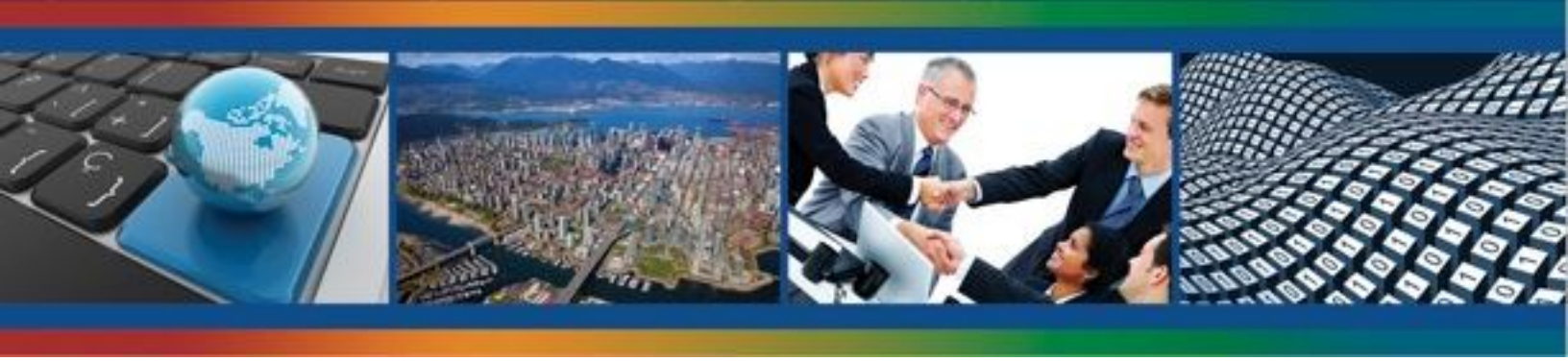


CANADIAN GEOSPATIAL DATA INFRASTRUCTURE
INFORMATION PRODUCT 20e

Primer on Policy Implications of Cloud Computing

Hickling Arthurs Low
Science & Technology Policy Research and Analysis Resource team

2012

Natural Resources Canada | Ressources naturelles Canada

Canada

Table of Contents

1. Preamble

This guide is one in a series of Operational Policy documents being developed by GeoConnections. This guide is intended to inform CGDI stakeholders about the nature and scope of cloud computing and the realities, challenges and good practices of related operational policies.

Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand. Computing clouds provide computation, software, data access, and storage resources without requiring cloud users to know the details of the computing infrastructure. For geospatial data and software providers, cloud computing represents a potential new way of doing business, by providing lower cost or free options for clients to access products and services online. Rather than acquiring software for in-house implementation and downloading complete databases, clients can "rent" the software and access only the data they need through web services, on an as-required basis. The "cloud" is poised to become the accepted place for a broader range of relatively unsophisticated users of geospatial data to access and use this powerful technology.

The **GeoConnections** *program is a national initiative led by Natural Resources Canada. GeoConnections supports the integration and use of the* **Canadian Geospatial Data Infrastructure (CGDI).**

The **CGDI** *is an on-line resource that improves the sharing, access and use of Canadian geospatial information – information tied to geographic locations in Canada. It helps decision makers from all levels of government, the private sector, non-government organizations and academia make better decisions on social, economic and environmental priorities.*

Moving to the cloud seems inevitable. A Cloud Computing Roadmap is an integral component of the Government of Canada's information technology shared services (ITSS) model (Danek, 2010). Shared Services Canada is responsible for the delivery of certain IT services on behalf of all government departments, including data centre management. At the provincial level, at least two governments are assessing cloud computing (CC). The Government of Ontario is exploring the potential of CC as a better way of using and delivering online services (Microsoft, 2011). And in its IM/IT strategy document, the Government of British Columbia identifies the leveraging of CC services as one of two key IT/IM hosting strategies for the province (Office of the Chief Information Officer, 2011).

