CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Cloud Computing

TECHNOLOGY SPOTLIGHT

"The cloud is about how you do computing, not where you do computing."

—Paul Maritz, former CEO of VMware and Pivotal

While moving to the cloud could change the geographic location of where the computing services are provided, that is not what cloud computing is truly about. Cloud computing changes the way computing services is delivered to enable faster innovation, flexible resourcing, and economies of scale. These benefits are examined in further detail below.

Description

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." Simply put, cloud computing is a resource-provisioning model that allows for the delivery of on-demand computing resources over the Internet and a business model that often allows a pay-for-use basis. It is important to note that "the cloud" is not a unitary service. While there are many commercially available cloud computing environments and they each have their own unique qualities, the NIST has identified five essential characteristics[1] that define cloud computing:

1. **On-demand self service**
   Computing resources can be unilaterally provisioned by businesses without human interaction with a cloud service provider.
2. **Broad network access**
   Computing resources are accessible over standard networks across various client devices (e.g., phones, tablets, desktops, laptops).

1 The NIST Definition of Cloud Computing - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3. **Resource pooling**
   Computing resources are pooled to serve multiple businesses; resources are assigned dynamically to each business based on demand.
4. **Rapid elasticity**
   Computer resources can be scaled up and down rapidly commensurate with demand.
5. **Measured service**
   Computing resource usage can be monitored, controlled, and reported.

Cloud computing involves the use of the Internet combined with the provision of a range of services, such as:

- SaaS (Software as a Service) provides users with application software.
- PaaS (Platform as a Service) provides users with a computing platform or solution stack.
- IaaS (Infrastructure as a Service) provides a virtualized platform combined with storage and a network.

Importance

Cloud computing offers businesses cost-effective means of acquiring access to hardware, software, communications and processing capacity on a need-to-use basis. Cloud computing's main advantages are flexibility and scalability. It can help businesses accelerate the rollout of innovative functionality and removes high capital costs as a barrier to growth.

According to a Better Cloud report,[2] 73% of organizations plan to move nearly all their apps to a SaaS model by 2020 as many vendors are shifting development from on-premise software to the cloud. Despite the popularity of the cloud, it may not be the appropriate solution for all organizations. It is important to assess the related considerations and risks prior to moving to the cloud. Large Enterprise Resource Planning (ERP) vendors continue to offer on-premise solutions for organizations that prefer that option.

Business Benefits and Considerations

The benefits of employing cloud computing include:

- Computing resources are "rented" to meet varying requirements over time.
- The cloud service provider looks after managing the data centre infrastructure, including upgrades, security, and technology changes, which allows the entity to focus on its business.

2 www.bettercloud.com/monitor/wp-content/uploads/sites/3/2017/05/2017stateofthesaaspoweredworkplace-report-1.pdf

- Agility is improved by faster access to new software functionality.
- By its nature, the cloud creates off-site storage, thereby providing availability in case of a disaster at the business premises.
- Data and processing capabilities can be accessed from multiple locations.
- Specialized technology is available that can be readily accessed through the cloud (e.g., chatbots).
- There is greater ability to integrate and connect with technology solutions from both inside and outside the organization to facilitate movement of data from disparate systems and enable an ecosystem of interconnected applications.

However, it may also create risks around security, privacy, availability and continuity.

- **Security**
  The cloud is a big target due to the concentration of data from many customers. In 2017, data on 14 million Verizon customers was exposed due to an unsecured Amazon Web Services Storage server. Moving to the cloud does not eliminate the need for sound security practices such as cryptography (particularly public key infrastructure), strong passwords and multi-factor authentication, and firewalls.
- **Privacy**
  Additional care must be taken to ensure cloud providers protect the privacy of information processed or stored in the cloud.
- **Compliance**
  This includes legislation, regulation and industry requirements restricting where the data in the cloud must physically reside, the type of cloud that can be employed, or the specific security techniques that must be implemented.
- **Legal**
  Legal issues such as trademark infringement, security concerns and the sharing of proprietary data resources may arise.
- **Reliability**
  While cloud services are generally robust and include multiple redundancies, recent events have shown that even the largest cloud service providers are not immune to downtime. In 2007, Amazon Web Services went down for three hours due to an employee error. As a result, it was estimated the cost of that downtime to companies in the S&P 500 was approximately US$150 million.[3] Therefore, for mission-critical activities, it may be worthwhile to consider the use of multiple cloud providers.

3 www.npr.org/sections/thetwo-way/2017/03/03/518322734/amazon-and-the-150-million-typo?t=1529930367722

Managers must understand the risks each specific cloud computing environment represents and change their practices to address such risks. At the same time, IT functions will need to place a greater emphasis on vendor management to help with risk mitigation. These risks may include not knowing where data is stored; whether data is adequately protected; whether the service provider may subcontract to another party who may lack the controls of the original contracting party; or whether the third-party vendor may change or upgrade the software, forcing the business into expensive changes, upgrades and conversions. The following table summarizes the potential risk areas and mitigation strategies for cloud computing.

