Ten Things to Consider Before Moving to the Cloud

Malik Datardina, CPA, CA, CISA
Author
Malik Datardina, CPA, CA, CISA

Information Management and Technology Advisory Committee
Mario R. Durigon, CPA, CA (Chair)
Chris Anderson, CA(NZ), CISA, CMC, CISSP (Vice Chair)
Gary S. Baker, CPA, CA, CGEIT
Efrim Boritz, FCPA, FCA, CISA, PhD
Malik Datardina, CPA, CA, CISA
Nancy Y. Cheng, FCPA, FCA
Andrew Kwong, CPA, CA, MBA
Richard Livesly, MBA, CGEIT
Jodie N. Lobana, CPA, CA, CPA (IL), CIA, CISA
Maura O’Shea, CPA, CA
Robert Parker, FCPA, FCA, CISA
Robert J. Reimer, CPA, CA, CISA, CISM, CGEIT, CRISC
Steve Soychak, CPA, CMA
Bryan C. Walker, CPA, CA

CPA Canada Contact
Cecilia Banh, CPA, CA, MAcc
Principal, Research Guidance and Support

The Information Management and Technology Advisory Committee (IMTAC) is part of the Research Guidance and Support Group at the Chartered Professional Accountants of Canada. The advisory committee provides guidance and advice to CPAs about information management and technology matters affecting the profession and business community. For more information about IMTAC, please visit us at www.cpacanada.ca/IMTAC
# Table of Contents

**Introduction**  
1

**Planning Considerations**  
4
Lesson 1: Avoid the temptation of on-boarding to the cloud too quickly  
4
Lesson 2: Assess the cloud vendor’s financial stability and longevity  
7
Lesson 3: Involve all key stakeholders  
10

**Cost Considerations**  
12
Lesson 4: Understand how cloud pricing works  
12
Lesson 5: Assess and quantify cloud integration challenges  
13
Lesson 6: Calculate the total cost of ownership before committing to the cloud  
15

**Negotiation Considerations**  
17
Lesson 7: Allocate responsibilities clearly in the cloud service agreement  
17
Lesson 8: Negotiate the necessary level of application support  
18

**Maintenance Considerations**  
19
Lesson 9: Assess the impact of upgrading and modifying the cloud  
19
Lesson 10: Assess the compatibility of the cloud provider’s standards  
20
Is Moving to the Cloud Worth It? 22

Appendix: Security Issues Related to Cloud Computing 23

Assessing the Security Risks of Moving to the Cloud 23
  What Are the Security Risks with Cloud Computing? 23
    Shared Access 24
    Anonymous Access 24
  Data Ownership and Confidentiality 24
  Evaluating the Risk of Cloud Computing on IT General Controls 25

Putting Security in Perspective 26
Cloud computing is defined by the National Institute of Standards and Technology as “the provision of computational resources on demand via computer network.” Cloud computing does not represent new technology; instead it offers an alternative way to consume technology. One way to gauge the current state of a hyped technology, such as cloud computing, is to examine its current position on Gartner’s Hype Cycle, which follows a particular technology’s path from its inception to mainstream adoption. According to Gartner, cloud computing has passed beyond the hype phase (also known as the “peak of inflated expectations”) and is now working its way through the “trough of disillusionment,” where cloud computing customers begin to see past the lofty promises of the technology and realize the potential challenges of implementing cloud-based solutions within their organizations.

Cloud computing has some key advantages, including:

- **The ability to fund IT projects from operational expenditures:** Since cloud computing is a service, the costs are expensed instead of being capitalized. The fees paid are tax deductible and do not need to be capitalized and depreciated for tax purposes.³

- **Patching, upgrades and other maintenance are included with SaaS applications:** With Software as a Service (SaaS),⁴ patching, upgrades and other maintenance fees are included as part of the subscription fee. The cloud service provider (CSP) looks after managing the technology infrastructure, allowing the customer to focus on its business.

---

1 The Gartner Hype Cycle is a five-phase development curve that describes the different phases of a technology’s maturity, which includes the Innovation Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment and finally the Plateau of Productivity. See [www.gartner.com/technology/research/methodologies/hype-cycle.jsp](http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp) for more information.

2 See [www.gartner.com/newsroom/id/2819918](http://www.gartner.com/newsroom/id/2819918) for Gartner’s 2014 Hype Cycle.


• **Accessibility through the browser:** Offering easy access through the browser, cloud computing allows users access to the application from absolutely anywhere as long as they have a compatible browser and an Internet connection.

• **More efficient use of IT resources:** At the Infrastructure as a Service (IaaS)\(^5\) layer, organizations can temporarily rent public cloud resources, such as servers, instead of having to buy, implement and maintain the servers themselves. For example, when Animoto’s video generation app went viral it went from serving 25,000 users (approximately 50 servers) to serving 250,000 users (approximately 3,500 servers) within three days.\(^6\) Through the use of cloud computing Animoto avoided the need to buy excess server capacity that would have been idle up to the spike in demand and idle after the spike in demand subsided. Also, organizations can use cloud-based technologies to consolidate internal resources through a private cloud.

• **Off-site storage:** The cloud creates off-site storage, thereby providing availability in case of disaster at the business premise.