In an international example, the US federal government has introduced a "cloud-first" policy for new government computing solutions (Zients, 2010). American adoption estimates across all sectors peg growth in spending for managed cloud services at $14B by 2014 compared with $3B in Feb 2011. According to a Financial Times article in May 2011, the global value of the cloud sector could reach $150B by 2014. Other estimates differ, but all agree that cloud computing is becoming a significant business. A growing number of organizations already on the cloud further reflect this trend.

This guide introduces key issues in geospatial operational policy, imperative to the success of any venture into cloud computing. Operational policies are the guidelines, directives and policies that an organization employs to address the life cycle of geospatial data (i.e., collection, management, dissemination and use).

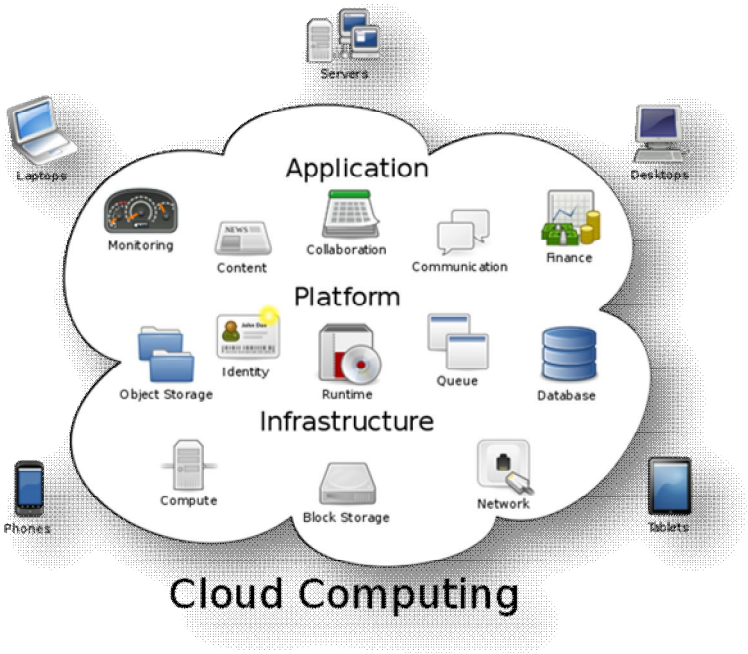
This guide will be of interest to anyone seeking a better understanding of cloud computing and areas of related operational policy, such as liability, privacy and confidentiality, security, licensing, copyright, archiving, regulations and standards.

2. An Introduction to the Cloud

2.1 Cloud Computing

Recognized as one of the foremost experts on CC, the US 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 (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mel & Grance, 2011). Figure 1 illustrates the components of cloud computing from a functional perspective. End users can access cloud based specialized applications (e.g., GIS software) through a web browser or a light weight desktop or mobile app while the more general business software and data are stored on servers that are part of the infrastructure at a remote location. Applications developers within the user organization can use the platform services of programming languages and tools to develop their own customized applications. In addition to data storage, the infrastructure provides computing or processing and network components.

Figure 1: Cloud Computing Functional model



Source: Wikimedia Commons

2.2 Cloud Computing Service Classes

Cloud computing today manifests in one of four different classes of service: infrastructure, platform, software and data.

- *Infrastructure as a Service (IaaS)* provides computing resources like processing, storage, and networks. Clients select what computing resources they need. As their need changes, the cloud service responds. The same infrastructure (storage, processing, memory, network, and virtual machines) is shared among all clients and, typically, the physical location of the resource is irrelevant to the client. A well known example is the Amazon Elastic Compute Cloud (EC2).
- *Platform as a Service (PaaS)* provides an environment for organizations to create and deploy applications using programming languages and tools supported by the provider, along with the Infrastructure needed for that deployment. Microsoft Azure Engine and Google App Engine are notable examples.
- *Software as a Service (SaaS)* provides clients with access to online business application(s) that come with the infrastructure to support them. Salesforce.com and the Esri ArcGIS and the cloud implementation are examples.
- *Data as a Service (DaaS)* is typically implemented within a SaaS, PaaS or IaaS solution and provides (often spatial) data within applications that support data discovery, access, manipulation, and use. For Geospatial Cloud Computing, DaaS components are typically essential, since most clients need base spatial data – such as Google Maps and/or more specific boundary and thematic mapping – for their business applications. One example is Pitney Bowes Data Insight's Data Market.

