CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

ITAC Brief
Cloud Computing: A Primer

Malik Datardina, CA • Yvon Audette, CGEIT

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

ITAC Brief
Cloud Computing: A Primer

Malik Datardina, CA • Yvon Audette, CGEIT

This publication was originally published by The Canadian Institute of Chartered Accountants in 2011. It has been reissued by Chartered Professional Accountants of Canada.

Author and Project Director

Malik Datardina, CA, CISA

Co-Author

Yvon Audette, CGEIT, KPMG LLP, Toronto

Information Technology Advisory Committee

Chair

Ray Henrickson, CA•IT, CA•CISA, Scotiabank, Toronto

Members

Chris Anderson CA(NZ), CISA, CMC, CISSP, PCI QSA, Grant Thornton, Toronto

Efrim Boritz, FCA, CA•IT/CISA, PhD, University of Waterloo, Toronto

Nancy Y. Cheng, FCA, Office of the Auditor General of Canada, Ottawa

Malik Datardina, CA, CISA, Data Sync Consulting Inc., Mississauga
(consultant for the Committee)

Mario Durigon, CA, KPMG LLP, Toronto

Henry Grunberg, CA•IT, Ernst & Young LLP, Toronto

Andrew Kwong, CA, Deloitte & Touche LLP, Toronto

Carole Le Néal, CISA, CISSP, CIA, Mouvement des caisses Desjardins, Montreal

Richard Livesley, Bank of Montreal, Toronto

Robert G. Parker, FCA, CA•CISA, Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•IT, CA•CISA, CISM, CGEIT, PricewaterhouseCoopers LLP, Winnipeg

CICA Staff

Bryan C. Walker, CA, Director, Guidance and Support

The Information Technology Advisory Committee (ITAC) is part of the Guidance and Support Group at the CICA. Its role is to provide support and advice on IT matters to the CA profession and the business community. For more information about ITAC, please visit us at www.cica.ca/itac.

Library and Archives Canada Cataloguing in Publication

Datardina, Malik

Cloud computing / Malik Datardina and Yvon Audette.

ISBN 978-1-55385-565-1

1. Cloud computing. 2. Business enterprises--Computer networks--Management. 3. Information technology--Management. I. Audette, Yvon, 1968- II. Canadian Institute of Chartered Accountants III. Title.

TK5105.88813.D38 2011 004'.36 C2011-901691-5

INTRODUCTION

Cloud computing has quickly grown from a concept into a mainstream phenomenon. In 2008, Nick Carr published, *The Big Switch*, which was one of the first publications to explore the impact of "utility computing" — the ability to pay for computing resources by the meter. Within three years, the phenomenon has entered into the mainstream not only through Microsoft's print and TV ads,[1] but also Amazon's hosting (and then "unhosting") of Wikileaks from its cloud service offering: Amazon Web Services.

In this ITAC Brief, we explore some key areas within the topic of cloud computing. We begin with the generally accepted definition of cloud computing, identify its value proposition, explore the audit and control implications of cloud, and close off with a list of further cloud computing resources.

1 An example of such an ad is available here: http://www.youtube.com/watch?v=-HRrbLA7rss&feature=relmfu

WHAT IS CLOUD COMPUTING?

Although there is no official definition of cloud computing, the *NIST Definition of Cloud Computing* has more or less become the *de facto* standard. As discussed in greater detail below, the definition includes:

1. Cloud service models,
2. Characteristics of cloud computing, and
3. Cloud deployment models.

1. Cloud Service Models

The cloud service models are commonly referred to as the "SPI Model," which refers to the key "as-a-Service" models of cloud service providers including, Software as-a-Service, Platform-as-a-Service, and Infrastructure as-a-Service.[2]

Software-as-a-Service (SaaS)

NIST defines SaaS providers as those companies that allow the customer to access "the provider's applications running on a Cloud infrastructure". These cloud services are consumed right through the browser. The most prominent example within this category is Salesforce.com. They have been in the business of cloud-served CRM for over 10 years. Other companies include Google Apps,[3] Intuit,[4] and many others. For additional examples, see the section on the *Value of Cloud Computing*.

Platform-as-a-Service (PaaS)

Cloud service providers in this category take care of the underlying infrastructure, but provide the tools required to build applications.[5] Depending on the PaaS provider, users have the ability to deliver applications directly to consumers via the web or deliver applications only to employees within the enterprise. Two examples of PaaS providers include Google App Engine (which allows for development in the Python or Java programming languages) and Microsoft Windows Azure (which supports the .NET development framework).

Some PaaS vendors will provide development for another Software-as-a-Service (SaaS) offering. For example, Bungee Labs built an inventory management application that seamlessly integrates with Salesforce.com's CRM application. SaaS companies *themselves* may offer PaaS services as well. For example, companies such as Salesforce and Intuit, offer PaaS (force.com and Intuit Partner Platform, respectively) to programmers to build apps to serve the customers of their respective SaaS offerings.

