scope=site

Abstract. The article discusses the software-as-a-service (SaaS) option that companies use to save money and simplify corporate computing infrastructures. The author indicates that the Internet's routing infrastructure and the laws of physics affect the levels of performance associated with SaaS. Other topics include limitations that engineers face when developing distributed applications, the combined impact of the speed of light and the physics of distance on a distributed application, and network hops with which software engineers should be familiar.

Comments. This article primarily addresses the technical category of cloud computing IT-related risks. Although bandwidth affects performance, propagation delay impacts performance as well and is described as an important physical limit with respect to network performance. Suggested strategies to maximize performance and mitigate performance-related risks are described. The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. This article is judged to be credible because the author is a Professor of Engineering and Applied Science and it is published in a peer-reviewed journal.

Vaquero, L., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review, 39*(1), 50-55. doi: http://doi.acm.org/10.1145/1496091.1496100

Abstract. This paper discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches.

Comments. This article is applicable to describing the definition of cloud computing and distinguishing cloud computing from grid computing. Features are compared between cloud computing and grid computing. Lack of standardization is one feature that is appears to be a cloud computing IT-related risk. The reference is included in the data set for coding, and supports ideas presented in the Delimitations, Definitions, and Review of the Literature sections of this study. This article is judged to be credible as it contains several citations to academic and professional sources. The authors are researchers at Telefónica Investigación y Desarrollo (TID) and SAP Research.

Viega, J. (2009). Cloud computing and the common man. *Computer, 42* (8), 106-108. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=05197438

Abstract. The cloud offers several advantages, but until some of its risks are better understood many major players might hold back.

Comments. This article describes the three primary cloud service delivery models (IaaS, PaaS, and SaaS) and the IT-related cloud computing risks within each model. The reference is included in the data set for coding, and supports ideas presented in the Problem Area/Significance and Review of the Literature sections of this study. This article is judged to be credible because the author has written many security books and has performed extensive standards work in the IEEE and IETF. The article is published in a peer-reviewed journal.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stèoßer, J. (2009). Cloud computing - A classification, business models, and research directions. *Business & Information Systems Engineering*, *1*(5), 391-399. Retrieved from: http://www.springerlink.com/content/w3h62858jpkw56kh

Abstract. Lately, a new computing paradigm has emerged: "Cloud Computing". It seems to be promoted as heavily as the "Grid" was a few years ago, causing broad discussions on the differences between Grid and Cloud Computing. The first contribution of this paper is thus a detailed discussion about the different characteristics of Grid Computing and Cloud Computing. This technical classification allows for a well-founded discussion of the business opportunities of the Cloud Computing paradigm. To this end, this paper first presents a business model framework for Clouds. It subsequently reviews and classifies current Cloud offerings in the light of this framework. Finally, this paper discusses challenges that have to be mastered in order to make the Cloud vision come true and points to promising areas for future research.

Comments. This article better identifies what cloud computing is and provides a business model framework that gives examples of providers as they relate to each cloud service delivery model (e.g. IaaS, PaaS, and SaaS). The reference is included in the data set for coding, and supports ideas presented in the Review of the Literature section of this study. The authors consist of professors and graduate students from the Institute of Information Systems and Management at the Karlsruhe Institute of Technology. This article is an electronic translation from the German journal Wirtschaftsinformatik, which is peer-reviewed.

Review of the Literature

This review identifies the key reported IT-related risks that should be considered by security practitioners when evaluating public cloud computing service providers. Over fifty references, produced by technical and legal experts from public and private organizations in the United States and abroad, are evaluated, organized, and synthesized for this study. Of the aforementioned collection, approximately thirty references are used to identify and describe the various IT-related cloud computing risks that organizations need to evaluate and mitigate.

This review focuses on a presentation of the primary IT-related risks of cloud computing and suggested mitigation strategies. IT-related risks are classified into three risk categories: (1) policy and organizational risks, (2) technical risks, and (3) legal risks. Mitigation strategies include: (1) audit controls, (2) policies and procedures, (3) service level agreements, and (4) other forms of governance.

Risk Categories

Policy and organizational risks.

These are business-related IT risks that organizations may face when considering cloud computing service providers. Such risks include lock-in, loss of governance, compliance challenges, loss of business reputation, and cloud service termination or failure.

Lock-in. Brandel (2009) states that vendor lock-in is one of the primary concerns expressed by IT leaders when considering a move to cloud computing service providers (p. 23). Lock-in refers to the inability of a customer to move their data and/or programs away from a cloud computing service provider (Armbrust, et al., 2009, p. 15). Although some cloud computing vendors debate whether lock-in exists, most agree there are reasons for concern (Brandel, 2009, p. 23). As noted by Armbrust et al. (2009), "concern about the difficulty of extracting data from the cloud is preventing some organizations from adopting cloud computing" (p. 15).

Additionally, although Armbrust, et al. (2009) note that interoperability has improved among platforms, application programming interfaces for cloud computing itself are still largely proprietary (p. 15), particularly at the SaaS and PaaS level (Brandel, 2009, p. 24). Such interfaces restrict the ability for consumers to swap one provider for another (Buyya, Yeo, & Venugopal, 2008, p. 7). According to Douglis (2009), interoperability is not only important to consumers but to the cloud ecosystem as a whole (p. 5). ENISA (2009) states that there are currently few "tools, procedures or standard data formats or services interfaces that guarantee data, application or services portability" that as a result "can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment" (p. 9).

The observation is made that "cloud providers may have an incentive to prevent (directly or indirectly) the portability of their customers services and data" (ENISA, 2009, p. 24). While customer lock-in may be attractive to cloud computing providers, customers are vulnerable to price increases, to reliability problems, or even to providers going out of business (Armbrust, et al., 2009, p 15). In addition, if customers "grow dissatisfied with the service or the vendor goes under, data and/or applications will need to be reformatted to be moved, which could be complex and costly" (Brandel, 2009, p. 24). Viega (2009) suggests that one motivating factor for lock-in is that vendors look to increase their prices (p. 107).