As the adoption of cloud computing grows, we wanted to explore the practical realities of implementing the cloud. Given the many advantages of cloud computing, this publication highlights the challenges and issues associated with cloud computing implementations to help organizations properly budget and plan before moving to the cloud. Through interviews with organizations that have implemented the cloud, along with advice from consultants and subject matter experts, the following 10 lessons emerged from our interviews:

**Planning considerations:**
Lesson 1: Avoid the temptation of on-boarding to the cloud too quickly
Lesson 2: Assess the cloud vendor’s financial stability and longevity
Lesson 3: Involve all key stakeholders

**Cost considerations:**
Lesson 4: Understand how cloud pricing works
Lesson 5: Assess and quantify cloud integration challenges
Lesson 6: Calculate the total cost of ownership before committing to the cloud

**Negotiation considerations:**
Lesson 7: Allocate responsibilities clearly in the cloud service agreement
Lesson 8: Negotiate the necessary level of application support

---

5 According to NIST, IaaS CSPs “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.” See [http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf](http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf) (September 2011)

Maintenance considerations:
Lesson 9: Assess the impact of upgrading and modifying the cloud
Lesson 10: Assess the compatibility of the cloud provider’s standards

These lessons mostly reflect the experience of large organizations implementing third-party SaaS applications. Large organizations have challenges with the cloud because of the integration hurdles they have to overcome to make the cloud work with all the data and systems that they have in place. Organizations that have no systems (e.g., startups) or have basic applications that operate in silos (e.g., a company with email, office productivity, and a basic accounting application) will not face these issues and will have a much simpler experience adopting a SaaS application. Although these lessons are derived from interviews with large organizations, they can also be applied to small and medium-sized enterprises (SMEs), as each lesson is based on well-established IT practices. SMEs can assess the relevance of the lessons to their particular context.

For organizations that need additional information on the cloud—including key benefits and risks—refer to CPA Canada’s publications Cloud Computing: a Primer and SMPs and the Cloud: Key Benefits & Risks.
Planning Considerations

**Lesson 1: Avoid the temptation of on-boarding to the cloud too quickly**

**Challenge:** Cloud computing has a higher risk of being adopted prematurely by an organization than traditional software due to the pre-fabricated nature of the cloud-based solution, as well as promises of a shorter implementation time.

With any new technology, there is a risk that an organization will be caught up in the hype and implement the technology without proper vetting. Organizations that implement solutions based on hype may encounter issues that they did not expect, which may result in cost overruns. Furthermore, the lack of sufficient vetting of the cloud-based application may result in buying a sub-optimal solution. There may be another application available that would have met the organization’s needs in a more effective and cost-efficient manner.

The risk of buying on hype is higher with cloud-based applications because unlike on-premise enterprise class software and traditional outsourcing arrangements, it is much easier for organizations to connect directly with the CSP and circumvent the IT department as well as existing procurement processes. Cloud computing, in a sense, is similar to a pre-fabricated house that is ready to install. Management should be aware of the risk that users can simply purchase cloud services with their credit cards and have the cloud solution up and running relatively quickly. Traditional controls to monitor or block the implementation of applications (e.g., access control management, administrative rights control) won’t work because the application is accessed off-premise through the web browser. It is a known risk that some departments circumvent the traditional procurement controls by acquiring cloud solutions on corporate credit cards, effectively bringing in cloud computing solutions through the expense report process. Consequently, organizations must make all employees aware that acquiring cloud-based applications is subject to the same level of controls as when buying an enterprise resource planning (ERP) solution or outsourcing IT to a third party. A policy should be in place that prohibits the acquisition of cloud-based applications through the expense report process and mandates that all applications be routed through the established procurement process.
process. Such a policy should be supplemented by an awareness campaign that makes employees aware of the risks of putting the organization’s data onto the cloud and how it can be difficult to integrate such applications with the overall system environment after the fact. At the end of the day, making the decision to move to the cloud should be managed like a capital project, requiring a clearly defined scope and a project team to manage and implement.

**Lessons learned:** In order to ensure that cloud computing services are acquired in an authorized manner, organizations should have a cloud computing policy that includes the following:

- **Definition of cloud computing:** The policy should help organizations communicate the salient differences between cloud computing applications and traditional applications. Cloud computing should also be treated as a capital project that would require the same controls, review and approval that are placed on capital investments.

- **Explanation of how cloud computing fits into the overall business and IT strategy:** On-boarding to the cloud can affect other objectives of the organization. For example, one organization noted how implementing the cloud actually impeded its overall big data and analytics strategy because the cloud application created another silo of data within the organization, making it more difficult to obtain this data for the purpose of running enterprise-wide analytics.

- **Explanation of cloud computing risks:** Describe the information security, privacy and other risks associated with moving to the cloud. Since security is a major concern in cloud computing, a separate Appendix has been included to discuss the security considerations.

When evaluating a potential cloud solution, identify the underlying business requirements and then methodically scrutinize the features of the new technology. For example, business management should draft a list of the desired functionality in terms of must-haves and nice-to-haves and subject all desired vendors—cloud and otherwise—to a rigorous Request for Proposal (RFP) process. One organization noted that vendors who claim to meet all the requirements should actually be scrutinized to a higher degree, such as requiring detailed demonstrations of the application. Organizations should also request references from the CSP and contact them independently.

Organizations should take advantage of the pre-fabricated nature of the cloud and ask the CSP to complete a proof of concept (POC) prior to signing an agreement. One organization convinced the CSP to implement a pilot and committed to purchasing the licences only if it

---

7 For example, the casual approach that a user has to the cloud may lead to organizations unwittingly exposed to significant risks. See Deloitte, “Pragmatic cloud computing: Six keys to successfully using the cloud,” Melbourne, Australia, 2012, available at [http://etherworks.com.au/index.php?option=com_k2&id=86_feead2d9f340248df504838d292bc3e&lang=en&task=download&view=item](http://etherworks.com.au/index.php?option=com_k2&id=86_feead2d9f340248df504838d292bc3e&lang=en&task=download&view=item)
Planning Considerations

was satisfied with the results of the pilot. This approach resulted in the CSP resolving and dealing with integration challenges before the organization started to pay for the licences. Not only did this save the organization money, but it also ensured it was getting the application that met its business requirements.