---

2 For a more expansive list, see David S. Linthicum, *Cloud Computing and SOA Convergence in your Enterprise* (Boston: Addison-Wesley Professional, 2009).

3 www.google.com/apps/intl/en/business/index.html

4 http://www.quickbooksonline.intuit.com

5 For definitions used, see: http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

Infrastructure-as-a-Service (IaaS)

As defined by NIST, IaaS companies "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".[6] Amazon Web Services (AWS) is by far the leading provider of IaaS. The company offers Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Virtual Private Cloud (VPC), Amazon SimpleDB, and other cloud service offerings. Through the EC2 service, customers can deploy "Amazon Machine Images" (AMIs), which consists of a "pre-configured operating system and virtual application software which is used to create a virtual machine".[7] Through these virtual instances, companies can host their internal application, as well as a website accessible to the public at large. Arguably, the most famous example of the latter is Wikileaks's website, which was hosted by Amazon for a short period in 2010. Additional examples of IaaS providers include, Rackspace, GoGrid, and Storm On Demand Cloud Hosting.

Other players within the IaaS space are companies, such as Rightscale, which offer cloud management services. Rightscale provides "ServerTemplates"[8] that can be seamlessly deployed amongst multiple cloud providers (e.g., AWS, Rackspace, etc.).

2. Characteristics of Cloud

In addition to defining specific cloud models, NIST also identifies the following key characteristics of cloud:

- *"Broad network access"*: As indicated by the term "cloud", the processing happens at the cloud service provider's location. The user is, therefore, able to access the application through a browser or other "thin or thick client platforms" located on the users' desktop, smartphone, tablet, or other computing device.
- *"Rapid elasticity" and "on-demand self-service"*: Cloud computing is able to scale up and down on demand. As the company's demand for computing resources increase, the cloud service provider is able to provision the resources in a fully automated manner and does not require manual intervention from the provider.
- *"Measured service" and pay-as-you-go pricing*: NIST points out that the services should delivered in a manner that is transparent to the customer. From a pricing perspective, this means that cloud services are sold based on usage instead of requiring an upfront commitment in terms of hardware, software or a specific amount of computing resources. Clouds allow the customer to pay for only what they use, similar to the way utilities are paid for (hence the term "utility computing"). The unit of usage varies from vendor to vendor. For example, Amazon Web Services are sold by the hour, whereas Google Apps' pricing is based on the number of users.

---

6 For definitions used see: http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

7 Taken from Amazon, see: http://aws.amazon.com/amis

8 For the differences between Rightscale's ServerTemplate and machine images (e.g., offered by Amazon or other IaaS providers), see www.rightscale.com/products/advantages/servertemplates-vs-machine-images.php

- *"Resource pooling"*: Cloud computing vendors are able to serve multiple customers with pooled computing resources that use "a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand". One of the consequences of this model is that the exact physical location of the computing resource may not be known, but can be pinpointed to "a higher level of abstraction (e.g., country, state, or datacenter)".

These characteristics illustrate how the cloud computing model of outsourced IT is more efficient than traditional IT outsourcing models. Using manual labour to provision additional resources required by the customer is more expensive than using the cloud providers, such as Amazon, which provision such resources in an automated fashion. Similar cost advantages are also gained by using pooled resources instead of deploying a single physical server for each individual customer.

3. Cloud Deployment Models

The cloud deployment models identified by NIST are differentiated based on the level of control/ownership the customer or group of customers have over the underlying cloud infrastructure, as well as where the cloud is hosted. The model also infers the level of comingling of data, i.e., multiple customers sharing the pooled computing resources. These include:

- *Public Cloud*: The cloud infrastructure is hosted by an external provider, such as Salesforce (SaaS), Microsoft Azure (PaaS), or Amazon Web Services (IaaS). The underlying technologies are controlled by the vendor and the customer's data is comingled with the data of other customers who are also purchasing services from the vendor.
- *Private Cloud*: No comingling occurs within this model as the cloud infrastructure is either hosted internally or hosted with an external provider who manages the cloud exclusively for that customer.
- *Community Cloud*: The cloud infrastructure is controlled by multiple customers who come together to build a cloud that meets their particular needs, especially from a control, security or compliance perspective. For example, Mount Sinai Hospital and 14 other local Toronto hospitals are working to build a community cloud to access a fetal ultrasound application and store related patient data.[9]
- *Hybrid Cloud*: NIST defines this model as cloud infrastructure that is "a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability".

9 Laura Smith, "A health care community cloud takes shape": http://searchcio.techtarget.com/news/2240026119/A-health-care-community-cloud-takes-shape (December 21, 2010).

Are Private Clouds Really Clouds and Are They Inherently More Secure?