Douglis (2009) notes that in addition to wanting to be able to move from one cloud provider to another without dramatic reimplementation, customers may also want to be able to use multiple clouds at once (p. 5). As cloud computing is still maturing, not many users have faced these problems yet (Kim, 2009, p. 68).

Loss of governance. ENISA (2009) identifies the potential loss of governance as a top security risk, as customers may cede control to cloud computing service providers on a number of issues that may impact their security, mission, and goals (p. 28). According to the Cloud Security Alliance (2009), businesses are vulnerable when they entrust their data to a third party, and many things can go wrong (p. 33). For example, Ryan (2008) cautions that non-IT personnel within the customer's organization could easily violate governance policies by moving sensitive customer data into the cloud (p. 34).

Finnie (2008) states that cloud computing is a "minefield" for most CIOs and IT organizations (p. 22), meaning that the impact from the loss of control may lead to the inability to comply with security requirements, a lack of confidentiality, integrity, and availability of data, a deterioration of performance and quality of service, and the introduction of compliance challenges (ENISA, 2009, p. 28). Many of the leading cloud service providers do not accept responsibility for the data stored in their infrastructure, which means that they also do not accept any transference of risk (Cloud Security Alliance, 2009, p. 26).

Compliance challenges. According to the Cloud Security Alliance (2009), the lack of governance over audits and industry standard assessments may leave cloud computing customers "without a view into the processes, procedures, and practices of the provider in the areas of access, identity management, and segregation of duties non-inclusively leaving control risks an unknown quantity" (p. 27). That is, cloud computing service providers need to be more transparent so customers can ensure they meet the appropriate rules and regulations. Organizations that seek to obtain certification (such as in an industry standard or a regulatory requirement) may be put at risk because cloud computing service providers may not be able to provide evidence of their own compliance with the necessary requirements or may not permit an audit by the cloud customer (ENISA, 2009, p. 9). For example, Amazon's EC2 service offering may not allow customers to achieve Payment Card Industry (PCI) compliance on their platform, effectively preventing customers from using EC2 to handle credit card transactions (ENISA, 2009, p. 29). For PCI related transactions, the Cloud Security Alliance (2009) recommends that organizations should use existing payment processors that are certified and have passed their point-in-time assessment (pp. 27-28).

Loss of business reputation. Businesses that use cloud computing services are at risk in that one customer's bad behavior can negatively impact the reputation of the cloud as a whole (Armbrust, et al., 2009, p. 18). Armbrust, et al. (2009) cite an example, hypothesizing that IP addresses by spam-prevention services may limit the types of applications that can be hosted on the cloud (p. 18). In addition, Armbrust, et al. (2009) believe that any potential legal liabilities in this example, would remain with the customer, not with the cloud computing service provider (p. 18).

Cloud service termination or failure. The financial viability of cloud service providers is a critical issue and should be evaluated as part of initial due diligence when considering a move to a cloud computing service provider, and on an ongoing basis (Cloud Security Alliance, 2009, p. 26). It is possible that in the short or medium term that some cloud computing services could be terminated due to competitive or financial pressures (ENISA, 2009, p. 30). Not only can service terminations impact cloud computing customers, but downstream customers as well (ENISA, 2009, p. 30). The termination of a cloud service contract is the point at which data is most at risk of data loss because both the client and provider are distracted (Cloud Security Alliance, 2009, p. 32). Armbrust, et al. (2009) and Cachin, Keidar and Shraer (2009) refer to the 2008 failure of The Linkup, an online storage service, as a worst case example of a cloud computing storage provider going out of business. To soften the blow of such disruptions, the Cloud Security Alliance (2009) recommends that cloud computing customers should consider having an alternate location that can take on the services previously rendered by the cloud computing service provider (p. 50). Such a location could either be the customer's own data center, or at another cloud computing service provider site. Viega (2009) also states that customers should maintain their own backups in addition to those taken by the cloud computing service provider, but adds that it is generally easier with IaaS than with PaaS or Saas (p. 108).

Technical Risks

These are IT-related risks that have a direct, technological impact on the cloud computing systems that host customer programs and/or data. Such risks include availability of service, resource exhaustion, intercepting data in transit, data transfer bottlenecks, and distributed denial of service.

Availability of service. Armbrust, et al. (2009) describe availability of service as the number one obstacle to the growth of cloud computing (p. 14). Management of a cloud computing service by a single vendor creates a potential environment for a single point of failure. As noted by Armbrust et al. (2009) this is because even if the vendor has multiple datacenters in different geographic regions using different network providers, the vendor may have common software infrastructure and accounting systems, or may go out of business altogether (Armbrust, et al., 2009, p. 14). Although Armbrust, et al. (2009) believe few enterprise IT infrastructures are as good as Amazon's Simple Storage Service (S3) or Google's AppEngine and Gmail, reported multi-hour outages from both companies underscore the risk that cloud computing problems can and do occur (p. 14). In another reported instance, Salesforce.com suffered a six hour outage in February 2008 (Leavitt, 2009, p. 19).

Abadi (2009) states that "clouds are typically built on top of cheap, commodity hardware, for which failure is not uncommon. Consequently, the probability of a failure occurring during a long-running data analysis task is relatively high" (p. 6).

Network performance can also be a problem for customers who are located a long geographical distance from the cloud provider (Leavitt, 2009, p. 18). Network latency and propagation delay are limited by the speed of light, which is finite, and are factors that are overlooked by engineers developing cloud based applications (Smith, J., 2009, p. 60). Without adequate network performance, applications communicating over large distances can slow down (Smith, J., 2009, p. 64).

Resource exhaustion. Cloud computing services are considered on-demand, which suggests a level of calculated risk because resources of a cloud service are allocated to statistical projections (ENISA, 2009, p. 33). Although virtual machines used in cloud computing efficiently share CPUs and main memory, disk I/O sharing is more problematic (Armburst, et al., 2009, p. 17). In particular, high performance computing applications and transactional database systems may lead to performance unpredictability and/or resource exhaustion. With respect to high performance computing applications, Armbrust, et al. (2009) believe the problem with virtual machines and operating systems is that they do not currently provide a programmatic way to ensure all threads of a program run simultaneously (p. 17).

