HANIF SHAMJI, MBA, CPA, CGA
CHARTERED PROFESSIONAL ACCOUNTANT
FINANCE BUSINESS PARTER -
OPERATIONS AND STRATEGY PROFESSIONAL

# Cloud Computing Considerations Part II – May 26, 2015

With the trend towards clouding, companies will increasingly need to consider security issues surrounding their cloud infrastructure. Organizations will need to adopt a strategy that considers innovation, mobility, and analytics. There are a variety of cloud models that includes private, and public cloud patterns, which allows an organisation to focus on growth while enabling it to improve security protocols. The usage of cloud computing is expected to grow as companies use it to supplement their IT infrastructure.

**Types of Clouds**
As popularity of cloud computing increases, it is increasingly important to understand the types of cloud computing solutions that are available including;

- **Public Cloud** – such solutions are available over the Internet and are available for free or on a pay-per-use charge basis.
- **Community Cloud** – resources shared among organisations that share resources including similar security, compliance, and legal concerns.
- **Private Cloud** – cloud managed entirely for a particular organisation. Such a solution may be controlled internally, externally, or a combination of an external and internal solution.
- **Hybrid Cloud** – consists of two or more of the cloud solution types

**Before a cloud computing solution is implemented some considerations include:**

1. Determining the business requirements - How will the cloud solution provide benefits, how it will be an improvement over current processes, as well as addressing security, and compliance concerns.
2. Determine what type of devices will use and support the cloud solution.
3. How will access protocols be established and maintained?


 

4. How many users will use the cloud, what will be the cost? Where will they access cloud information from
5. How long will information be retained? Legal and regulatory requirements may have established legal requirements. As well consider how are access, update and retention logs maintained and created.

**Cloud Security**

Cloud providers need to address security and privacy concerns by providing access controls that authenticate users to mitigate the inherent risk of cloud computing. As well the use of hardware and software based controls may be used to prevent and detect unauthorised access levels to cloud services based on group access whereby related users share access.

Consider as an example, payroll solutions whereby payroll related data is processed and stored remotely anywhere in the world often referred to as hosted solutions; the risk associated with such information in light of PIPEDA and security concerns for the company. Cloud computing can be used to support services to an organisation at a lower cost; however, the risks will need to be evaluated and mitigated where possible.

**Due Diligence**

Due Diligence of data security does not end when the responsibility is handed over to a vendor. Questions including how the vendor addresses confidentiality, data protection, and who has access. Cloud providers may undergo a security audit. In some situations, a copy of the supplier's security check. If it is not possible to get a copy of the audit, a review of who undertook the examination, the deficiencies found, the methodology used, as well as the scope the audit.

A cloud service provider could be a target for hackers, which could put organisational information at risk. A large number of security breaches are not often noticed immediately and took days or weeks to see. This is a concern as if companies are not tracking the impact of security breaches in real time they won't be able to take a proactive approach to protect organizationally, or client data. As the complexity of safety concerns increase, it may be necessary to leverage on the expertise of others to mitigate potential risks that may exist.

Even with the development of well-intended security policies and procedures without an awareness of information security they could for example download software on their computer which can be a critical point in the weakness of the internal organisational network and its ability to provide defences from data breaches. This can be especially important in industries, which are highly regulated and have sensitive information such as financial services, and healthcare. Organizations that build a robust security framework, which is backed by ongoing employee awareness, will go a long way in assisting with security concerns.

**Document Version Tracking**

The cloud solution should offer document version tracking this is often useful when several people are working on the same document at a time. A log is kept to track changes made to the file and offers the ability to roll back to a prior version. The use of accessing files via a cloud-based network can also assist in preventing problems associated with broken links in Excel files, which can corrupt data, or not be able to have information relevant information from source files updated as required.
Various solutions can be used to host the sharing of cloud-based data such as SharePoint. Consider when selecting a host solution how will productivity be improved for staff within the office, as well as those that are mobile. Security and internal controls should be a major factor in selecting a hosting


 

solution. As well the net benefits regarding monetary and non-monetary value will need to be evaluated.

With the trend towards clouding, companies will increasingly need to consider security issues surrounding their cloud infrastructure. Organizations will need to adopt a strategy that considers innovation, mobility, and analytics. There are a variety of cloud models that includes private, and public cloud patterns, which allows an organisation to focus on growth while enabling it to improve security protocols. The usage of cloud computing is expected to grow as companies use it to supplement their IT infrastructure.

**Types of Clouds**
It is increasingly important to understand the types of cloud computing solutions that are available.