The private cloud model initially was the one that raised the most controversy. Unlike public clouds, this model does not have the cost advantage of utilizing resources on demand. Also, the underlying hardware and software infrastructure must be purchased in advance. However, its chief advantage over the public cloud model is that it remains under the exclusive control of the customer. Although this does not protect the computing environment from traditional security risks of malware, hacking, and the like, it ensures that the data is *physically* segregated from other entities. This advantage is important as a survey sponsored by Novell found that 91% of respondents were concerned about the security issues associated with the public cloud — with 50% identifying security as the key obstacle to adopting cloud.

Another perspective is that private clouds are the start of a journey that could lead to public cloud use. The same Novell survey found that 89% saw that private clouds as "the next logical step for organizations already implementing virtualization".[10] Jim Ebzery, a Novell executive, noted that companies are starting with private cloud with the aim of moving to public clouds. This view is also shared by Gartner analyst Thomas Bittman, who sees private cloud as a possible "stepping stone" to the public cloud.[11]

With that being said, private clouds are not automatically more secure than public clouds. As George Reese[12] points out,

> ...[the] key to securely deploying a public cloud infrastructure is transparency. That statement should not be confused with the fallacy that transparency is security. Transparency is a necessary element to assessing the risks associated with any infrastructure. It can also help you establish compensating controls to address less than ideal facts about the target infrastructure.... Transparency, however, does not magically render any environment secure.[13]

---

10 "Novell survey reveals widespread enterprise adoption of private clouds", www.informationweek.in/Cloud_Computing/10-10-05/Novell_survey_reveals_widespread_enterprise_adoption_of_private_clouds.aspx (October 5, 2010).

11 http://blogs.gartner.com/thomas_bittman/2009/10/22/talk-of-clouds-and-virtualization-in-orlando/

12 George Reese, *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud* (Sebastopol: O'Reilly, April 3, 2009), included in the further reading lists below.

13 George Reese, "The Delusion of Private Cloud Security", http://broadcast.oreilly.com/2010/08/the-delusion-of-private-cloud-security.html (August 7, 2010).

In order to be more secure than the public cloud alternative, companies must retain the necessary talent to secure the underlying cloud infrastructure. Reese also notes that “IT shops in general for low-tech companies are going to be less competent as a group in IT security than their public cloud IT counterparts”. Therefore, private clouds are not inherently more secure, but do give direct control of the underlying cloud infrastructure to the company deploying the private cloud.

VALUE OF CLOUD COMPUTING

In reality there is nothing *technologically* new about cloud computing: virtualization, multi-tenancy, and other cloud-enabling technologies have been around for a long period of time. Furthermore, public clouds, such as Salesforce.com, Netsuite, Hotmail and others, have been in the market since at least the late 1990s. However, what is new is that cloud offers a new way to consume IT: computer resources can be rented. From this seemingly insignificant shift, many advantages are available, including:

Ability to Fund IT Projects from Operational Expenditures

With the ability to rent computer resources, companies have the ability to shift the IT spend from capital expenditures ("CapEx") to operational expenditures ("OpEx"). For start-ups, this is an especially important advantage: they can conserve their capital by renting the required resources. All companies who want to pursue IT projects, but have difficulty obtaining capital up front, can also leverage cloud computing from this perspective.

Pay-As-You-Go Approach to Technology

Prior to cloud computing, companies needed to obtain millions of dollars to build data centres to host and deliver their applications. Companies that were "web only" or delivered content through the web (e.g., on-demand video) had the additional challenge of buying the right amount of capacity: too much spend meant depleting one's capital without capturing revenue and too little meant a poor user experience that would turnoff customers. With cloud, such companies pay exactly for the resources they use. For a start-up, this allows a better matching of cash outflows (on technology) with use of their services. Companies that opt for a hybrid cloud deployment model can use private clouds to deal with expected levels of resource usage, but move processing to the public cloud to deal with unexpected spikes in demand.

Maintenance, Patching and Upgrades Can Be Delivered as Part of the SaaS Delivery

With SaaS, patching, upgrades and other maintenance fees are included as part of the subscription fee. For example, Workday[14] automatically upgrades its application every four months. IaaS have a partial advantage in this area. The actual day-to-day upkeep of the systems belongs to the IaaS provider, but "much of the software management costs may remain—upgrades, applying patches, and so on".[15] For PaaS companies, the patching of the underlying server belongs to the provider, but the patching of the application belongs to the user (i.e., the developer of the application).[16]

More Efficient Use of Computing Resources

The advantages cited above are usually obtained through the use of public clouds. However, both public and private clouds enjoy a more efficient allocation of computing resources. Through deployments of private clouds, companies can consolidate resources. For example, with virtualization multiple servers can be hosted in a single

---

14 www.workday.com; see section in this article, "Are clouds less expensive?" for more on what Workday offers.

15 Michael Armburst, et al., "Above the Clouds: A Berkley View of Cloud Computing" (February 10, 2009), p. 13, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

16 Tim Mather et al., "Cloud Security and Privacy" (Cambridge: O'Reilly Media Inc, 2009), p. 131.

physical environment. Also, through automated self-provisioning of resources, users can roll out a virtual server within minutes — not having to wait months for internal IT to buy, patch and install the server. Public clouds, as discussed above, allow companies to scale up and down their resources to match the level of traffic or volume they are experiencing.