In some applications transactional database systems may not be suitable for the cloud, as "getting additional computational resources is not as simple as a magic upgrade to a bigger and more powerful machine on the fly" (Abadi, 2009, p. 2). Furthermore, Abadi (2009) argues that read intensive analytical data management systems are more appropriate than transactional data management applications for deployment in the cloud, as providers may not be able to offload data processing in a parallel manner (p. 2).

With regard to data storage, Youseff, et al. (2008) argue that availability, scalability and performance are conflicting goals, as the requirements for each of these individual needs are rigorous (p. 5).

Intercepting data in transit. As a distributed architecture, cloud computing implies more data is in transit than in traditional infrastructures (ENISA, 2009, p. 37). Brynko (2008) states that data is usually at risk when it is in transit, so organizations need to make sure data are encrypted at all phases (p. 23). According to the Cloud Security Alliance (2009), cloud computing "can be thought of as radical deperimeterization", that results in security issues (p. 72). Encryption should be strong and employ key management that allows customers to keep data encrypted and therefore private (Cloud Security Alliance, 2009, p. 72). Possible threat sources without proper encryption include sniffing, spoofing, man-in-the-middle attacks, side channel and replay attacks (ENISA, 2009, p. 37).

Data transfer bottlenecks. As Armbrust, et al. (2009) observe, applications are becoming more data-intensive and expensive (p. 16). It is generally less expensive to ship large volumes of data (e.g. via FedEx), as “disk capacity and cost-per-gigabyte are growing much faster than network cost-performance” (Armbrust, et al., 2009, p. 16).

Abadi (2009) cautions customers to be careful when examining the details of data replication schemes that cloud vendors provide, noting that Amazon’s EBS (elastic block store) will only replicate data within the same availability zone and is thus more prone to failures (p. 3).

In addition to wide area network (WAN) bottlenecks, intra-cloud networking technology may be a bottleneck as well (Armbrust, et al., 2009, p. 16). Although 10 Gigabit Ethernet is commonly used for the aggregation links in cloud networks, it is currently too expensive to be used by individual servers, which often utilize slower 1 Gigabit Ethernet links (Armbrust, et al., 2009, p. 16).

Distributed denial of service. Armbrust, et al. (2009) characterize Distributed Denial of Service (DDoS) attacks as another risk to using cloud computing services (p. 14). As the industry matures, to the extent that it goes toward a single interface, Douglis (2009) warns that cloud computing systems may become an easier target for attackers to threaten (p. 6). Viruses might be transmitted, or the victims of a hack attack may negatively impact other companies with data located in the same environment (Cloud Security Alliance, 2009, p. 33).

Criminals may also seek to extort payment from cloud computing vendors to prevent the launch of a DDoS attack that typically utilizes botnets (Armbrust, et al., 2009, p. 14). However, Armbrust, et al. (2009) believe such vendors already have DDoS protection as a core competency (p. 15). Kaufman (2009) states that Google and Amazon have the infrastructure to deflect an attack, but not all cloud providers have such an ability (p. 63). At this point in time, ENISA (2009) classifies DDoS as a medium risk (p. 39).

Legal Risks

These include the IT-related risks that are legal in nature, and can also have a negative impact on an organization using cloud computing services. Legal risks include subpoena and e-discovery, changes of jurisdiction, data privacy, and licensing.

Subpoena and e-discovery. If computer systems are confiscated by law enforcement agencies or through civil suits, the centralization of storage and shared tenancy of physical hardware imparts more risk of unwanted data disclosure to cloud computing clients (ENISA, 2009, p. 44). For example, Abadi (2009) notes that U.S. Patriot Act allows the government to, among other things, demand access to data stored on any computer, and if the data is stored by a third party, the data is to be handed over without the knowledge or permission of the company or person using the hosting service (p. 3). Cloud computing service providers are presumably less likely than the customers themselves to go to court on the customers' behalf (Hayes, 2008, p. 11). Armbrust, et al. (2009) state that "some businesses may not like the ability of a country to get access to their data via the court system; for example, a European customer might be concerned about using SaaS in the United States given the USA Patriot Act" (p. 15).

There are also procedural concerns associated with subpoenas and e-discovery. According to Gatewood (2009), the latest update to the U.S. Federal Rules of Civil Procedure in December 2006 places a large burden on organizations preparing for discovery (p. 34). When responding to legal requests, organizations not only have to put together all relevant data within 14 days, but also have the difficulty "of identifying and documenting vendor relationships and data stored with multiple vendors in the cloud" and must "identify the location of relevant information and verify the information has not been and cannot be altered" (Gatewood, 2009, p. 34). Costs associated with electronic discovery activities (usually for civil litigation) are one of the largest controlled costs in business (Cloud Security Alliance, 2009, p. 41).

Changes of jurisdiction. The risks may be high for customer data that are held in multiple jurisdictions (ENISA, 2009, p. 45). For example, Gatewood (2009) notes that although organizations may do business with a vendor down the street, data may be stored far away in a different state or country (p. 33). Furthermore, customer data held in countries that do not respect the rule of law or international agreements could be subject to enforced disclosure or seizure (ENISA, 2009, p. 45). According to Gatewood (2009), "if an organization does business internationally, it has no choice but to consider the international data management and compliance obligations and restrictions that are implicated by a cloud computing model" (p. 35). With different jurisdictions applying their own laws, the issues and risks of data being unintentionally disclosed will grow in complexity as cloud computing is more widely adopted (Cloud Security Alliance, 2009, p. 49). Resolving these security and regulatory concerns could take years (Kaufman, 2009, p. 63). In addition to data being exposed, an organization's reputation and trust with customers could be negatively impacted (ENISA, 2009, p. 45).