Organizations must also assess whether there is a fit with the underlying requirements and the fundamental cloud computing business model. Cloud computing pools its resources and essentially has a one-size-fits-all approach to serving its customers by offering a standardized level of functionality to all of its users. Consequently, a CSP will rarely customize the way it deals with a specific customer. Although CSPs may accommodate large players who are willing to pay extra, there are instances where even large companies can’t get concessions from CSPs. For example, Eli Lilly (a leading pharmaceutical company) terminated its use of *Amazon EC2* because of an inability to negotiate contractual terms with Amazon Web Services.* Consequently, if an organization has customized requirements for information security, availability and support, etc., then there is a low likelihood that a cloud-based application will meet those customized needs.

Consideration should be given to the strategic nature of the functionality of the processes being moved to the cloud, especially at the application or SaaS layer. Cloud computing is optimized to handle an organization’s non-core and non-strategic applications. This is similar to the philosophy of traditional outsourcing, where third parties handle the non-strategic aspects of the technology environment. On the other hand, moving strategic applications to the cloud requires the organization to work with the CSP to integrate that strategic technology into the CSP shared environment. In other words, the organization must trust the CSP to keep this proprietary technology confidential and not share it with other customers of the cloud computing service. Organizations contemplating such a use of cloud computing should consult an intellectual property lawyer to ensure they are truly protected by the CSP’s agreement.

A separate but related risk is the issue of storing sensitive data on the cloud. Organizations should already have a policy in place that requires them to assess the sensitivity of their data. Although specific categories vary from organization to organization, usually there are four categories: highly confidential, confidential, internal and public (ordered from most sensitive to least sensitive). Each category should have a standard set of controls tied to that data. For example, an organization could have a policy in place that requires highly confidential data to be encrypted prior to transmission. Organizations should understand the sensitivity of the data they have before moving to the cloud. Highly sensitive data, such as trade secrets or other strategically important information, should not be moved to the cloud. Such information is sought by hackers and others. Regulated data, such as personal health information,

---

8 The vendor is mentioned 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 vendor.

also needs to be carefully reviewed from this perspective. For example, in Ontario there is no explicit prohibition on moving personal health information to the cloud, but due to the requirement to notify users of data breach\(^{10}\) (e.g., loss/theft of data) it may be prudent to keep such data off CSPs that do not encrypt the data all the time.\(^{11}\) As discussed in the Appendix, moving sensitive data into a shared environment where anonymous access is permitted carries the risk that hackers and others may gain access to such data.

Organizations also need to determine whether the rights to the data are effectively transferred to the CSP. As noted by Bill Snyder,\(^{12}\) “laws pertaining to cloud storage are so new and so vague that it isn’t even clear the data you upload to a storage site is still yours.” Specifically, he notes how Verizon states in the contract that it “shall have the right, but not the obligation, to monitor the use of, and to screen, refuse, move or remove any content transmitted to or from, any Additional Service for compliance with law or the terms of this Agreement.” Snyder further explains how this clause allowed Verizon to scan the content from one of its subscribers, who was found to have illegal content and was later apprehended by police. If a similar clause exists in the agreement with the CSP, then the organization could be subject to similar monitoring. Refer to the Appendix for further information on data ownership and confidentiality.

**Lesson 2: Assess the cloud vendor’s financial stability and longevity**

**CHALLENGE:** Given the hype around cloud computing, CSPs are more likely to be acquired or “acqhired” by larger players in the industry.

Assessing vendor viability or the longevity of a potential outsourcing partner is a well-recognized best practice. Several of the CSPs are small niche vendors, however, and before investing time and effort in integrating a potential cloud computing application, it is prudent to ensure that the CSP is financially viable. Aside from insolvency, another reason the cloud application may become unavailable is that a larger technology vendor may acquire the CSP in order to increase the market share of its existing product line. The vendor will likely discontinue the use of the application in order to achieve this objective. A large vendor may also buy the CSP primarily for its talent, which is termed “acqhire.” In this case, it is acquiring the CSP’s employees and not its cloud services.

---


11 When data is encrypted “by strong (i.e. hard-to-decipher) encryption, there is no actual loss of information and no need to notify patients.” See [https://oplfrpd5.cmpa-acpm.ca/-/protecting-patient-health-information-in-electronic-records](https://oplfrpd5.cmpa-acpm.ca/-/protecting-patient-health-information-in-electronic-records)

Lessons learned: It can be challenging to assess the viability and longevity of startup and niche players who don’t have a long history and a set of financials. One organization noted that when it could not obtain financial statements from a potential vendor, it inquired who the investors in the CSP were and performed background checks accordingly. The company also asked for the CSP’s product development roadmap to gain insight into the future development plans for the software, looking for signs of the CSP’s commitment to the longevity of its software.

Organizations need to ensure they have a backup plan should their CSP be acquired, go bankrupt or become unavailable. One organization noted how the cloud-based application it was using ended up being purchased by another vendor and found the development roadmap had changed and no longer met its business requirements. As a result, it had to move to a new CSP. Consequently, organizations need to proactively address the risk of CSP failure as a part of their backup and recovery strategies as well as their disaster recovery plan (DRP). This includes addressing the following issues:

- **Contractual provisions to access data:** Where possible, the organization should contractually obligate the CSP to provide its data in a usable format if the CSP is bought out or goes bankrupt. As noted in a blog post by a cloud-based e-discovery site, the “agreement should state that the data of the company should be the property of the company alone and not the property of the cloud vendor.”\(^\text{13}\)

- **Data backups:** Organizations should have their data backed up from the cloud provider even if they are able to include a contractual provision to access their data in the case the CSP is no longer in business. Organizations should not assume that they will always have a window of opportunity to get their data out of the cloud in a timely manner, as the cloud computing application may become permanently unavailable due to physical destruction or unforeseen circumstances. For example, the U.S. government shut down Megaupload (a cloud-based storage service) due to alleged copyright violations and instituted a “long, drawn-out process that would require third parties—often individuals or small companies—to travel to courts far away and engage in multiple hearings” in order to get their data back.\(^\text{14}\)