Some illustrative examples that highlight the above advantages include:

- *Flightcaster*[17] a start-up company that offers a mobile application that predicts flight delays. The program incorporates data from the FAA, airlines, weather data, and uses machine learning and inference techniques, or "big crunch analytics" used by the likes of Facebook and Google, to make its predictions. Although this is technical, it highlights the fact the company's business model depends on high-powered IT resources. According to Bradford Cross, a senior architect at Flightcaster, only two people (including himself) built all the intelligence and scalable analytics. He stated that this endeavour would have been impossible two years ago, as it is dependent on procuring IT resources from the cloud. It would have cost millions of dollars to build the underlying fault tolerant systems and Flightcaster would have had to hire and pay the staff to maintain it.[18]
- *Animoto*[19] is another start-up that leverages cloud computing. The company offers has an application that creates videos by combining photos uploaded by users with music using a special program to create a synchronized experience. The company used Rightscale to manage their cloud computing infrastructure. With this infrastructure in place, they were able to seamlessly expand their environment from serving 25,000 users (approx. 50 servers) to serving 250,000 users (approx. 3,500 servers) *within three days*.[20]
- *The Washington Post* used cloud computing to convert 17,481 non-searchable PDF pages into machine readable text. Using Amazon's EC2 service, the company turned on 200 server instances and completed the job within 26 hours. The cost: $144.62.[21] The New York Times used the cloud in a similar manner: they converted 11 million articles, or 4 terabytes worth of TIFF files, into easier-to-distribute pdf files. The cost for the job was $240 and was completed within 24 hours over 100 servers. Derek Gottfrid, the software programmer from the NY Times who ran the job, admitted that the company would have likely abandoned the job due to either cost concerns or resource constraints.[22]

Are Clouds Less Expensive?

Some see clouds as the less expensive option in comparison to the on-premise application. For example, Workday delivers enterprise-focused software (HRM, payroll, and financial management) through a Software-as-a-Service model. According to the co-CEO of the company, Aneel Bhusri, Workday is a better alternative because it

---

17 www.flightcaster.com

18 John M. Willis, "Haddop and Cascading With Flightcaster", www.johnmwillis.com/ec2/cloud-cafe-38-haddop-and-cascasding-with-flightcaster (August 19, 2009).

19 www.animoto.com/

20 "Animoto's Facebook scale-up", http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/ (April 23, 2008).

21 http://aws.amazon.com/solutions/case-studies/washington-post/

22 Nicholas Carr, "The new economics of computing", www.roughtype.com/archives/2008/11/the_new_economi.php, (November 5, 2008).

is more cost effective and can be implemented in a shorter period of time. According to Bhusri, Sony Pictures Entertainment chose Workday because it was "one-half the time at one-third the cost". This is in spite of the fact that the Sony Pictures Entertainment *had already paid for the software licences for SAP HR*.[23]

Although this is a compelling case to demonstrate that cloud is more cost-effective, there are many factors to consider when evaluating the cost-savings from cloud. This includes:

- *Identifying the business case*: Prior to examining cost issues, the company must determine the actual business case for using cloud. In certain instances, the benefits are overwhelming, as was the case with the Washington Post and the New York Times. In other instances, executives need to sit with their CIOs and determine how the advantages of cloud discussed above will enhance their ability to better serve their customers and deliver value to their stakeholders. Additionally, concerns such as privacy, security, and other compliance requirements may be insurmountable obstacles to cloud. In such cases, cost savings are irrelevant.
- *Bandwidth*: In order to determine the cost of bandwidth, it is required to estimate the amount of data that will be transferred from the cloud provider to the customer. Different vendors charge different amounts. For example, Microsoft charges 10 cents to upload data and 15 cents to download.[24] According to Bernard Golden, an author on virtualization and a cloud computing consultant, this cost was found to be the greatest source of variability within the estimation process.[25] Also, the bandwidth provided by the ISP may be insufficient to handle the data requirements of the application.[26]
- *Integration*: Companies also need to investigate the effort and resources required to integrate the new cloud application, both with on-premise software and other applications residing in the cloud. This can be especially difficult with legacy applications. For example, one company had to build its own interface to integrate a cloud application with on-premise software that ran on an AS/400 server.[27]
- *Spot price versus wholesale price*: As pointed out by Frank Gillett of Forrester, consuming IT through the cloud is the equivalent of buying commodities on the "spot market" — it is more expensive to pay "per hour, than if you make an upfront commitment".[28] To take this further, when a company reaches a certain size it is likely that it is more cost effective to host one's own applications and required infrastructure instead of renting from an IaaS provider.

---

23 Dana Gardner, "Move to Cloud Increasingly Requires Adoption of Modern Middleware to Support PaaS and Dynamic Workloads", http://briefingsdirect.blogspot.com/2009/10/executive-interview-workdays-aneel.html (October 14, 2009).