Data privacy. Gatewood (2009) states that privacy "is one of the longest standing and most important concerns with cloud computing" (p. 34). In many instances, the obligations of data privacy are the responsibility of senior management (Cloud Security Alliance, 2009, p. 30). In the United States, under Sarbanes-Oxley (SOX), responsibility for an organization's financial data falls on the shoulders of the Chief Executive Officer and Chief Financial Officer (Cloud Security Alliance, p. 30). Under the Gramm Leach Bliley Act (GLBA), responsibility for security safeguards rests with the Board of Directors of financial institutions (Cloud Security Alliance, 2009, p. 30). Under the Health Information Portability and Accountability Act (HIPPA), security safeguards require covered entities to designate a security officer to ensure compliance with the law (Cloud Security Alliance, 2009, p. 30).

Government agencies in both the United States and the European Union have consistently held organizations liable for activities of their subcontractors (Cloud Security Alliance, 2009, p. 31). Cloud computing introduces the risk that information belonging to one organization may be resident in several locations and coexist with another organization's data (Gatewood, 2009, p. 34). The type and location of data may result in a number of legal issues related to data privacy, and violations and may pertain to financial data, intellectual property, health and other information (Gatewood, 2009, pp. 34-35).

Abadi (2009) states that cloud computing vendors give the customer little control over where data is stored and that unless the data is encrypted, it may be accessed by a third party without the customer's knowledge (p. 3). Abadi (2009) argues there are enormous data privacy risks when storing mission-critical transactional data at the lowest granularity (customer data or credit card numbers) on a host that is not trusted and believes "any increase in potential security breaches or privacy violations is typically unacceptable" (p. 4). Data privacy is also a concern when a cloud resource is deleted, especially in the case of multiple tenancy and the reuse of hardware resources (ENISA, 2009, p. 10). Pearson (2009) notes another concern that when vendors offer more flexible cloud services to meet customer needs that the unintended consequence is reduced safety of data (p. 45).

Cachin, et al. (2009) describe that unauthorized access to data can also occur when hackers are not involved (p. 82). Software malfunctions led to recent data breaches at Google Docs and Amazon S3 (Cachin, et al., 2009, p. 82).

Pearson (2009) states that new privacy risks will arise as cloud computing usage increases (p. 46). Although Gatewood (2009) notes that e-mail communications are a natural fit for cloud computing, he raises concerns about the pervasiveness of e-mail and how an organization's records management data that reside in e-mail entail a substantial amount of risk (p. 33). As noted by Davis and Kennedy (2009), law firms themselves are not immune from the risks of cloud computing, and have unique obligations of confidentiality (p. 3). This point is noteworthy, as there are a growing number of legal vendors in the cloud space in the areas of case management and electronic discovery (Davis & Kennedy, 2009, p. 2).

Licensing. There is also a risk that organizations may pay more than desired to license software on systems hosted by cloud computing service providers. ENISA (2009) states that "licensing conditions, such as per-seat agreements, and online licensing checks may be unworkable in a cloud environment" (p. 46). Many service providers "originally relied on open source software in part because the licensing model for commercial software is not a good match" to cloud computing (Armbrust, et al., 2009, p. 19). As a result, open source licensing models will need to remain popular and/or commercial software companies will need to change their licensing structure to better fit cloud computing (Armbrust, et al., 2009, p. 19). Hayes (2008) warns that the open source movement may have a difficult time adapting to the cloud computing model, given the additional technical complexities involved (p. 11).

Mitigation Strategies

Entering into an agreement with a cloud services provider without first establishing business objectives may result in significant problems (Jericho Forum, 2009, p. 7). Gatewood (2009) states that cloud computing is a valuable tool that is not going away, but "it's a tool that needs to be understood and managed" (p. 36). Currently, there are no publicly available standards specific to cloud computing security (ISACA, 2009a, p. 9). As a result, organizations considering cloud services need to exercise in depth due diligence prior to the execution of any agreements (Cloud Security Alliance, 2009, p. 27).

Fortunately, there are mitigation strategies cloud computing customers can follow that may reduce the level of IT-related risks. Each of the following mitigation categories described below (audit controls, policies and procedures, service level agreements, and other forms of governance) addresses risks in each of the three IT-related cloud computing risk categories.

Mitigation strategy #1: Audit controls

When considering a cloud-based initiative or reviewing a solution already in place, Gatewood (2009) recommends determining a vendor's internal audit process, how often it is audited by external agencies, the standards the vendor is held to, and whether or not it is open to being audited for compliance (p. 35). Maintaining compliance with security policies and regulatory requirements can be difficult to demonstrate (Cloud Security Alliance, 2009, p. 44). Gatewood (2009) observes that as vendors rush to develop and present cloud-based solutions, they may fall short on including the necessary records management controls (p. 33). Gatewood (2009) states that "typically the level of control surrounding [an] application and content rises as the solution becomes more narrow and specific to a task or function. More generalized implementations typically have fewer controls compared to highly specialized point solutions" (p. 33).

There are challenges to conducting audits in the cloud environment. Auditing cloud providers can be difficult and expensive (Cloud Security Alliance, 2009, p. 44). Sponsoring an external audit may be appropriate, but a formal adopted framework and properly identified scope is necessary (Cloud Security Alliance, 2009, p. 44). Furthermore, some cloud providers won't allow compliance auditors on site (Rash, 2009, p. 8)

In the future, having management controls in place will be even more important (Gatewood, 2009, p. 36). To be effective in ensuring that security programs are compliant with the relevant rules and regulations, The Cloud Security Alliance (2009) recommends that organizations: (a) know their legal obligations, (b) classify and label their data and systems, (c) conduct an external risk assessment, and (d) conduct due diligence and consider mandating that cloud computing service providers be certified at the appropriate security level (p. 45). Rai and Chukwuma (2009) recommend that audits of cloud computing implementations focus on three elements: the client environment, the provider environment, and the cloud itself, which addresses secure communication between the client and the provider (p. 23).

Mitigation strategy #2: Policies and procedures

ISACA (2009a) states that “businesses must work with legal, security, and assurance professionals to ensure that the appropriate levels of security and privacy are achieved” (p. 10). When reviewing policies and procedures related to cloud computing services, Gatewood (2009) recommends determining if the vendor’s policies and procedures, and related information management approaches, are acceptable; if they are not, the data should either be moved or the vendor should make an auditable change specific to the needs of the client organization (p. 35).