The four classes of service above intersect or overlap, and in many cases the actual service acquired will have components of more than one class, as illustrated in Figure 2. For instance, the Province of Ontario's GeoPortal provides various ministry business units with IaaS, SaaS and DaaS, but not PaaS. In other words, the Ontario GeoPortal provides the technology infrastructure for the business systems, a suite of standard software tools for data access and integration, and a significant amount of spatial data and services from a variety of sources. It is not, however, a "platform" with tools and widgets for the creation of new cloud-based applications.

Figure 2: Cloud Computing Service Models

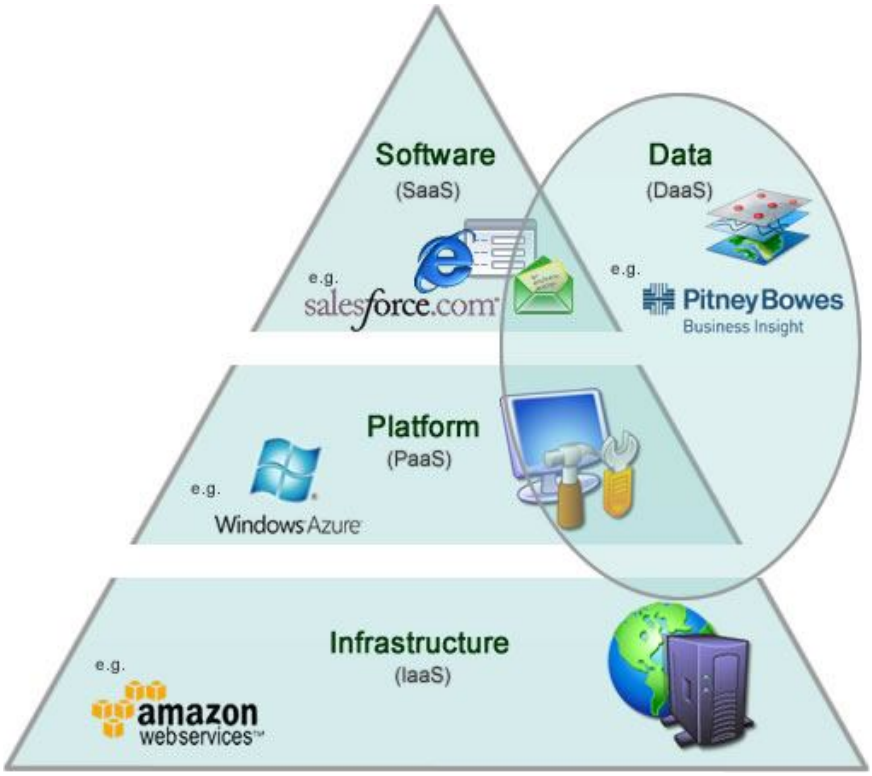


Figure 3 illustrates the broad range of CC service providers in the market today. These companies represent a cross section of the IaaS, PaaS, SaaS and DaaS players in cloud computing services. They include some of the best known companies in the information technology sector, plus companies in the geospatial information sector that have moved their software and data into the cloud.

