SMPs and the Cloud: Key Benefits & Risks

Author: Malik Datardina, CPA, CA, CISA

Introduction

Cloud computing does not represent new technology. Instead, it offers an alternative way to *consume* technology – on an "as needed" basis instead of investing in hardware and software upfront. Cloud computing is defined by The National Institute of Standards and Technology as "the provision of computational resources on demand via computer network." Should small-and-medium sized practitioners (SMPs) use cloud computing within their practice? Although only the individual SMP can answer that question, this article will assist SMPs in identifying key benefits and risks associated with cloud computing. While cloud computing is available in a variety of service models (e.g. public, private, hybrid etc.) and deployment models (Software-as-a Service (SaaS), Infrastructure-as-a-Service, Platform-as-a-Service, etc.), the public Software-as-a-Service (SaaS) category[1] will be most relevant to SMPs. For more details on cloud deployment and service models, see CPA Canada's[2] publication "Cloud Computing: A Primer"[3]. To illustrate the differences in cloud versus desktop applications, the Appendix looks at QuickBooks as an example.

What is the Benefit of Cloud Computing?

The key benefits of cloud computing are:

- **Access what you need, when you need it:** With the pay as you go approach to software, applications can be "rented" for the time required. For example, when Animoto's[4] application went viral, they were able to seamlessly expand their cloud-based environment from serving 25,000 users (approximately 50 servers) to serving 250,000 users (approximately 3,500 servers) within three days.[5] Without using the cloud, Animoto would have been either unable to keep up with the sudden spike in demand or they would have spent hundreds of thousands of dollars to buy and maintain the 3,500 servers to meet such demand.
- **Expense it!** Since cloud computing is a service, the fees paid are tax deductible and do not need to be capitalized and depreciated for tax purposes.[6]
- **Upgrades are included**: With SaaS, patching, upgrades and other maintenance fees are included as part of the subscription fee. For example, Workday Human Capital Management, a SaaS based human resource management system, automatically upgrades its application every four months.
- **Eliminating patching, upgrades and other maintenance.** When using SaaS, the service provider takes care of the system maintenance for the application. For example, an organization can pay Google $50/month to manage its email[7] in the cloud, which means the organization no longer needs to maintain an email server, patch it or upgrade the software. In terms of new features, the service provider (e.g. Google) rolls them out in a manner that is invisible to the user organization.

- **Accessibility through the browser:** Applications can be accessed from anywhere the user can access a compatible browser and an Internet connection.
- **Greater enterprise agility:** Internal IT often requires long lead times to implement solutions. With cloud-based solutions, the applications are already running and it is a matter of integrating that application into the existing IT infrastructure at the firm. This ability to deliver business processes faster is one of the key factors driving the adoption of cloud computing amongst organizations.

What are the Risks Associated with Cloud Computing?

When considering cloud computing, it is tempting to focus solely on issues related to confidentiality (discussed below under 'Confidentiality and Privacy Issues'). However, from a business case perspective, there are many other issues that need to be considered prior to determining whether cloud computing is actually feasible. These include:

- **Loss of direct control**: Cloud computing is essentially a form of outsourcing, which means control of the application is handed over to a third party. Consequently when using the cloud, SMPs must feel confident that the outsourcing related risks have been addressed. In other words, the best practices that apply to outsourcing also apply to cloud computing (e.g. getting a Service Organization Control (SOC) audit report over the operating effectiveness of controls, maintaining local backups, vendor selection, relative merits of software offering, assessing vendor reliability, etc.). This includes assessing the viability of the cloud provider and understanding what will happen to your data if the company goes out of business or is bought out.
- **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" (i.e. it is more expensive to pay "per hour, than if you make an upfront commitment"[8]). Consequently, SMPs should compare the cost of the SaaS application (e.g. Salesforce.com, Microsoft Dynamics online, etc.) to the on-premise alternative (e.g. Oracle CRM, Microsoft Dynamics, etc.).
- **Who are you relying on?** Practitioners should also be aware that their cloud service provider may rely on other cloud providers. For example, if a practitioner were to use a SaaS-based customer relationship management (CRM) application that relies on Amazon's Web Service (AWS), they *could* experience an outage if AWS were to become unavailable. Consequently, outsourcing considerations should apply to these secondary providers as well.
- **Standard contract offers little, if any, protection**: The default "terms of services" offered by cloud providers indemnify the providers of basically everything, such as downtime, lack of security, and any other issue. Consequently, SMPs should get qualified legal counsel to review the terms of service to understand how a breach, outage or other failure at the cloud service provider will be handled by the provider and what recourse is offered to the firm.
- **Cost overruns**: Although cloud computing uses the on-demand model of pricing, firms need to be aware that users are not in the habit of "turning off the apps" when they are no longer needed. Consequently, if there are no procedures to ensure cloud services are turned off, it can result in cost overruns. For example, if an accounting firm were to "rent" secure Amazon Web Services servers during tax time, they have to remember to shut down the extra servers rented after tax season is over. Otherwise the amount paid to Amazon could exceed the cost of buying and maintaining their own

servers. Firms, therefore, should institute procedures to monitor on-going costs to identify variances against budgets.