***Service level agreements (SLAs)*.** Given the nature of cloud computing, ENISA (2009) suggests that standard contract clauses with vendors may require additional review (p. 6). A Service Level Agreement is an extremely important item of documentation for both the consumer and the cloud service provider, that if used properly: (1) identifies and defines customer needs, (2) provides a framework for understanding, (3) simplifies complex issues, (4) reduces areas of conflict, (5) encourages dialog in the event of disputes, and (6) eliminates unrealistic expectations (Kandukuri, Paturi, & Rakshit, 2009, p. 517). Security and availability of service are two major issues that are avoided by the use of lenient SLAs (Youseff, et al., 2008, p. 4)

Service Level Agreements are included in the online contracts defining cloud services, but are potentially non-negotiable (Cloud Security Alliance, 2009, p. 26). If customers want to utilize the cloud service, they may have to accept the online terms with conditional clauses and privacy statements that are subject to change without notice (Cloud Security Alliance, 2009, p. 26).

According to the Cloud Security Alliance (2009), “Service Level Agreements tend to focus on availability of services and may not explain service quality, resolution times, critical success factors, key performance indicators, or offer any recourse…” (p. 26). In response, Buyya, et al. (2008) state that customers should demand specific SLAs that cloud computing service providers must meet to satisfy required quality of service (QoS) requirements (p. 3). Important QoS parameters that customers should consider as part of an SLA also include time, cost, reliability, and trust/security (Buyya, et al., 2008, p. 5). Furthermore, Buyya, et al. (2008) believe QoS requirements cannot be static and should be updated over time in concert with changes in business operations (p. 5). In an SLA, the delivery of new or remediated services may not be defined or mentioned (Cloud Security Alliance, 2009, p. 26).

Service level agreements can also be used to mitigate regulatory pressures concerning where data is processed, while specifying strict constraints on the location of cloud computing service provider resources (Buyya, et al., 2008, p. 8).

Mitigation strategy #3: Other forms of governance

There are additional ways in which cloud computing customers can operate within a favorable environment, including establishing and promoting cloud standards and utilizing brokers and markets.

Establish and promote cloud standards. With a standardized cloud application programming interface (API), customers will have an easier time migrating data between service providers (Weinhardt, Anandasivam, Blau, Borissov, Meinl, Michalk, & Stèoßer, 2009, p. 397). Although Weinhardt, et al. (2009) concede that it may be too early for an agreed-upon application programming interface or reference implementation to be established, standardization will be required for cloud computing to be more fully accepted (p. 397).

***Utilize Brokers/Markets*.** Gatewood (2009) doubts that an organization storing information in the cloud is able to comply with all the rules and regulations it faces. He states the "true federation of … controls will need to expand beyond the organization itself and into the data repositories outside of the organization," (p. 36) and believes that the tools by which these controls are managed do not exist today. By engaging in education and developing proactive relationships, it will be more possible to "identify cloud-based initiatives early and raise awareness throughout the organization" (Gatewood, 2009, p. 36).

Buyya, et al. (2008) maintain that cloud computing consumers will benefit by embracing a market system for cloud services that allows participants to locate providers or consumers with suitable offers (p. 7). Although such a system does not exist yet, it could include brokers that buy capacity from cloud computing providers and sub-lease it to consumers (Buyya, et al., 2008, p. 7). Buyya, et al. (2008) contend that a market exchange for cloud computing services can "bridge disparate clouds allowing consumers to choose a provider that suits their requirements by either executing SLAs in advance or by buying capacity on the spot. Providers can use the markets in order to perform effective capacity planning" (p. 7).

Conclusions

Armbrust, et al. (2009) describe cloud computing as an old idea that has recently emerged as a commercial reality (p. 2). Erdogmus (2009) believes the “benefits of scalability, reliability, security, ease of deployment, and ease of management for customers, traded off against worries of trust, privacy, availability, performance, ownership, and supplier persistence, still stand” (p. 5). That is, the economies of scale and flexibility of cloud computing are both a friend and a foe from a security point of view (ENISA, 2009, p. 4).

Armbrust, et.al (2009) believe that service providers will overcome many of the challenges that come with cloud computing (p. 19). Meanwhile, Finnie (2008) recommends that organizations experiment with cloud computing solutions to get up to speed on the technical solutions. However, organizations need to evaluate the current risks and mitigation strategies for safe and successful cloud computing implementations. According to the Cloud Security Alliance (2009), cloud computing requires good governance, risk management, and common sense on the part of organizations (p. 5).

Cloud Computing IT-related Risks: Severity, Probability and Impact

Figure 1 presents an overview of the fourteen key IT-related cloud computing risks, which are fully described in the Review of Literature section of this paper. Each risk is reviewed within three major risk categories as defined by ENISA (2009, p. 23). Although there are additional IT-related cloud computing risks, the risks described in this review are intended to represent the most frequently cited concerns for security practitioners to consider. Three aspects of each risk category are summarized, including the risk level, probability and impact for each risk, as rated by ENISA (2009), except where noted below.

Risk Category	Risk	Risk Level	Probability	Impact
Policy and Organizational	Lock-in	High	High	Medium
	Loss of governance	High	Very High	Very High (IaaS Very High, Saas Low)
	Compliance challenges	High	Very High (depends on PCI, SOX)	High
	Loss of business reputation	Medium	Low	High
	Cloud service termination or failure	Medium	N/A (not rated by ENISA)	Very High
Technical	Availability of service	N/A – Although not listed as a specific risk by ENISA (2009), this risk was frequently cited by other experts, including Armbrust, et al. (2009), which listed Availability of Service as the top obstacle to cloud computing acceptance (p. 14).		
	Resource exhaustion	Medium	Medium (Additional Capacity) Low (Current Capacity)	Low/Medium (Additional Capacity) High (Current Capacity)
	Intercepting data in transit	Medium	Medium	High
	Data transfer bottlenecks	High	Medium	Very High
	Distributed denial of service	Medium	Medium (Customer) Low (Provider)	High (Customer) Very High (Provider)
Legal	Subpoena and e-discovery	High	High	Medium
	Changes of jurisdiction	High	Very High	High
	Data privacy	High	High	High
	Licensing	Medium	Medium	Medium