- **Establishing a “Data Exit Strategy” to get data off of the cloud:** Although having the data off of the cloud is critical, organizations also need to determine how they will access and use this data should the provider become unavailable. One way to do this is to find an alternative CSP. For example, SunGard Availability Services\(^\text{15}\) could be used as an


\(^\text{14}\) Cohn, Cindy and Samuels, Julie “Megaupload and the Government’s Attack on Cloud Computing,” [www.eff.org/deeplinks/2012/10/governments-attack-cloud-computing](http://www.eff.org/deeplinks/2012/10/governments-attack-cloud-computing) (October 31, 2012)

\(^\text{15}\) Ibid., footnote 8.
alternative service provider for Amazon Web Services.\textsuperscript{16} Another alternative is to use an on-premise equivalent. However, this is not as straightforward as it seems. For example, users of QuickBooks\textsuperscript{17} can download their data from QuickBooks Online. However, to import data onto the offline version of QuickBooks requires conversion of that data and some elements can’t be converted.\textsuperscript{18} Regardless, organizations must identify the solution proactively and have a plan to migrate from their current CSP to the alternative CSP or on-premise solution. Disaster recovery planning must be applied to cloud-based applications just as it would be applied to on-premise applications.

\textsuperscript{16} Ibid., footnote 8.

\textsuperscript{17} Ibid., footnote 8.

\textsuperscript{18} See the following Intuit link that discusses this issue: \url{https://qbo.intuit.com/redir/qbconvert}
Ensuring data confidentiality: The pooled nature of the cloud infrastructure makes it difficult to apply traditional data destruction techniques, such as destroying the physical media that held the confidential data. The organization should therefore make sure there is a clause in the CSP agreement that ensures all company data is destroyed and unrecoverable when the organization terminates its use of the CSP.

Lesson 3: Involve all key stakeholders

CHALLENGE: The ready-to-install nature of cloud computing leads business users to feel they don’t need to involve IT specialists and other subject matter experts such as contractual or legal specialists who will thoroughly review the contract and understand the implications.

There is a risk that business users may be overconfident in believing they can implement cloud-based solutions without the assistance of other departments such as IT and legal. This could be due to the fact the users are comfortable with how they use cloud-based applications in their personal lives (e.g., Google docs, Gmail, Hotmail, etc.) or that they want to circumvent IT for the sake of expediency. Without the right subject matter experts involved in the RFP process, the evaluation team may lack the technical depth to assess the impact of the architectural differences between various service providers.

Lessons learned: One organization noted it implemented a cloud-based application without involving the right IT and information security subject matter experts, which resulted in issues in these areas. For example, the technical security access requirements were not embedded in the RFP and contract negotiation processes. The security requirements were identified later and it took significant time and effort to address them, delaying the implementation of the application.

From an overall IT perspective, an IT specialist can understand the resources required (time-lines, staff support, external resources, etc.) to integrate a cloud-based application into the organization’s infrastructure. Specialists will also be able to inform the CSP of the relevant internal standards adopted by the organization that it must comply with. For example, one organization used Information Technology Infrastructure Library (ITIL), which is a set of best practices that organizations use to improve their internal IT service management (i.e. delivering support IT services to the business). However, as the organization did not include this as part of its contractual requirement that the CSP must abide by, it had to accommodate the IT service quality standards of the cloud provider instead.

IT specialists can also help negotiate the service level agreement (SLA) with the CSP. One organization noted that had the IT specialists been present at the negotiating table, it would have been able to design more robust provisions in the SLA. As the contract currently stands, the onus is on the organization to prove that the CSP is at fault when an outage occurs.
In hindsight, the organization should have included provisions that would hold the CSP responsible for monitoring the level of service delivered. This would make it easier for the organization to pinpoint the issue during a service outage and make the CSP accountable. Without this provision, it becomes nearly impossible to prove the service outage is the fault of the CSP. The company noted that it has not been able to get service credits to compensate for outages. Organizations should thoroughly scrutinize the exact procedure for getting refunds and credits for a service outage.

From a contractual perspective, organizations should use legal counsel or other specialists to assess the impact of the various implications of the contract.¹⁹ For example, one organization had to pay the CSP for the licence fees during the nearly yearlong implementation period before it started to use the cloud services. On a positive note, the organization had been proactive in mandating the CSP cover the costs of change requests related to the implementation. Although the CSP attempted to charge for change requests, the organization was able to prove it had no obligation to pay for them due to the provision in the contract.

Organizations could make it the responsibility of the procurement department to oversee the acquisition process to ensure that the right stakeholders are involved and that all proper procedures are completed. Without having the relevant technical expertise at the negotiating table, organizations may not identify all the costs and other effects the cloud-based solution will have on their business.

Cost Considerations

**Lesson 4: Understand how cloud pricing works**

CHALLENGE: Cloud-based pricing models may not scale down on lower usage due to the structure of the agreement. Unlike on-premise applications, which are paid for upfront, there is a risk that prices may increase unpredictably in the future.

As discussed in CPA Canada’s *Cloud Computing: a Primer*, cloud computing contracts offer on-demand computing that enables organizations to expand and reduce the amount of computing resources they require in an automated manner. For example, *The Washington Post* used the equivalent of 200 servers for 26 hours for about $145 to convert image files into searchable text.\(^{20}\) However, this can be attributed to the fact its CSP, Amazon Web Services (AWS),\(^{21}\) offers a pay-as-you-use costing structure so that its customers only pay for what they actually use. It costs less when less of the service is used, similar to the way utility providers bill for their services.