- **Network Reliability and Bandwidth costs**: Use of cloud-based applications requires a fast, reliable network and Internet connection. Also, SMPs need to assess how much the SaaS provider will charge for uploading and downloading data from their cloud. For example, Microsoft charges 10 cents to upload data and 15 cents to download.[9]
- **Integration challenges**: SMPs also need to investigate the resources required to integrate the new cloud application, with the pre-existing applications used within the firm. Without integration, firms run the risk of managing disparate applications. For example, when an employee leaves the firm, the IT administrator would have to manually cut-off access at *each* cloud service provider if the access management is not integrated within the firm's existing IT administration. Firms must therefore identify and estimate all costs, such as integration, to appreciate the cloud's "total cost of ownership".

Confidentiality and Privacy Issues

The largest concern when discussing the cloud is security. Of particular concern is ensuring confidentiality of client information – which is required by the rules of professional conduct[10]. Confidentiality and privacy issues are particularly important to practitioners who are required by professional conduct rules to ensure the confidentiality of client data, including tax returns, working papers, and any other client information retained by the practitioner. For many firms, the risk of a breach may rule out the use of cloud computing applications – especially if data is stored at the cloud service provider in an unencrypted format. However, firms may deem the risk to be less for non-confidential data, such as marketing materials.

Security risk: Is my co-tenant a hacker?

What sets the cloud apart from traditional IT outsourcing is that you are in a shared environment. Your "co-tenant" may just need a valid credit card to anonymously gain "tenancy" into the cloud service provider's environment. In fact, hackers have used this cloak of anonymity within the cloud to launch cyber-attacks, such as the infamous breach against the Sony Playstation Network.[11] Another potential issue is that hackers may find vulnerabilities in the shared computing environment and exploit these vulnerabilities to attack "co-tenants". To date, there are no known cases of cloud computing service providers getting breached by malicious hackers. However, security researchers were able to exploit vulnerabilities in Amazon Web Services to "see" what was going on in the target's machine.

Not everyone agrees that cloud computing is a greater security risk. The counter argument is that large cloud service providers will have state-of- the- art security since it is of strategic importance to their business. To support this argument, one could point to the fact that salesforce.com has experienced one known security breach, which was attributed to human error instead of a sophisticated attack launched by hackers.[12] To mitigate risks, organizations need to determine what assurance the cloud service provider is offering by way of audit reports (e.g. SOC 2,SOC 3, etc.) or having a 'right to audit clause' in the service level agreement[13].

Law enforcement: Warrantless access to your client's data

In Canada as well as the US, law enforcement can access data stored on any system (including those owned by cloud service providers) without a warrant or the consent of the organizations that own the data.[14] However, such concerns did not stop Lakehead University from outsourcing its email to Google.[15] From a privacy perspective, as long as the firm is "transparent" and gives notice to their clients that the information "may be accessed by the courts, law enforcement and national security authorities", then they are in compliance with privacy laws.[16] For example, the Privacy Commissioner of Canada dismissed privacy complaints against CIBC for outsourcing their credit card processing to the US for many reasons including the fact that CIBC gave its customers notice that US law enforcement may access their data.[17] Practitioners need to be aware of what their clients are comfortable with. Though some practitioners may be comfortable with this issue, their clients may not and would rather keep their information off the cloud.

Putting the Cloud in Perspective

The cloud offers a unique way to consume technology, which can be advantageous in some circumstances. For example, firms that are starting up may see it beneficial to buy SaaS-based audit engagement management software – if they feel their potential clients are comfortable with having their data on the cloud and they have comfort that the data will remain confidential. Other firms may see it beneficial to use cloud-based backup services that allow them to encrypt the data with their own encryption keys, which ensure that not even the cloud provider or law enforcement can access the data.[18] In other words, the fundamentals of acquiring software do not change: SMPs need to determine what business needs the application to fulfill and whether the risks can be mitigated to a satisfactory level. Key consideration for the latter is whether the practitioner can gain adequate comfort that their clients' information will remain confidential when residing at the cloud service provider.

Appendix: Illustrative Example – QuickBooks Cloud versus Desktop Version

SMPs may find that their clients are contemplating the move from their desktop accounting package to the various cloud-based packages. GigaOm technology-research site contrasted the 2010 QuickBooks[19] online to its desktop counterpart:[20]

Criteria	QuickBooks 2010 (desktop package)	QuickBooks Online Plus (SaaS)	Comment
Cost	$300	$35 per month or $420 per year	When moving to the cloud, the user should assess the net difference in functionality between the desktop and the cloud based version and determine whether the additional functions offered by the cloud version justify the additional cost.
Accountant Access	User must grant their accountant remote access to their system	Accountant (who is authorized by the user) can access the application through their Web browser	Other cloud-based accounting packages (e.g., Zoho) cite the ability to grant access to their customer's accountant as a feature worth advertising.[21]
Functionality	Able to create specialized reports	Limited functionality when compared to the desktop version, such as the inability to generate specialized reports, reduced customizability of forms, and inability to edit lists en-masse.	Regardless if it is SaaS or a desktop application, the accounting package needs to deliver the core functionality required by the user.
Backup & Security	Users must maintain offsite backups themselves, as well as secure their own data.	Data is stored off-premise by the cloud provider and users can download a copy creating a local backup. Offsite data is secured by the cloud provider and their team of specialists.	Data redundancy is easier to achieve with the cloud, since the user only needs to periodically download a local copy. With respect to security, the desktop version runs the risk of the client data being compromised if the device with the application is lost/stolen. Whereas in the cloud model, the data is not stored on the device and is retrievable through the Web browser.[22]

As illustrated by this brief analysis, SMPs and their clients need to evaluate the pros and cons of the cloud-based offerings as compared to a desktop on-premise version to determine if the move to the cloud makes sense. The decision to adopt the cloud is not a clear cut choice and will depend on the consideration of various factors such as functionality, price, security, maintenance, integration, etc.

---

[1] With SaaS, the actual application (managed by a third-party thereby making it a public cloud) is consumed right through the browser. In the SaaS model the user organization is responsible for only managing the application (e.g. control access to the application, number of seats, etc.), whereas the cloud service provider is responsible to secure the application, underlying operating system, etc. The balance of responsibilities, however, ultimately depends on the terms of service. Practitioners should, therefore, scrutinize the agreement to determine how these responsibilities are allocated between them and the cloud service provider.

[2] The Canadian Institute of Chartered Accountants (CICA) and the Certified Management Accountants of Canada (CMA Canada) joined together January 1, 2013, to create Chartered Professional Accountants of Canada (CPA Canada) as the national organization to support unification of the Canadian accounting profession under the CPA banner.

[3] http://www.cica.ca/focus-on-practice-areas/information-technology/publications/item48755.pdf

[4] Animoto offers an application that creates videos by combining photos uploaded by users with music using a special program to create a synchronized experience. They use Amazon Web Services, a cloud service provider that offers Infrastructure-as-a-Service.

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

[6] https://www.deloitte.com/view/en_ca/ca/e6427526d9549210VgnVCM100000ba42f00aRCRD.htm [Accessed December 31,2012]

[7] The monthly price also include Google's cloud-based office productivity suite, which include word processing , spreadsheets, etc.

[8] 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).

[9] 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/

[10] See the Handbook; CI 208 – Confidentiality of Information

[11] Hackers used Amazon Web Services to launch the attack against the Sony Playstation Network to breach the data associated with 77 million account holders. See: http://www.theregister.co.uk/2011/05/14/playstation_network_attack_from_amazon/ [Accessed December 31,2012]

[12] http://www.zdnet.com/blog/berlind/phishing-based-breach-of-salesforce-com-customer-data-is-more-evidence-of-industrys-need-to-act-on-spam-now/880 [Accessed December 31,2012]

[13] Getting a right to audit clause may not always be possible, especially if the SaaS provider is large and the organization seeking the right to audit clause is small.

[14] www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp [Accessed July 15,2013]

[15] http://www.itbusiness.ca/it/client/en/Home/News.asp?id=53561&bSearch=True [Accessed December 31,2012]

[16] Processing Personal Data Across Borders: Guidelines, (January, 2009) online: Office of the Privacy Commissioner of Canada < http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf >. [Accessed December 31,2012]

[17] The Privacy Commissioner found CIBC in compliance as "CIBC notified its customers of the risk that their personal information might be accessed under the provisions of the USA PATRIOT Act whilst in the hands of a U.S.-based third-party service provider. Thus, by providing such information, the bank was informing its customers about its policies and practices related to the management of their personal information, in accordance with Principle 4.8." See the full judgement for the full context and other important details: http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.asp [Accessed December 31,2012]

[18] See: http://broadcast.oreilly.com/2010/02/the-sacred-barrier.html by George Reese, author of Cloud Application Architectures and founder of EnStratus, [Accessed December 31,2012]

[19] This example is provided for illustrative purposes only. CPA Canada and the author of this document have not performed any due diligence and do not implicitly or explicitly endorse this application.

[20] http://gigaom.com/2010/05/17/quickbooks-desktop-or-online/ [Accessed June 7, 2013]

[21] www.zoho.com/books/accounting-software/invite-your-accountant.html [Accessed June 7, 2013]

[22] For additional security considerations for the cloud, refer to the discussion under "Confidentiality & Privacy Issues"

About the Author

Malik Datardina, CPA, CA, CISA, is a Senior Manager at Deloitte. He is a technical consultant for CPA Canada's Information Management and Technology Advisory Committee.