Figure 1 - Key IT Related Cloud Computing Risks

The policy and organizational cloud computing IT risks described in this study are business-driven, and the collective level of risk, probability, and impact justifies their inclusion. In addition to ENISA’s ratings, Armbrust, et al. (2009) consider lock-in as the number two obstacle to the growth of cloud computing, second only to availability of service (p. 15). The Cloud Security Alliance (2009) cautions that governance – or the loss thereof – at cloud provider facilities transfers risk to customers without recourse or recompense (p. 26). Compliance challenges span different industries and currently bring into question whether or not cloud computing service providers meet the necessary rules and regulations for which customers are held accountable (Gatewood, 2009, p. 36). While the probability of a customer having its reputation damaged by another customer hosted by a cloud computing service provider is low, the resulting potential negative impact is high (ENISA, 2009, p. 29). Although ENISA (2009) does not rate the probability of a cloud computing service company terminating or failing, such providers can and do fail (Cachin, et al., 2009, p. 82).

The technical IT-related risks in this study highlight the potential performance and security problems with computing systems managed by cloud computing service providers. Although ENISA (2009) does not identify availability of service as a specific risk, several experts cited this risk as a major concern, including Armbrust, et al. (2009, p. 14). Resource exhaustion risks are possible, with specific types of database systems particularly vulnerable (Abadi, 2009, p. 2). Data in transit is at risk, and calls for data encryption (Brynko, 2008, p. 23). Given the distributed makeup of cloud computing systems, data transfer bottlenecks may continue to be a risk as long as the price/performance ratio of networking equipment is too high (Armbrust, et al., 2009, p. 16). The stakes are very high with respect to risks associated with distributed denial of service attacks, as Kaufman (2009) states that not all cloud computing service providers have the infrastructure to combat such attacks (p. 63).

The legal-oriented IT-related risks described in this study also have the potential to severely and negatively impact organizations utilizing cloud computing services. Abadi (2009) and Armbrust, et al. (2009) describe the high probability of disclosure subpoena and e-discovery risks that cloud computing customers may face with respect to the U.S. Patriot Act and other laws. The Cloud Security Alliance (2009) warns that changes in jurisdiction as they pertain to cloud computing service providers is complex and may lead to undesired data disclosure due to the proclivities of local jurisdictions applying their own laws (p. 49). According to Gatewood (2009), data privacy risks can result in a number of legal issues and may pertain to financial, health and other types of data (p. 34-35). Licensing risks, which primarily pertain to the pricing of software, may be prevalent in certain conditions and not a good fit in a cloud computing environment (ENISA, 2009, p. 46).

Mitigation Strategies for Cloud Computing IT-related Risks

Although the IT-related risks associated with cloud computing are numerous, there are precautions that organizations can take to mitigate such risks. The Cloud Security Alliance (2009) states that development of cloud services "is in an inevitable evolution of the information society with a need for clearly defined governance and well thought out enterprise risk strategies appropriate for each different cloud offering" (p. 29). Cloud computing IT-related risk mitigation strategies reviewed in this study include: audit controls, policies and procedures, service level agreements, and other forms of governance.

Audit controls ensure that cloud computing service providers maintain compliance with security policies and other regulations (Cloud Security Alliance, 2009, p. 44). Gatewood (2009) recommends that customers determine how their cloud computing service providers audit themselves on behalf of other customers and third parties (p. 35). Cloud computing customers also need to conduct the appropriate level of due diligence to ensure security requirements are properly addressed (Cloud Security Alliance, p. 45).

Gatewood (2009) recommends that cloud computing customers ensure that effective policies and procedures are in place and acceptable regarding the handling and management of information (p. 35). Service level agreements between the service provider and the customer can help mitigate regulatory pressures with respect to where data is processed (Buyya, et al., 2008, p. 8).

Other forms of governance that may mitigate risks include the establishment and promotion of cloud standards, brokers, and markets. Support for a standard application programming interface may give cloud computing customers the ability to migrate to other service provider more easily (Weinhardt, et al., 2009, p. 397). In addition, cloud computing customers may benefit from supporting a market-based system using brokers that provides better choice and flexibility (Buyya, et al., 2008, p. 7).

To take full advantage of the benefits of cloud computing, consumers, businesses, cloud computing service providers, and information security practitioners will continue to "need to collaborate to shine a light on the potential issues and solutions … and to discover those not yet identified" (Cloud Security Alliance, 2009, p. 29).

References

Abadi, D. (2009). Data management in the cloud: Limitations and opportunities. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*. Retrieved from http://cs-www.cs.yale.edu/homes/dna/papers/abadi-cloud-ieee09.pdf

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. (2009). *Above the Clouds: A Berkeley view of cloud computing.* Retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

AWS. (n.d.). What is AWS? Retrieved from http://aws.amazon.com/what-is-aws/

Brandel, M. (2009). Exit strategy. (Cover story). *Computerworld*, *43*(13), 22-26. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=37614378&loginpage=login.asp&site=ehost-live&scope=site

Brynko, B. (2008). Cloud computing: Knowing the ground rules. *Information Today*, *25* (10), 23. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=35126515&loginpage=login.asp&site=ehost-live&scope=site

Busch, C. De Maret, P., Flynn, T. Kellum, R., Le, S., Meyers, B., Saunders, M., White, R., & Palmquist, M. (2005). *Content Analysis.* Writing@CSU. Colorado State University Department of English. Retrieved from http://writing.colostate.edu/guides/research/content/

Buyya, R. , Yeo, C. , & Venugopal, S. (2008). *Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities.* Retrieved from http://www.gridbus.org/papers/hpcc2008_keynote_cloudcomputing.pdf

Cachin, C., Keidar, I., & Shraer, A. (2009). Trusting the cloud. *SIGACT News*, *40*(2), 81-86. doi: http://doi.acm.org/10.1145/1556154.1556173