**Lessons learned:** Not all cloud-based solutions follow a pay-as-you-use costing structure. First, organizations need to recognize the type of cloud services they are paying for. Infrastructure as a Service (IaaS) does not work in the same way as Software as a Service (SaaS). The commoditized nature of IaaS lends itself to expansion and contraction. Although SaaS theoretically can work in the same manner, in practice it works differently due to the way SaaS providers structure their contracts. Large organizations get bigger discounts for the high volume of user licences they pre-purchase. For example, if Company A has agreed to buy licences for 5,000 users but now wants to reduce the licences to 4,500 users, it may end up paying more per user because it is no longer eligible for its volume discount.

---


\(^{21}\) Amazon Web Services (AWS) offers the basic computing resources at the Infrastructure as a Service (IaaS) layer.
Another pricing problem is that there is nothing stopping the CSP from raising its fees in the future. The organization could be forced to endure unexpected cost increases from the CSP because it could not lock in prices over the long term. This is unlike an on-premise application where the organization buys the hardware and software upfront and the maintenance fees can be fixed over a period of years. In a ZDNet article, Will Venters of the London School of Economics notes that forcing future price increases on customers is part of the profit-making strategy of SaaS providers. “In SaaS you are often locked into the development pathway of the SaaS provider,” he says. “You can’t stick with XP the same way we all stuck with Windows XP because we didn’t like Vista.”22 Venters is illustrating the stark difference between buying an application such as Windows XP, which has been used for more than a decade, and going to the cloud: the costs of the in-house application are paid upfront, whereas an organization has to pay fees to the CSP as long as it uses its service. Depending on the CSP and the negotiating power of the organization, however, it may be possible to set a fixed price. One organization was able to lock in the pricing for a fixed number of licences for a multi-year period. It was, however, unable to reduce the number of licences if it wished to retain this special pricing, and would have to pay a penalty if it prematurely terminated the agreement. Furthermore, when it increased the number of licences, it had to pay market prices and was not eligible for the discounted price that it had initially negotiated. In other words, the reality of SaaS pricing is that it does not expand and contract on an “as needed basis.”

Lesson 5: Assess and quantify cloud integration challenges

CHALLENGE: Cloud-based applications can pose significant integration challenges that can negatively impact timelines and increase the overall costs of the application.

A key factor that causes variability in pricing is assessing the level of integration required. The challenge of integrating cloud-based applications into on-premise applications is noted in Cloud Computing: a Primer: “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.”23

Lessons learned: Organizations with multiple systems may face cloud integration challenges. Out-of-the-box cloud solutions tend to work for a standard single system (e.g. a mainstream non-customized ERP). Here are some of the specific integration challenges faced by the companies interviewed:

22 www.zdnet.com/saas-cloud-pricing-can-it-ever-add-up-7000011847 (March 1, 2013)
• **Siloed applications:** One organization warned that if SaaS applications grow in an uncontrolled manner, you could end up with an infrastructure where each SaaS application sits in isolation and is unable to integrate with other applications. Controls need to be in place to ensure that all cloud-based applications go through a centralized process, such as procurement, to ensure that all such applications are inventoried. The next step is to implement a plan that outlines how an organization will integrate these applications into the overall computing environment.

• **Data management and conversion:** Organizations should assess the effort and time required to migrate the data from the legacy application to the cloud. One organization noted it had significant issues getting data converted into a format usable by the cloud-based application. Organizations must have a detailed understanding of the data requirements of the cloud-based application, how the application will interface and exchange data with existing applications, and how they will migrate the data from the legacy application to the cloud-based application in a valid, complete and accurate manner. A related challenge is configuring the cloud-based application to handle non-standard data feeds from the organization. One organization noted that its cloud-based application couldn’t handle data feeds from multiple systems, requiring the organization to design and build processes to feed the data into the cloud-based application.

• **Access management:** When implementing a cloud-based application it can be a challenge to ensure that information security and access management controls are applied to the cloud application. Specifically, organizations that use physical security devices to authenticate systems will have difficulties in implementing such controls. One organization had to invest effort and money into access management controls to ensure that the cloud-based application met the organization’s information security standards. A related challenge is to ensure that the single sign-on (SSO) access management is implemented in the cloud. Specifically, organizations need to understand how employees can seamlessly access the various cloud-based applications using their existing access management protocol. As noted in Lesson 3, organizations need to involve information security specialists in the vendor selection process who will assess in detail how the current security standards will be met. Such considerations are critical to ensure that only authorized individuals can access the applications and, more importantly, the data housed in those applications. For example, one area of potential risk is timely termination of access to the cloud-based applications, such as when an employee leaves the organization. The organization needs to involve the information security specialist to ensure that the technical specifications required to make this happen are defined in the RFP as well as in the contract with the CSP. In terms of third-party cloud access management solutions, one organization found that such solutions are in their infancy and that the market is still maturing. Consequently, an organization should have mitigating controls to ensure that processes and procedures are established to monitor access to the various cloud
services it uses. For example, where cloud services have not been integrated into the centralized access management system, manual procedures will be needed to periodically review access and ensure that access rights reflect the current role of the employee. These procedures should also be added to the employee termination process—even if it means manually logging into each of the cloud services and removing the terminated employee’s access one at a time.

- **Extended timelines:** Inadequately assessing the integration and implementation challenges can significantly impact timelines. Cloud-based vendors often advertise implementation timelines that are appropriate for organizations that use the application in isolation or as part of an ecosystem of applications that should seamlessly integrate with one another. Consequently, timelines can increase dramatically where the organization has to integrate the cloud-based application into its heterogeneous application environment. One company’s CSP promised a three-month implementation timeline that ended up taking 10 to 12 months. Lengthy system implementation timelines are not unique to cloud-based applications. However, if organizations require a solution to come online within a specific time frame to meet a specific business objective, they need to invest the same level of effort and scrutiny in assessing the potential implementation challenges of the cloud as they would for any other application.