24 Allan Leinwand, "The Hidden Cost of the Cloud: Bandwidth Charges" (July 17, 2009).http://gigaom.com/2009/07/17/the-hidden-cost-of-the-cloud-bandwidth-charges/

25 Bernard Golden, "The Skinny Straw: Cloud Computing's Bottleneck and How to Address It",www.cio.com/article/499137/The_Skinny_Straw_Cloud_Computing_s_Bottleneck_and_How_to_Address_It (August 6, 2009).

26 *Ibid*.

27 Kim S. Nash, "Cloud Computing: What CIOs Need to Know About Integration" www.cio.com/article/593811/Cloud_Computing_What_CIOs_Need_to_Know_About_Integration (May 15, 2010).

28 Dana Gardner, "Dana Gardner Interviews Forrester's Frank Gillett on Future of Mission-Critical Cloud Computing", http://briefingsdirect.blogspot.com/2009/06/dana-gardner-interviews-forresters.html,(June 01, 2009).

RISKS AND CHALLENGES IN THE CLOUD

It is important to point out that cloud computing is in its early stages of adoptions. Around the time that this ITAC Brief was published, cloud computing was at the "Peak of Inflated Expectations" of Gartner's Hype Cycle and entering into the "Trough of Disillusionment".[29] Consequently, there are many risks and challenges that need to be addressed.

Governance

As illustrated with the Washington Post's and New York Times' "cloud use case", an employee can purchase cloud computing services with a credit card. This opens up the risk of "rogue clouds": the risk that departments will purchase cloud computing services through the "expense report process" — circumventing the regular *controlled* IT procurement process.[30] This will not only result in data being exposed to cloud-oriented security risks, but can also face cost overruns.[31] With respect to the latter, the risk is similar to switching from an "all-included-utilities" rental apartment to a "hydro-is-extra" arrangement: the first utilities bill will likely be high as the user is not accustomed to being billed for the resources used. Furthermore, if the application becomes significant to the overall operations of the organization, IT may be faced with the challenge of integrating the cloud service into the rest of on-premise computing environment. However, the key implication of this risk is that companies may already be on the cloud without knowing it.

As with traditional outsourcing projects, the issue of vendor viability is also a concern. Digital Railroad, a cloud-based service for storing and selling photos on behalf of professional photographers, suddenly shut down. Another related risk is that the vendor, although viable, may be acquired. This will leave the customer at the mercy of the acquiring company, which could shut down the service that the customer is using. Both these issues illustrate that, although the cloud is a new way of procuring technology, companies still need to have a back-up and availability strategies to ensure that their data is available off the cloud.

The other challenge with respect to vendor viability is to understand who the vendor relies upon. For example, Amazon's S3 cloud storage service outage prevented Twitter from serving the avatar images of their users.[32] In other words, when companies rely on Twitter they are also relying on Amazon.

---

29 "Gartner's 2010 Hype Cycle Special Report Evaluates Maturity of 1,800 Technologies", www.gartner.com/it/page.jsp?id=1447613 (October 7, 2010).

30 Chris Murphy, "Get Ready For Rogue Clouds", www.informationweek.com/blog/main/archives/2008/12/get_ready_for_r.html (December 9, 2008).

31 Daryl C. Plummer, "Cloud Elasticity Could Make You Go Broke", http://blogs.gartner.com/daryl_plummer/2009/ 03/11/cloud-elasticity-could-make-you-go-broke/ (March 11, 2009).

32 Jon Brodkin, "More outages hit Amazon's S3 storage service", www.computerworlduk.com/news/security/10155/more-outages-hit-amazons-s3-storage-service/ (July 22, 2008).

Security

As noted in the Novell survey, the most prominent concern with cloud computing is security. Once the information is put on a public cloud — outside of the company's firewall — there is a risk that it could be accessed by unauthorized users. This stems from the fact that cloud computing uses multi-tenancy, where data from multiple customers comingle within the cloud provider's application. An example of such a risk to an IaaS provider (e.g., AWS) is "side-channel-attacks", where a potential malicious user can gain access to an organization's computer resources.[33] Attackers achieve this by identifying the location of the victim's instance, gaining "co-residency" with the intended victim, and exploiting information released by the virtual machine to attack the intended victim.[34] The other risk with multi-tenancy is that the cloud provider may accidentally divulge the information to the wrong user. For example, Google Docs had a security flaw where it accidentally shared documents with anyone who had been granted access to the document in the past.[35]

Security risks also emerge from the use of virtualization, which many cloud deployments depend on. According to Gartner, "60 percent of virtualized servers will be less secure than the physical servers they replace".[36] Some of these issues are due to technical reason, but the cited Gartner's press release also points out a lack of organizational controls, such as not involving information security personnel in virtualization projects and inadequate attention to preserving segregation of duties.