These include:

- **Public Cloud** – such solutions are available over the Internet and are available for free or on a pay-per-use charge basis.
- **Community Cloud** – resources among organisations that share resources including similar security, compliance, and legal concerns.
- **Private Cloud** – cloud managed entirely for a particular organisation. Such a solution may be controlled internally, externally, or a combination of an external and internal solution.
- **Hybrid Cloud** – consists of two or more of the cloud solution types

**Before a cloud computing solution is implemented some considerations include:**
1. Determining the business requirements - How will the cloud solution provide benefits, how it will be an improvement over current processes, as well as addressing security, and compliance concerns.
2. Determine what type of devices will use and support of cloud solutions.
3. How will access protocols be established and maintained?
4. How many users will use the cloud, what will be the cost? Where will they access cloud information from
5. How long will information be retained? Legal and regulatory requirements may have established legal requirements. As well consider how are access, update and retention logs maintained and developed.

**Cloud Security**
Cloud providers need to address security and privacy concerns by providing access controls that authenticate users to mitigate the inherent risk of cloud computing. As well the use of hardware and software based controls may be used to prevent and detect unauthorised access. Access levels to cloud services based on group access whereby related users share access.
Consider as an example, payroll solutions whereby payroll related data is processed and stored remotely anywhere in the world such as through hosted solutions; the risk associated with such information in light of PIPEDA and security concerns for the company. Cloud computing can be used to support services to an organisation at a lower cost; however, the risks will need to be evaluated and mitigated where possible.

**Due Diligence**
Due Diligence of data security does not end when the responsibility is handed over to a vendor. Questions including how the vendor addresses confidentiality, data protection, and who has access t. Cloud providers may undergo a security audit. In some situations, a copy of the vendor's security audit. If it is not possible to get a copy of the audit, a review of who undertook the audit, the deficiencies found, the methodology used as part of the scope the audit should be considered.

A cloud service provider could be a target for hackers, which could put organisational information at risk. A large number of security breaches are not


 

often noticed immediately and took days or weeks to see. This is a concern as if companies are not tracking the impact of security breaches in real time they won't be able to take a proactive approach to protect organizationally, or client data. As the complexity of security concerns increase, it may be necessary to leverage on the expertise of others to mitigate potential risks that may exist.

Even with the development of well-intended security policies and procedures without an awareness of information security they could for example download software on their computer which can be a critical point in the weakness of the internal organisational network and its ability to provide defences from data breaches. This can be especially important in industries, which are highly regulated and have sensitive information such as financial services, and healthcare. Organizations that build a robust security framework, which is backed by ongoing employee awareness, will go a long way in assisting with security concerns.

**Document Version Tracking**
Document version tracking is useful when several people are working on the same document at a time. A log is kept to track changes made to the file and offers the ability to roll back to a prior version. The use of accessing files via a cloud-based network can also assist in preventing problems associated with broken links in Excel files, which can corrupt data, or not be able to have information relevant information from source files updated as required. Various solutions can be used to host the sharing of cloud-based data such as SharePoint. Consider when selecting a host solution how will productivity be improved for staff within the office, as well as those that are mobile. Security and internal controls should be a major factor in selecting a hosting solution. As well the net benefits regarding monetary and non-monetary value will need to be evaluated.

**Internal Controls**
Review of your vendor's data security procedure undertaken even after an implementation of a cloud solution. It requires layered security policies managed through internal controls. Solutions are not one-time solutions but monitored given technological changes or pressures from both internal as well as external forces.

- Applying controls for the management of data
- Manage access and credentials
- Establish security policies for the organisation
- Protect and manage remote access

**Service Provider Responsibilities**
As well consider how a cloud computing service provider can fulfil responsibilities towards compliance related to privacy laws, and best practices. Consider how the service provider report security incidents that have occurred? Evaluate the internal controls of the service provider in light of the unique security concerns. In higher risk situations, continuous monitoring of the service provider may be necessary to ensure that it is maintaining adequate internal controls including appropriate plans and resources in place to ensure the continuity of operations if an unexpected disruption occurs.

Review of your vendor's data security procedure even after an implementation. It requires layered security policies managed through internal controls. Solutions are not one-time solutions but monitored given technological changes or pressures from both internal as well as external forces.

- Applying controls for the management of data
- Manage access and credentials
- Establish security policies for the organisation
- Protect and manage remote access

**Service Provider Responsibilities**

As well consider how a cloud computing service provider can fulfil responsibilities towards compliance related to privacy laws, and best practices. How does the service provider report security incidents? An evaluation of internal controls of the service provider light of the unique security concerns. In higher risk situations, continuous monitoring of the service provider may be necessary to ensure that it is maintaining adequate internal controls including appropriate plans and resources in place to ensure the continuity of operations if an unexpected disruption occurs.

***About the author:***
*Hanif Shamji, MBA, CPA, CGA* is a Finance Business Partner / Sr. Financial Analyst / Business Analyst with an information technology background, experienced in several industries.
Contact: info@hanifshamji.ca
http://www.hanifshamji.ca/


 