- **Data security and control:** To be in compliance with internal policies and external regulations (e.g., privacy laws, Payment Card Industry Data Security Standard), it is critical to know in advance how data will be secured. Also, it should be understood in which country the data will reside, since different countries have specific regulations that the CSPs must abide by. See the Appendix for more details.

**Lesson 6: Calculate the total cost of ownership before committing to the cloud**

**CHALLENGE:** Without assessing the total cost of ownership (TCO), organizations may pay too much for the desired level of functionality or fail to select the application that best meets their needs.

When implementing any system, it is critical to evaluate the TCO. With cloud-based applications, organizations should be aware that the advertised price per user or price per usage might not address all the costs of implementing and integrating the solution into the organization’s computing environment. One organization, for example, noted that the costs of implementation were approximately 35% higher than expected.
Lessons learned: There can be a number of additional costs involved with implementation:

• **Payment of licences during the implementation phase:** Some CSPs require their customers to pay for licence fees at the implementation stage, before the application is ready to use.

• **Implementation consulting costs:** Organizations may have to pay for consultants at the CSP or an external systems integrator consultant. To understand the TCO, organizations should ask the CSP to clearly state the activities it will and won’t do during the implementation period.

• **Simultaneous payments for old and new applications:** If the implementation of a new cloud service is delayed, then the organization may have to pay to maintain the old application or renew the contract with the previous CSP. One organization got into a situation where it had to renew its contract with the old CSP because the new cloud service wasn’t ready. A clause in the contract should be put in place that requires payment only when the application is fully functional and available to the organization. Also, penalty clauses should be put in place to ensure the organization can recoup the costs of renewing contracts with legacy providers.

• **Additional service fees:** Some CSPs will charge for all aspects of the service provided, including analytical functions. For example, one organization unexpectedly had to pay for data that was only being kept for historical purposes. To avoid this charge, it implemented a manual process to filter the inactive data and retain it in its own environment. Organizations must understand how the CSP will handle different transactions and then determine which services will require additional fees.

• **Outsourcing fees:** One cloud-computing expert noted that CSPs can charge for every aspect of the outsourcing arrangement. For example, when obtaining a service that requires a Secure Sockets Layer (SSL) certificate, the CSP can charge a monthly fee for the service, whereas getting an internal IT person to implement the SSL certificate would require a nominal one-time charge.
Lesson 7: Allocate responsibilities clearly in the cloud service agreement

CHALLENGE: There is a lack of clear accountability among the CSP, external parties and the user organization.

There is a risk that the customer may assume the CSP is performing a task while the CSP assumes the customer is looking after the task. This risk is amplified when the customer has outsourced its IT to third parties. For example, Company A is currently outsourcing its IT services to IT Inc. Company A has now decided to outsource its payroll to CloudPay, a CSP. The risk here is that IT Inc. may assume that all the payroll tasks are moving to CloudPay, while CloudPay is assuming that IT Inc. will retain some of those responsibilities, resulting in gaps in service.

Lessons learned: When negotiating a contract with a CSP, clearly state the responsibilities of each party involved and how they will coordinate with each other to ensure that all tasks are completed. In the above scenario, Company A should first identify and itemize all tasks and responsibilities associated with the current arrangement with IT Inc. (i.e. before CloudPay is brought into the picture). Company A should then ensure that each of these tasks and responsibilities is clearly allocated to either IT Inc., CloudPay or Company A. Without such coordination and clear demarcation of the lines of responsibility, there could be confusion in the execution of these tasks, resulting in errors or delays. One organization noted that there were scheduling issues with integrating the Application Programming Interface (API)\(^\text{24}\) into the environment due to the lack of coordination between the outsourcer and the CSP. Awareness of the SLA and regular communication between all parties involved will help ensure that tasks are being completed as they are assigned.

\(^{24}\) The Application Programming Interface (API) is the way the cloud-based application talks to the customer's systems.
Lesson 8: Negotiate the necessary level of application support

CHALLENGE: Support levels may not meet expectations due to the standardized services offered by cloud providers.

The level of application support can be quite different in the cloud world compared to dealing with traditional application and outsourcing vendors. As noted earlier, the business model that cloud vendors adopt is to provide a standard level of service to all customers. Such a model can potentially limit the level of direct service the CSP will provide if there are issues after the application goes live.

Lessons learned: Organizations that are used to having their vendor assign a single point of contact to address technical support issues or other challenges will not likely find that level of support from CSPs, regardless of the size of the organization. For example, one of the larger organizations interviewed found that the responsiveness of the CSP was lower than expected; it was not given the priority service it was used to getting from its other vendors. If organizations have business requirements that demand timely support, the pooled approach of support provided by CSPs may not meet their needs.

One organization noted that it is critical to review the SLA terms related to support. Based on its experience, not all levels of support are equal. It found that the “high priority” level of support offered by the CSP was not as good as the support provided by the actual implementation team. Fortunately, it had negotiated a longer period of support from the implementation team than the standard contract stipulated. Organizations should understand the different levels of support available from the CSP and negotiate the level of support that is most beneficial to them.
Lesson 9: Assess the impact of upgrading and modifying the cloud

CHALLENGE: The cost of maintaining and upgrading cloud-based applications can be higher than expected.

One feature of cloud computing is that it has greater agility to meet the future needs of the business. For example, one of the touted benefits of Microsoft’s cloud-based version of its Office suite, Office365, is that users don’t have to worry about upgrading features or maintaining the application. This is unlike installed software, which requires users to periodically install patches. This can be a complex exercise where the software patches released by the vendors need to be properly tested and then installed to fix issues, enhance functionality or plug security holes in the software. However, the ability to achieve these benefits depends on how the cloud-based application is integrated into the existing infrastructure and what features the organization needs.