Covering all the security issues associated with cloud computing goes well beyond the scope of this publication. However, there are many resources available for further reading. See the section below "Security Guidance and Standards for Cloud" as well as "Cloud Computing: Further Resources".

---

33 Thomas Ristenpart et al., "Hey, You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds", Proceedings of the ACM Conference on Computer and Communications Security (CCS) (Chicago, IL, November 2009), http://cseweb.ucsd.edu/~savage/papers/CCS09.pdf

34 *Ibid*.

35 Jason Kincaid, "Google Privacy Blunder Shares Your Docs Without Permission", http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/(March 7, 2009).

36 "Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than the Physical Servers They Replace Through 2012", www.gartner.com/it/page.jsp?id=1322414 (March 15, 2010).

Audit

Both internal and external auditors will begin to face the challenges of public cloud computing as it gets integrated into processes over which auditors are required to provide assurance. As cloud service providers are independent, it is necessary either to be able to audit their facilities or to obtain a report on controls. From a proactive standpoint, auditors should work with IT or other departments using public clouds to ensure that the agreements they have with public cloud providers either contain an audit clause or include a provision to provide a report on controls, such as a SysTrust report. Although this is best practice, auditors should be aware that large companies, such as Amazon, are not likely to customize their offering to meet the needs of the user. For example, it is speculated that Eli Lilly abandoned further expansion of its use of AWS because the "two sides could not agree to terms over legal liability and indemnification issues should there be outages or data breaches that affect Eli Lilly's business."[37]

One of the more cloud-specific audit challenges is the problem of disappearing evidence. The ability to use computing on an as-needed basis, similar to a utility, is a key benefit of cloud computing. Users can simply turn it off when it is not needed. As identified by KPMG's Shahed Latif,[38] when the customer shuts off the service — the audit evidence that resides on the virtual server is gone "once the tap is shut off".[39]

When planning the audit, it is also necessary to determine the number of cloud service providers that are actually involved in the application that is used by the company or client. As discussed in the *Cloud Services Model* section above, SaaS companies make it possible for *independent* developers to build apps that are sold to their SaaS customers. As these apps can be seamlessly integrated with the SaaS application, the end-user may not know that they are in fact not only dealing with Salesforce.com or Intuit, but a completely independent party. In such situations where the SaaS provider offers a report on controls, auditors will need to assess what additional work needs to be performed to gain comfort over the processing done by the application built by the third-party developer.

---

37 Joe Maitland, "Eli Lilly ends talks to expand Amazon Web Services use", http://searchcloudcomputing.techtarget.com/news/1517662/Eli-Lilly-ends-talks-to-expand-Amazon-Web-Services-use (August 2, 2010).

38 Shahed Latif is a co-author of *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*; see Books section below for more information about the book.

39 OreillyMedia, "O'Reilly Webcast — Cloud Security & Privacy", www.youtube.com/watch?v=tF2EV5olkbQ (September 30, 2009).

Audit plans must also determine where the responsibility of the provider ends and where it begins for the customer. For example, Salesforce.com provides access to its Trust Services report, which opines on Security, Confidentiality, and Availability.[40] However, ensuring that terminated employees no longer have access to such a SaaS application is the responsibility of the customer.

As with the security section, the full range of audit issues go beyond the scope of this Brief. However, the Information Systems Audit and Control Association (ISACA) has been active in the area of cloud computing and has a number of articles and publications to assist assurance practitioners with cloud specific issues:[41]

- Cloud Computing Management Audit/Assurance Program
- Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives
- IT Audits of Cloud and SaaS
- Making Sure You Really Are Walking on Cloud Nine.

The American Institute of Certificated Public Accountants (AICPA) does not have cloud-specific resources but, at the time of writing this Brief, AICPA was in the process of unveiling guidance for the new Service Organization Control Reports (which will replace the SAS 70 reports):[42]

- SOC 1 Report — Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
- SOC 2 Report — Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- SOC 3 Report — Trust Services Report for Service Organizations.

40 See http://trust.salesforce.com/trust/assets/pdf/Misc_SysTrust.pdf

41 Please note these publications may require membership access to ISACA; for more information, see, www.isaca.org

42 For more information, see www.aicpa.org

CLOUD-AS-A-CONTROL

One of the interesting aspects of cloud is applying the economics of cloud to the concept of control. As discussed above, cloud allows computing resources to be rented on-demand. In certain cases, this advantage of cloud can alter the "cost-benefit" analysis of controls; where previously control could not be pursued due to exorbitant costs. The list below is not by any means exhaustive, but gives some idea of this impact of cloud on controls.

System Testing in the Cloud

With the ability to use systems on demand, companies no longer need to sink thousands of dollars to create a test environment to mirror production. Instead they can rent an environment on as-need basis from an IaaS provider like Amazon or use the services from companies such as Soasta.[43] From a control perspective, benefit of having a proper test environment can now be realized due to the economics of cloud computing. That being said, proper controls still need be in place when using such services. For example, production data should not be used on cloud-hosted test environments; just as it should not be used on an internally-hosted test environment.