Cloud Security Alliance. (2009). *Security guidance for critical areas of focus in cloud computing.* Retrieved from http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

Creeger M. (2009). CTO roundtable: Cloud computing. *Communications of the ACM*, *52* (8), 50-56. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=43479961&loginpage=login.asp&site=ehost-live&scope=site

Davis, R., & Kennedy, D. (2009). Working in the cloud. *ABA Journal*, *95*31-32. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=44181137&loginpage=login.asp&site=ehost-live&scope=site

Douglis, F. (2009). Staring at clouds. Internet Computing, *IEEE*, *13(3)*, 4-6. doi: http://doi.ieeecomputersociety.org/10.1109/MIC.2009.70

ENISA. (2009). *Cloud computing: benefits, risks and recommendations for information security*. Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Erdogmus, H. (2009). Cloud Computing: Does nirvana hide behind the nebula? *IEEE Software*, *26*(2), 4-6. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04786942

Finnie, S. (2008, October 6). Peering behind the cloud. *Computerworld*, p. 22. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=34703832&loginpage=Login.asp&site=ehost-live&scope=site

Gatewood, B. (2009). Clouds on the information horizon: How to avoid the storm. *Information Management (15352897)*, *43*(4), 32-36. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=43659227&loginpage=login.asp&site=ehost-live&scope=site

Google Apps. (n.d.). Google introduces new business version of popular hosted applications. Retrieved from http://www.google.com/intl/en/press/pressrel/google_apps.html

Grid Computing. (n.d.). *BusinessDictionary.com* Retrieved from http://www.businessdictionary.com/definition/grid-computing.html

Hayes, B. (2008). Cloud computing. *Communications of the ACM*, *51*(7), 9-11. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=34059107&loginpage=login.asp&site=ehost-live&scope=site

Hewitt, M. (2002). Trent focus for research and development in primary health care: Carrying out a literature review. *Trent Focus Group*. Retrieved from http://ce.uoregon.edu/aim/Capstone07/HewittLitReview.pdf

IDC. (2009a). IDC's new IT cloud services forecast: 2009-2013. Retrieved from http://blogs.idc.com/ie/?p=543

IDC. (2009b). IDC Trademarks. Retrieved from http://www.idc.com/about/trademarks.jsp

ISACA. (2009a). *Cloud Computing: Business benefits with security, governance and assurance perspectives.* Retrieved from http://www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=53044

ISACA. (2009b). ISACA overview and history. Retrieved from http://www.isaca.org/template.cfm?section=About_ISACA

Jericho Forum. (2009). *Cloud cube model: Selecting cloud formations for secure collaboration.* Retrieved from https://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Kandukuri, B., Paturi, V., & Rakshit, A. (2009). *Cloud security issues*. Services Computing, 2009. SCC 2009. IEEE International Conference on Services Computing. doi: http://doi.ieeecomputersociety.org/10.1109/SCC.2009.84

Kaufman, L. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE, 7*(4). doi: http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2009.87

Kim, W. (2009). Cloud computing: Today and tomorrow. *Journal of Object Technology*, *8* (1), 65-72. Retrieved from http://www.jot.fm/issues/issue_2009_01/column4.pdf

Lasica, J. (2009). Identity in the age of cloud computing: The next-generation Internet's impact on business, governance and social interaction. *Washington, D.C: Aspen Institute.* Retrieved from: http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/Identity_in_the_Age_of_Cloud_Computing.pdf

Leavitt, N. (2009). Is cloud computing really ready for prime time? *Computer*, *42* (1), 15-25. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04755149

Leedy, P. & Ormrod, J. (2005). *Practical research*. Upper Saddle River, NJ: Pearson Education.

Literature review. (2007). University of North Carolina. Retrieved from: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Mell, P. & Grance, T. (2009.) The NIST definition of cloud computing. Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

Nelson, M. (2009a). Building an open cloud. *Science*, *324*(5935), 1656-1657. Retrieved from Science Magazine: http://www.sciencemag.org.libproxy.uoregon.edu/cgi/reprint/324/5935/1656.pdf

Nelson, M. (2009b). The cloud, the crowd, and public policy. *Issues in Science & Technology*, *25*(4), 71-76. Retrieved from Academic Search Premier database:

http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=43278297&loginpage=login.asp&site=ehost-live&scope=site

Obenzinger, H. (2005.) *What can a literature review do for me?* Retrieved from http://ce.uoregon.edu/aim/Capstone07/LiteratureReviewHandout.pdf

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *Software engineering challenges of cloud computing, 2009. CLOUD '09.* doi: http://dx.doi.org/10.1109/CLOUD.2009.5071532

Rai, S., & Chukwuma, P. (2009). Security in a cloud. *Internal Auditor, 66*(4), 21-23. Retrieved from Business Source Premier database: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=43703716&loginpage=Login.asp&site=ehost-live&scope=site

Rapple, B. (n.d.). *Writing a literature review.* Retrieved from http://libguides.bc.edu/print_content.php?pid=1194&sid=4957

Rash, W. (2009). Is cloud computing secure? Prove it. *eWeek, 26*(16), 8-10. Retrieved from Academic Search Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=aph&AN=44601453&loginpage=login.asp&site=ehost-live&scope=site

Risk categories. (n.d.). Disaster Recovery Journal. Retrieved from http://www.drj.com/index.php?option=com_glossary&func=view&Itemid=297&catid=35&term=Risk+Categories

Ryan, V. (2008). A place in the cloud. *CFO, 24*(8), 31-35. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=34514238&loginpage=login.asp&site=ehost-live&scope=site

Service Cloud. (n.d.). The service cloud. Retrieved from http://www.salesforce.com/assets/pdf/datasheets/DS_ServiceCloud.pdf

Smith, J. (2009). Fighting physics: A tough battle. *Communications of the ACM*, *52*(7), 60-65. Retrieved from Business Source Premier database: http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=buh&AN=43019152&loginpage=login.asp&site=ehost-live&scope=site

Smith, T. (2009). Scholarly or popular? Retrieved from UO Libraries: http://libweb.uoregon.edu/guides/findarticles/distinguish.html

Soghoian, C. (2009). Caught in the cloud: Privacy, encryption, and government back doors in the Web 2.0 Era. Retrieved from Social Science Research Network: http://ssrn.com/abstract=1421553

Stolvoort, A. (2007). Utility computing. IBM Technology Update. Retrieved from http://www-05.ibm.com/nl/events/presentations/Utility_Computing.pdf

Stoneburner, G., Hayden, C. & Feringa, A. (2004). Engineering principles for information technology security (a baseline for achieving security), Revision A. *NIST Special Publication 800-27 Rev A.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Vaquero, L., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review, 39*(1), 50-55. doi: http://doi.acm.org/10.1145/1496091.1496100

Viega, J. (2009). Cloud computing and the common man. *Computer, 42* (8), 106-108. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=05197438

Wang, L., von Laszewski, G., Kunze, M., & Tao, J. (2008.) Cloud computing: a perspective study. Retrieved from Rochester Institute of Technology Digital Media Library: https://ritdml.rit.edu/dspace/bitstream/1850/7821/1/LWangConfProc11-16-2008.pdf

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., & Stèoßer, J. (2009). Cloud computing - A classification, business models, and research directions. *Business & Information Systems Engineering, 1*(5), 391-399. Retrieved from: http://www.springerlink.com/content/w3h62858jpkw56kh

Youseff, L., Butrico, M., & Da Silva, D. (2008.) Toward a unified ontology of cloud computing. *Grid Computing Environments Workshop, 2008.* Retrieved from http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf

Appendix A

Search Report

Search Engine / Database	Search Terms	Results	Quality of Results
Academic Search Premier	Cloud Computing	720	Fair.
	Cloud Computing Risks	30	Good.
	Cloud Computing Security	77	Good.
	Cloud Computing Security Risks	14	Good.
	Cloud Computing Technical Risks	1	Fair. Only one article, albeit peer reviewed.
	Cloud Computing Business Risks	10	Good.
	Cloud Computing Legal Risks	3	Fair.
	Cloud Computing Risk Mitigation	0	Poor. No results.
	Managed Cloud	81	Fair. There were many unrelated articles.
	Public Cloud	997	Fair. There were many unrelated articles.
	Infrastructure as a Service	61	Good.
	Platform as a Service	77	Good.
	Software as a Service	778	Fair. There were many unrelated articles.
ACM Digital Library	Cloud Computing	3,216	Poor. There were many unrelated articles.
	Cloud Computing Risks	449	Fair.
	Cloud Computing Security	690	Fair.
	Cloud Computing Security Risks	225	Fair.
	Cloud Computing Technical Risks	299	Fair.
	Cloud Computing Business Risks	224	Fair.
	Cloud Computing Legal	105	Fair.

	Risks		
	Cloud Computing Risk Mitigation	25	Fair.
	Managed Cloud	445	Good.
	Public Cloud	872	Fair.
	Infrastructure as a Service	22	Fair.
	Platform as a Service	18	Fair.
	Software as a Service	177	Good. Several cloud-related articles were displayed.
Business Source Premier	Cloud Computing	845	Fair.
	Cloud Computing Risks	50	Good.
	Cloud Computing Security	132	Good.
	Cloud Computing Security Risks	24	Good.
	Cloud Computing Technical Risks	0	Poor.
	Cloud Computing Business Risks	23	Good.
	Cloud Computing Legal Risks	5	Good.
	Cloud Computing Risk Mitigation	0	Poor. No results
	Managed Cloud	64	Fair.
	Public Cloud	626	Fair.
	Infrastructure as a Service	118	Good.
	Platform as a Service	124	Good.
	Software as a Service	1603	Fair.
Google Scholar	Cloud Computing	286000	Fair. Too broad.
	Cloud Computing Risks	25600	Fair. Too broad.
	Cloud Computing Security	32900	Fair. Too broad.
	Cloud Computing Security Risks	19500	Fair. Too broad.
	Cloud Computing Technical Risks	21500	Fair. Too broad.
	Cloud Computing Business Risks		Fair. Too broad.
	Cloud Computing Legal Risks	18900	Fair. Too broad.
	Cloud Computing Risk Mitigation	12000	Fair. Too broad.

	Managed Cloud	179000	Fair. Too broad.
	Public Cloud	433000	Fair. Too broad.
	Infrastructure as a Service	1380000	Fair. Too broad.
	Platform as a Service	1240000	Fair. Too broad.
	Software as a Service	2430000	Fair. Too broad.
IEEE Xplore	Cloud Computing	312	Good.
	Cloud Computing Risks	0	Poor.
	Cloud Computing Security	4	Fair. Did not have access to all articles.
	Cloud Computing Security Risks	0	Poor.
	Cloud Computing Technical Risks	0	Poor.
	Cloud Computing Business Risks	0	Poor.
	Cloud Computing Legal Risks	0	Poor.
	Cloud Computing Risk Mitigation	0	Poor.
	Managed Cloud	0	Poor.
	Public Cloud	7	Poor.
	Infrastructure as a Service	35	Fair.
	Platform as a Service	13	Fair.
	Software as a Service	111	Good.
WorldCat	Cloud Computing	284	Fair.
	Cloud Computing Risks	1	Poor. Only one irrelevant article.
	Cloud Computing Security	19	Fair. Half the results are from books and the electronic journals are largely unavailable.
	Cloud Computing Security Risks	1	Fair.
	Cloud Computing Technical	1	Poor. Only one irrelevant article.

	Cloud Computing Business	1	Poor. Only one irrelevant article.
	Cloud Computing Legal	0	Poor.
	Cloud Computing Risk Mitigation	2	Poor. Only two irrelevant articles.
	Managed Cloud	37	Fair.
	Public Cloud	5961	Poor. Too broad.
	Infrastructure as a Service	169	Poor. Too broad.
	Platform as a Service	45	Fair.
	Software as a Service	413	Fair.