Lessons learned: To assess the impact of future upgrades to the cloud-based application, the business should ensure that an IT specialist reviews in detail how the application works and has a good understanding of how the components integrate with one another. One organization discovered after the fact that the cloud-based application it was using was actually a collection of smaller applications. With more moving parts, more can go wrong when upgrading or modifying an application that is integrated into the on-premise applications. For example, when the application is upgraded, connections may break. This can result in paying for additional resources to ensure that the application is adequately tested before upgrading. Although the CSP may force the upgrade on its customers, there are CSPs who can give the customer the ability to control the delivery of the upgrade. One organization noted that CSPs offer two upgrade models: opt-in or opt-out. The opt-in model involves lower risk: the organization tests

25 Ibid., footnote 8.
26 www.pcworld.com/article/259644/three_reasons_you_should_switch_to_office_365.html
the upgrade and then asks the CSP to apply it. The opt-out model involves higher risk: the CSP informs the customer the upgrade will be applied at a certain date and then the onus is on the customer to review the effects of the upgrade and opt out if it will have a negative impact. Organizations should therefore choose the opt-in model where possible.

When upgrading a cloud-based application, organizations should be aware of how CSPs manage customer requests for new features and functionality. Some CSPs have customer councils that manage and prioritize requests from customers. If the organization can convince the customer council that the functionality is beneficial to the customer base, it can effectively get the desired functionality for free, as it will be rolled out by the CSP as part of the next update to the application. On the other hand, if the majority of customers vote against adding the functionality, then the organization may have to pay the consulting costs to have the CSP build the customized functionality. This is akin to the problem of customized ERPs: non-standard features end up costing organizations more money to implement, upgrade and maintain because they deviate from the standard installation of the application.

Lesson 10: Assess the compatibility of the cloud provider’s standards

CHALLENGE: Organizations may not be able to control their technological strategy if the CSP has standards that are incongruent or incompatible with the organization’s standards.

Organizations should analyze the compatibility between their internal standards and the standards of the CSP. These include technical, governance and even language standards that the organization wants the CSP to adopt. For example, CSPs that only provide service and support in English can cause difficulties for Canadian organizations with bilingual requirements. Additionally, organizations should recognize that there is a risk that the CSP will move away from the standards it currently has in place.

Lessons learned: One organization highlighted how the issue of standard incongruence with its CSP impacted its internal practices. Specifically, the CSP no longer supported the version of the web browser used by the organization and gave it a few months’ notice to migrate to a new browser in order to keep using the cloud-based application. The organization had applications that were built off the current version of the browser, so it had to configure a way to keep its legacy applications operating on the old browser while moving to the new browser. Ultimately, it had to develop a complex workaround to use both versions of the browser.

The same organization also had to re-evaluate its data standards (the format and structure of data). The organization had adopted the data standards established by the CSP in order to exchange data with the cloud-based application. This meant that IT and individual departments had to ensure their current data standards were appropriately migrated to the data standards prescribed by the CSP.
In terms of governance standards, one organization implemented Information Technology Infrastructure Library (ITIL) internally, but the CSP did not. Consequently, it had to grant the CSP an exemption when complying with ITIL and accommodate the IT service standards adopted by the CSP instead.

With respect to language, one organization was able to anticipate a potential standard incongruence and contractually required the CSP to provide the application and associated supporting materials in both English and French. However, the vendor had difficulties providing the materials in French because of translation errors. Although this problem was eventually resolved, it is important to note the requirements upfront and conduct the necessary testing before the application goes live. In this case, the organization was able to obtain service credits for the disruption of service this issue caused.

It is important to perform an analysis of standard congruence to ensure there is alignment between the organization and CSP and to specify in the contract the need for the CSP to comply with the organization’s standard. The organization must also assess the impact of the CSP adopting a new standard in the future, such as a new version of the web browser, and how such a situation will be handled.
Is Moving to the Cloud Worth It?

Cloud computing can be a challenge, especially for organizations with a mature technological infrastructure. In summary, organizations need to:

- **Treat cloud computing as a capital project:** Moving to the cloud needs to be managed like any other capital project, such as proper scoping of project objectives, ensuring key stakeholders are engaged, conducting a formal request for proposal, etc.

- **Protect and secure access to organizational data:** Organizations need to ensure the CSP protects their data from changes in ownership, software failure, etc. In addition, organizations need a plan to get their data off the cloud and be able to use the data within their own environment.

- **Understand integration challenges:** Bringing a cloud solution into a complex computing environment requires careful planning to ensure that all the integration challenges are identified and that the organization is aware of the amount of time and money required to deal with these challenges.

Not every cloud computing implementation will have a beneficial impact on the business, but many organizations do find that there is a positive ROI when moving to the cloud. However, this can take several years to achieve: one organization noted that it took four years before it saw a positive return on investment. Like any business decision, the advantages and challenges need to be weighed properly. The organizations interviewed were able to overcome the challenges identified and still have a positive net return on investment. Cloud computing is like any other technology: it has benefits and risks that need to be managed effectively.
Appendix: Security Issues Related to Cloud Computing

Assessing the Security Risks of Moving to the Cloud
Security risk remains top of mind when considering the cloud. Moving to the cloud moves confidential information to an environment outside the organization’s firewalls and into a shared environment, which leaves organizations dependent on the controls implemented by the cloud service provider (CSP). However, organizations have been outsourcing for decades—well before cloud computing was on the radar. Cloud computing is essentially a form of outsourcing, which means control of the application is handed over to a third party. It is important to distinguish between risks that are particular to cloud-based systems and those for on-premise systems. For example, cloud-based systems and on-premise systems need to have IT controls to authenticate users to access the system, but the difference is in how this will be accomplished.