Disaster Recovery (DR) and Business Continuity Planning (BCP) in the Cloud

As with system testing, cloud alters the cost-benefit calculation of building an alternative processing facility. As David Linthicum[44] points out, with a cloud-hosted alternative processing site no "data center investment is required, or hardware and software costs incurred. What's more, you can turn it on when needed, and they only bill you for the resources you actually leverage. This opens opportunities for businesses that typically could not afford a back-up center. The dollar estimate is that the cost is about a fourth that of traditional backup sites, mostly from ongoing operational savings."[45] The article also points out that, from a DR perspective, employees will have an easier time accessing the resources as they only need to get to a network connection, instead of an actual alternate processing facility.

Companies interested in backing up specific applications can identify specific SaaS players, depending on the application. For example, Google offers Google Message Continuity service, which provides a cloud-based back-up of the company's on-premise Microsoft Exchange Server. Using this service, users can switch to Gmail whenever their internal email server is unavailable.[46]

---

43 www.soasta.com

44 David Linthicum is considered a leading expert on cloud computing. He is invited to cloud conferences to deliver keynote speeches, has authored on the topic, and has a podcast. See the resources section for more information about him. His blog is at www.infoworld.com/blogs/david-linthicum

45 David Linthicum, "Leveraging Cloud Computing for Business Continuity", Disaster Recovery Journal (Summer 2010), pp. 28, 30, www.drjournal-digital.com/drjournal/2010Summer?pg=30#pg30

46 "Bringing Gmail's reliability to Microsoft® Exchange", http://googleenterprise.blogspot.com/2010/12/bringing-gmails-reliability-to.html, (December 09, 2010)

The Other "SaaS": Security-as-a-Service

Unlike system testing and DR through the cloud, security-as-a-service offer much more specific solutions that solve specific security problems. The most common application of such security services is anti-spam.[47] A subsidiary of Google (Postini) offers a service that protects against spam/viruses and also provides encryption of email.[48] Other security-as-a-service offerings exist, such as Identity Management-as-a-Service. However, evaluating their cost-benefit is similar to outsourcing other applications to the cloud vendors rather than offering compelling benefit-to-cost assessments that are often found when moving system testing or DR to the cloud.

The implication of cloud-as-a-control for management is that they can make their resources go further and build a better control environment. For auditors, controls that have been previously been ignored due to cost constraints need a second look to see whether cloud alters the economics enough to make the implementation of such controls feasible.

47 Andreas M. Antonopoulos, "Security-as-a-service growing", www.networkworld.com/columnists/2010/083110antonopoulos.html (August 31, 2010).

48 www.google.com/postini/email.html

SECURITY GUIDANCE AND STANDARDS FOR CLOUD

Although cloud computing is still in its early stages, a number of organizations provide guidance and standards. Some of the organizations include:

- **Jericho Forum** has published the "Cloud Cube";[49] which assists in identifying the best cloud deployment model for the user.
- **European Network and Information Security Agency (ENISA)** published a 125-page document entitled "Cloud Computing Risk Assessment",[50] which looks at both the security benefits and security risks of Cloud. The security risks are broken into 24 cloud-specific risks and 11 non-cloud security risks.
- **Cloud Security Alliance (CSA)** has published Version 2.1 of their guidance document, which breaks down the security issues into 13 domains. The CSA also has published "Top Threats to Cloud Computing" as well as the "Cloud Controls Matrix".[51]
- **Open Cloud Manifesto**[52] is an initiative to make cloud computing more open and interoperable. The initiative was started by Reuven Cohen (President of Enomaly, a cloud computing company, based out of Toronto), IBM and others. However, the initiative does ***not*** have support from Amazon, Google, Salesforce.com, or Microsoft.
- **Cloudaudit.org**[53] is an initiative led by Chris Hoff.[54] As per the website,[55] the "goal of CloudAudit (codename: A6) is to provide a common interface and namespace that allows Cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance (A6) of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology".

---

49 www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

50 www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

51 For these and additional research published by the CSA, see: www.cloudsecurityalliance.org/Research.html

52 www.opencloudmanifesto.org

53 www.cloudaudit.org

54 Chris Hoff is the Director of Cloud & Virtualization Solutions of the Security Technology Business Unit at Cisco Systems, and is one of the founders of the Cloud Security Alliance and the founder of the CloudAudit project. His blog is at www.rationalsurvivability.com/blog/

55 www.cloudaudit.org/page3/page3.html

CLOUD COMPUTING: FURTHER RESOURCES

Background Information on Cloud Computing and Its Prospects

NIST Resources on the Cloud:[56] As discussed in Section A, the documentation compiled by NIST has become the *de facto* standard in defining cloud computing. Most articles, books, podcasts and other publications leverage this model of cloud computing when discussing their perspective on the issue.