Risk Areas	Risk Mitigation Strategies
Businesses may not know the current location of their data or where it will eventually be stored.	• Ensure the service agreement clearly indicates data location or geographic region. • Require prior written consent or advance notice to change it.
Certain information stored in the cloud may be stored in contravention of Canadian laws, industry standards or contractual obligations of the business.	• Provide the cloud service provider with specific requirements for data storage. Alternatively, go with a large cloud service provider that offers Canadian data centres as an option to help meet data residency requirements. • Require the cloud service provider to agree to specific requirements in a contractual agreement. • Require the cloud service provider to provide a third-party assurance report (e.g., SOC 2 report) on security and, if needed, privacy and compliance with contractual obligations.
Information in the cloud may not be adequately protected.	• Specify security and protection requirements. • Specify any standards that must be met (e.g., ISO 27001/2, COBIT, PCI). • Require the cloud service provider to agree to specific requirements in a contractual agreement. • Require the cloud service provider to provide a third-party assurance report (e.g., SOC 2 report) on security and, if needed, privacy and compliance with contractual obligations.
Information and files belonging to the cloud service provider's customers are not adequately separated.	• Require the cloud service provider to ensure separate devices for storage of critical data. • Encrypt all business data stored in the cloud.

Issues can arise when outsourcing specific IT functions to a third-party cloud service provider. **The reliance placed on the third party's various IT functions, including security and privacy, may not be adequately identified or addressed.**	• Contract only with known viable and reputable cloud service providers. • Clarify the demarcation between the business's processes and technologies (i.e., computer and network) and the cloud service provider's technologies and responsibilities, and ensure the business's internal controls work up to the demarcation point. • Ensure the policies, procedures, business processes and technology solutions employed by the service provider meet the requirements of the business.
Companies may no longer need to own or license application or systems software, rather they can rent software over the Internet as a service (SaaS) as needed. **Rented software may not be sufficiently suitable for the company's functionality, security or performance needs.** **The cloud provider may not be willing to modify the software to meet the specific needs of one or two customers.**	• Identify key business requirements that must be met and use these in determining the suitability of potential cloud service providers. • Re-engineer business processes to conform to the SaaS model as much as possible to reduce costs and customization. • For unique business process or technical requirements ascertain whether the cloud service provider can accommodate the specific business requirements economically or if the cloud service provider could re-design its service offerings (i.e., processes and technology) to effectively support the business needs. • Consider modifying the in-house business processes and technology to provide a more effective interface with the cloud service provider. • Assess the risks of maintaining non-standard service requirements, particularly when the cloud service provider changes or upgrades technology.
In "buying a service", the business may not be fully aware of the risks it is undertaking.	• Include technology and business risk as part of the assessment of the use of any technology-based or technology-reliant service. • Ensure the business has the right to audit the service provider's security initiatives and activities. • Contractually require the cloud service provider to supply a third-party assurance report on controls that addresses financial, operational and/or regulatory risk. • Contractually require the cloud service provider to disclose breaches and remediation activities on a timely basis.

Risk Areas	Risk Mitigation Strategies
The business may not be aware of the cloud service provider's business continuity and disaster recovery plans. **The cloud service provider's business continuity and disaster recovery plans may not be able to resume or recover within the service needs of the business.**	• Perform extensive due diligence supported with contractual service and recovery provisions. • Monitor service and compliance levels through the cloud service provider's reporting and/or audit provisions within the contract. • Communicate annually the business needs and expectations and modify the contract if necessary.
The cloud service provider may rely on third parties such as telecommunication providers and may not have access to their BCP/DRP information.	• Ensure that re-outsourcing or use of third parties can be effectively assessed by the cloud service provider.
Difficulty may occur when retrieving data and files should the business cancel the services of the cloud service provider. **There may be difficulty in ensuring all business files and information have been deleted by the cloud service provider should the business cancel the service.**	• Identify and document an exit strategy as part of the business case to move data, processing or support to a cloud service,. • Identify the contractual requirements to ensure the exit strategy will work. • Ensure the exit strategy requirements are negotiated in the contract and ensure the cloud service provider continues to adhere to those requirements.
Moving to a cloud service provider may lock the business into that cloud service provider because it may be difficult or costly to leave.	• Identify and document the minimum technology requirements as part of the business case to move data, processing or support to a cloud service. • Avoid vendor-specific technology or software unless it is widely available from other sources. • Identify and negotiate requirements to ensure the cloud service provider is contractually bound to maintain current versions of the technology and software as well as support prior versions. • Document an exit strategy and determine whether the cloud service provider's offerings will meet the exit-strategy requirements.

There may be a lack of incident identification, escalation, remediation and reporting.	• Assess the cloud service provider's monitoring procedures and its identification and treatment of incidents, particularly those involving security, privacy, availability and continuity, prior to contracting. • Ensure the cloud service provider has sufficient qualified incident-support personnel. • Negotiate incident reporting criteria into the contract. • Monitor the cloud service provider's performance in addressing incidents, identifying their causes and implementing solutions.
The cloud service provider does not provide information on security and privacy.	• Stipulate in the contract that the cloud service provider must provide a third-party assurance report on the operational effectiveness of the cloud service provider's controls.

Conclusion

Cloud computing brings many benefits and is an important part of any digital strategy. However, businesses need to understand the potential risks so that they can enact appropriate mitigation strategies to protect their reputation and secure their data in the cloud.

This publication is part of the **Technology otlight series**.

The entire series covers technology trends that impact CPAs and are available on our website.