What Are the Security Risks with Cloud Computing?
Two characteristics of the cloud are its multi-tenant architecture and its ability to dynamically allocate resources in an automated manner. This is what distinguishes the cloud from traditional IT outsourcing, where a dedicated physical server would be maintained on behalf of the customer.

Consequently, there are three key risks that are unique to cloud computing: shared access, anonymous access, and data ownership and confidentiality.
Shared Access
Cloud computing leverages a shared environment to deliver IT to its customers, which means that the customers are sharing an environment with others. There is a risk that one customer can accidentally access another customer’s data. For example, customers who subscribed to Microsoft’s hosted Business Productivity Online Suite (BPOS) were able to access the offline address books of other customers “in a very specific circumstance.”

Anonymous Access
In the traditional IT outsourcing scenario, the IT outsourcer would screen each customer through the contracting process. Consequently, it would be very difficult for a hacker to masquerade as a customer to gain access to the IT outsourcing company’s facilities. However, to gain access to a CSP’s environment, a potential malicious user only needs a valid credit card to anonymously gain “tenancy.” 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. 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 CSPs being breached by malicious hackers. However, security researchers were able to exploit vulnerabilities in Amazon Web Services to “see” what was going on in the co-tenant’s virtual machine.

Data Ownership and Confidentiality
Prior to the cloud, organizations who outsourced their IT would have legal counsel involved in drafting the agreement with the IT service provider, which would enable the organization to put a clause in the agreement that would force the IT service provider to obtain permission before disclosing its data to anyone, including law enforcement agencies. With cloud computing, the service agreements are standardized and can effectively provide warrantless access to an organization’s data. In particular, Canadian companies may be concerned about cloud servers located in a jurisdiction outside of Canada, as the data would then be accessible to the law enforcement of that country. For example, if the server of the CSP were located in the United States, then data would be subject to the USA PATRIOT Act. The USA PATRIOT Act enables “U.S. law enforcement officials and intelligence agencies to demand that an organization or entity hand over stored records or data without a court order.”

However, the reach of the USA PATRIOT Act is not limited to servers located in the United States. As noted on the Government of Canada website, “When a supplier is hired to administer personal information and any part of its operations, including subcontractors, are outside of Canada, then the laws of the other country (or countries) may be applicable to information stored or accessible electronically in the foreign country. If a company located in the United States or with U.S. connections is hired, then the USA PATRIOT Act may be applicable.” A Canadian organization with US connections is potentially subject to the provisions of the USA PATRIOT Act, although the Canadian government says “chances of this happening are
remote.” Furthermore, Canadian law enforcement can also access data stored on any system (including those owned by CSPs) without a warrant or the consent of the organizations that own the data.

Even though organizations may be comfortable using cloud services in other countries, their customers may not be, as highlighted by a complaint made to the Canadian privacy commissioner by customers of CIBC regarding the bank’s outsourcing of credit card processing to the U.S. The CIBC’s customers did not like the idea that the U.S. government could potentially monitor their data. The Canadian privacy commissioner dismissed the complaint because CIBC had given its customers notice that U.S. law enforcement might access their data. From a privacy perspective, as long as the organization is “transparent” and gives notice to its customers that the information “may be accessed by the courts, law enforcement and national security authorities,” then they are in compliance with privacy laws. Before moving to a CSP outside of Canada, organizations should consider the risk of potentially losing customers who are not comfortable with this change and would rather keep their data off the cloud. Although this applies at the federal level, some provinces have other restrictions. In British Columbia, public bodies are prohibited from storing information outside of Canada unless they get consent to do so. Nova Scotia also contains similar prohibitions, but allows storage outside of Canada if “the head of a public body, or the responsible officer of a municipality, determines that it ‘meets the necessary requirements’ of the organization’s operation” and reports the reasons to the Minister of Justice. Organizations should be aware of their province’s restrictions to ensure they comply.

Evaluating the Risk of Cloud Computing on IT General Controls
Regardless whether the application is in the cloud or on-premise, organizations need to ensure that there is an adequate level of control to safeguard against the risk of logical and physical unauthorized access. Organizations should perform a mapping exercise to see what information security controls are in place on-premise and ensure that there is, at a minimum, the same level of IT controls in place for their cloud services. Take patching, for example, organizations need to ensure that they have a policy to patch all their different systems (e.g., Microsoft, Oracle, Linux, SAP, etc.) in the cloud, just as they would on-premise.

With respect to the authentication, in an *InfoWorld* article Roger Grimes notes how configuring single sign-on (SSO), privileged administrator accounts, and sharing of private keys can impact the risk that an organization faces when using the cloud. As noted in Lesson 5, even where the CSP can accommodate the authentication mechanism it can be a challenge to implement. That is, achieving the same level of security in the cloud as in-house could require more resources to implement, especially where the organization needs to integrate the cloud computing application into its infrastructure or have a high level of security controls (e.g., two-factor authentication of employees who remotely access the organization’s computing environment). Organizations should also assess the added security risk that they are taking because of the additional management of such a complex environment.
Putting Security in Perspective

Not everyone agrees that cloud computing poses a greater security risk than on-premise solutions. The counterargument is that large CSPs will have state-of-the-art security since it is of strategic importance to their business. In the infoWorld article Grimes states: “Although it may sound as if I’m down on public cloud computing, I’m actually a huge fan of it. I believe that most public cloud vendors do a far better job securing data than their customers do.” To add to this argument, one could point to the fact that salesforce.com has experienced only one known security breach, which was attributed to human error rather than a sophisticated attack launched by hackers.

Regardless of whether the system is located in the cloud or on-premise, IT general controls require the appropriate configuring of special privileged administrator access, cryptographic key management, patch management, disaster recovery, risk management, etc. In other words, organizations need to have controls in place regardless of whether the solution is at the CSP or in-house. To mitigate risks, organizations need to determine what assurance the CSP 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 with the CSP.