Computing in the Cloud: What, How and Why:[57] The actual presentation, by Edward W. Felten, starts just after the 6-minute point. The video provides a good history of computing and demonstrates how the shift to Cloud is "the pendulum swinging back" to the older paradigm of time-sharing on mainframes.

Era of the Cloud: Nicholas Carr (Google Atmosphere Session 2):[58] Nicholas makes the case that computing is going the way of electricity. Originally, companies used to generate their own electricity, but then moved to grid electricity as they found it made business sense. He argues that a similar trend is now occurring in technology; companies are finding cost efficiencies by moving their data centers to the cloud.

Above the Clouds: A Berkeley View of Cloud Computing:[59] published by UC Berkley explores the actual costs associated with deploying computing resources in the Cloud. The publication provides detailed costing information associated with their use of Amazon's Cloud computing services.

Podcasts

Cloud Computing Podcast[60] with David Linthicum (the author of the book "Cloud Computing and SOA Convergence in Your Enterprise"). The podcast is still "on air" and produces shows on a weekly basis. The series looks at news and trends and talks to high profile personalities in the industry. It covers the issues from a business perspective and is not pro-cloud or anti-cloud, but advocates cloud as an architectural pattern that will provide greater value to the business.

---

56 http://csrc.nist.gov/groups/SNS/cloud-computing

57 www.youtube.com/watch?v=MXoMWC6xPUw

58 www.youtube.com/watch?v=BYP3uMOobqk

59 http://d1smfj0g31qzek.cloudfront.net/abovetheclouds.pdf

60 www.cloudcomputingpodcast.libsyn.com/

The Cloud Computing Show[61] with Gary Orenstein has interviews with personalities in the field. It also has panels that examine issues and trends in the world of cloud. The show is more technical in nature.

Cloud Café[62] with John M. Willis, who was a consultant in cloud computing, until recently when he became the VP of Training & Services at Opscode.[63] Shows can be highly technical, but offer great insights regarding cloud computing. At the time of writing this Brief, no episodes had been published since the end of 2009.

IT Management and Cloud Podcast[64] with Michael Cote and John M. Willis. The show discusses industry trends and takes a more humorous approach to the topic. Looks at the topic from an operational perspective and also examines industry trends. The show is more technical. At the time of writing this Brief, no episodes had been published since October 2010.

Books

Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide
Author: David S. Linthicum
Publication Date: October 9, 2009 (Boston: Addison-Wesley Professional)

Summary: Provides a business-based perspective on the cloud. Building on the NIST SPI model, the book provides other types of "as-a-Service" offerings, such as Information-as-a-Service, Integration-as-a-Service, and others. Also, an entire chapter is dedicated to building the business case for clouds and exploring the issues. There is also a discussion on the connection between cloud computing and service-oriented architecture.

Cloud Application Architectures: Building Applications and Infrastructure in the Cloud
Author: George Reese
Publication Date: April 3, 2009 (Sebastopol: O'Reilly)

Summary: Although directed to technical specialists, the book provides insights on how cloud contrasts to on-premise computing from an economics perspective. For example, a sample ROI analysis compares cloud computing to the cost of the data center. The focus of the book is on the Infrastructure-as-a-Service and explores the cloud services provided my Amazon (e.g., Simple Storage Service, Elastic Compute Cloud, etc). The book also includes chapters dedicated to security and availability, with reference to the context of cloud computing.

---

61 www.cloudcomputingshow.blogspot.com/

62 www.johnmwillis.com/best-of/

63 www.opscode.com/blog/2010/02/03/opscode-announces-john-willis-as-new-vice-president-of-training-services/

64 www.redmonk.com/cote/topic/podcasts/itmanagementguys/

Cloud Computing For Dummies
Authors: Robin Bloor, Judith Hurwitz, Marcia Kaufman, and Fern Halper
Publication Date: October 30, 2009 (Hoboken: Wiley Publishing Inc.)

Summary: Provides an overview of the key issues when approaching cloud computing. Topics explored include: developing a cloud strategy, data management, hybrid and private clouds (including a brief look at vendors within this space), IaaS, PaaS, SaaS, governing the cloud, and other similar topics.

Cloud Security and Privacy:
An Enterprise Perspective on Risks and Compliance
Authors: Tim Mather, Subra Kumaraswamy, and Shahed Latif
Publication Date: September 22, 2009 (Sebastopol: O'Reilly)

Summary: The book begins with a look at the core cloud computing concepts. From a security perspective, topics explored include: infrastructure security (at the network, application, and host layers), data security, identity/access management, security management (including availability) and security-as-a(cloud)-services. The book also explores privacy, audit, and compliance issues. The book also includes sample SAS 70 and SysTrust reports, which are explored in greater detail in the chapter audit and assurance issues.

This publication was originally published by The Canadian Institute of Chartered Accountants (CICA) in 2011. It has been reissued by the Chartered Professional Accountants of Canada (CPA Canada) as originally published non-authoritative guidance.

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA