CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Cloud Computing

TECHNOLOGY SPOTLIGHT

Defined by The National Institute of Standards and Technology as "the provision of computational resources on demand via a computer network," cloud computing's advantages are flexibility and scalability.

However, it creates risks in security, privacy, availability and continuity. Surveys show that businesses are turning to the cloud as a means of accelerating the rollout of functionality to support business units while saving money.

While cloud computing may have many benefits, it comes with a financial and a business cost in terms of:

- **Privacy**—additional care to ensure that cloud providers protect the privacy of information processed or stored in the cloud.
- **Compliance**—legislation, regulation and industry requirements such as those of the payment-card industry may preclude the use of cloud services, may restrict the type of cloud that can be employed or require specific security techniques be implemented.
- **Legal**—such issues as trademark infringement, security concerns and the sharing of proprietary data resources may arise.
- **Security**—a contentious issue that may be delaying adoption of cloud computing, due in large part to the private and public sectors' unease about the external management of services and concerns over co-mingling of proprietary data among multiple users. Solutions vary from cryptography, particularly public key infrastructure, to the use of multiple cloud providers, and legal support.

This publication was originally published by The Canadian Institute of Chartered Accountants in 2012.
It has been reissued by Chartered Professional Accountants of Canada.

- **Sustainability**—of the financial and technological models of the cloud providers.
- **Abuse**—the cloud service provider is a big target for organized crime hackers due to the concentration of data from many customers. Individuals posing as legitimate customers can purchase cloud computing services for nefarious purposes. In 2009, a banking Trojan illegally used the popular Amazon service as a command and control channel that issued software updates and malicious instructions to PCs that infected them with malware. Businesses don't want to be inadvertently connected or associated with such activities.

According to an Information Week analytics survey, the drivers to adopting a SaaS model were speed to implementation, 3.9 (out of a maximum rating of 5); savings on capital expenditures, 3.5; and savings on operating expenses, 3.4.

Managers must be cognizant of the cloud's risks, including 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.

Description

Cloud computing is the use of the Internet and virtualization concepts to create an environment in which individuals and organizations can acquire storage and processing capacity.

The cloud 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

Conceptually cloud computing is not unlike service bureaus popular in the 1970s and 1980s. Cloud computing provides varying levels of technology services on a pay-for-use basis. Two areas must be assessed: technical and business.

- Business issues are concerned with the viability, financial stability, past performance and other matters that one would consider in entering any business relationship.
- Technical issues are concerned with meeting the company's functionality, security and performance needs.

Cloud computing offers businesses cost-effective means of acquiring hardware, software, communications and processing capacity on a need-to-use basis.

Business Benefits

The benefits of employing cloud computing include:

- Computing resources are "rented" to meet varying requirements over time;
- The business only purchases the resources it needs, and does not have to acquire infrastructure and capacity for peak periods;
- The cloud service provider looks after managing the technology infrastructure, allowing the entity to focus on its business;
- 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;
- Technology changes and upgrades are taken care of by the cloud service provider.

Issues and Risks	Possible Mitigation
Businesses may not know the current location of their data or where it will eventually be stored.	Request the proposed cloud service provider provide a third-party report covering its security, controls, availability and privacy initiatives.
The cloud service provider may re-outsource processing capacity, online storage or archiving of business information and thereby: • **Lessen the security, availability or protection of the business's information;** • **Violate laws and regulations governing personal information;** • **Violate contractual obligations between the business and its customers;** • **Create difficulties in retrieving business data if the sub-outsourcer encounters technical or financial difficulty.**	Ensure that any agreement between the businesses either: • Precludes re-outsourcing; or • Prior to re-outsourcing, the business must approve the re-outsourced business; and • The business has the option and ability to reverse its decision to allow re-outsourcing. The business should obtain a copy of an independent third-party report on the security, control, availability, privacy policy procedures, technology solutions and their operating effectiveness.
Certain information stored in the cloud may be stored in contravention of Canadian laws, industry standards or contractual obligations of the business.	Business to provide cloud service provider with specific requirements for data storage. Cloud service provider should agree to specific requirements in a contractual agreement. Cloud service provider to provide a third-party report on security and, if needed, privacy and compliance with contractual obligations.

Issues and Risks	Possible Mitigation
Information in the cloud may not be adequately protected.	Business to specify security and protection requirements. Business to specify any standards that must be met (e.g., ISO 27001/2, COBIT, PCI). Cloud service provider should agree to specific requirements in a contractual agreement. Cloud service provider to provide a third-party 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 resulting from 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 (computer and network) and the cloud service provider's technologies and responsibilities, and ensure that the businesses' internal controls work up to the demarcation point. Ensure that 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 but, rather, they can rent software over the Internet as a service (SaaS) on an as-needed basis. **Software rented 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 if the cloud service provider can accommodate the specific business requirements economically or if the cloud service provider could re-design its service offerings (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. Determine how temporary bridges (APS) could be developed and maintained over time. Assess the risks of maintaining non-standard service requirements, particularly when the cloud service provider changes or upgrades technology.

Issues and Risks	Possible Mitigation
In "buying a service" the business may not be fully aware of the risks that 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 audit report on controls that addresses financial, operational and/or regulatory risk. Contractually require the cloud service provider to disclose breaches; such disclosures must be on a timely basis.
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 in retrieving data and files should the business cancel the services of the cloud service provider. **Difficulty in ensuring that all business files and information have been deleted by the cloud service provider should the business cancel the services of the cloud service provider.**	As part of the business case to move data, processing or support to a cloud service, identify and document an exit strategy. 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, as it may be difficult or costly to leave.	As part of the business case to move data, processing or support to a cloud service, identify and document the minimum technology requirements, and 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 supporting prior versions. Document an exit strategy and determine if the cloud service provider's offerings will meet the exit strategy requirements.

Issues and Risks	Possible Mitigation
Lack of incident identification, escalation, remediation and reporting.	Prior to contracting assess the cloud service provider's monitoring procedures and its identification and treatment of incidents, particularly those involving security, privacy, availability and continuity. Ensure the cloud service provider has sufficient qualified incident- support personnel. Contractually negotiate incident reporting criteria and 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 an SSAE 16 (Handbook 3416) Type II assessment with a list of the controls and an assessment of their operational effectiveness.