Figure 3: Examples of Cloud Computing Service Providers

2.3 Cloud Computing Deployment Options

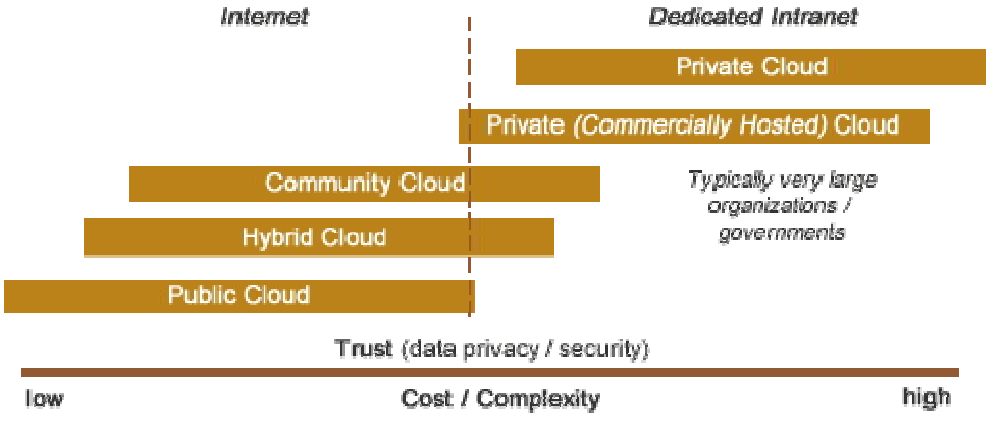
Cloud solutions are deployed in one of four ways: public cloud, private cloud, community cloud, or hybrid cloud.

- *Private cloud.* The cloud infrastructure is operated solely for one organization, on premise or off premise, and may be managed by the organization or a third party.
- *Community cloud.* The cloud infrastructure is shared by several organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations), on premise or off premise, and may be managed by the organizations or a third party.
- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud.* The cloud infrastructure is composed of two or more clouds (private, community, or public) that are bound together by standardized or proprietary technology that enables data and application portability.

Most cloud service providers offer their services in a public cloud scenario, with cost of private cloud options being significantly higher because they require an isolated and dedicated infrastructure. As a result, private clouds are typically only implemented by large organizations, such as a government department.

Figure 4 illustrates the types of Cloud Computing deployments and their associated levels of "trust", from data privacy and security perspectives, and the relative cost and complexity levels – in both cases going from low to high. Solutions on the left are Internet-based, and those on the right reflect an increasing reliance on private or dedicated Intranet implementations.

Figure 4: Cloud Computing Deployment Options



Some cloud solutions, such as the Ontario GeoPortal, offer a "distributed architecture" enabling client data that are too sensitive or otherwise cannot be implemented in the cloud outside the organization's firewall to still be integrated within the overall cloud solution.

In other words, there are multiple models and deployment options available to meet an organization's technical needs and security tolerance.

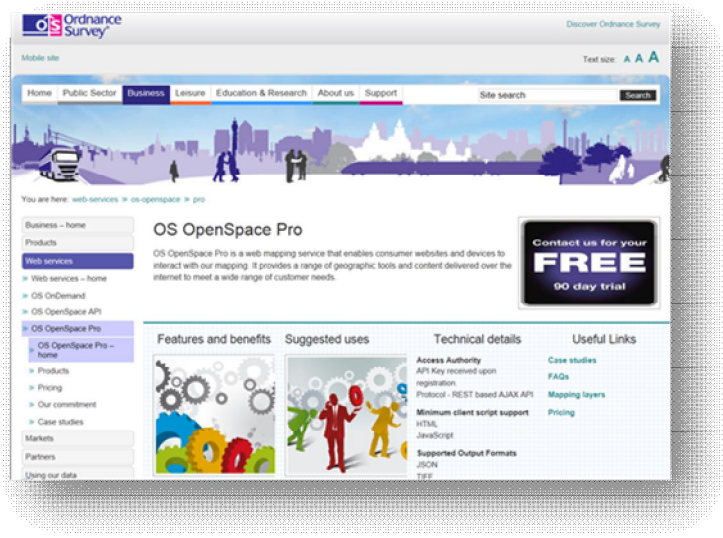
2.4 Geospatial Cloud Computing

A general term for the use of cloud computing in the geospatial information domain is geospatial cloud computing (GCC), which can be considered a cloud service that incorporates maps and the use and manipulation of spatial data. One typical difference between GCC and CC is its incorporation of spatial data.

GCC is helping popularize and enable the use of maps and geospatial data in business systems, as is demonstrated for example, by Google Earth and the Ontario GeoPortal example discussed in the next section. Cloud-based solutions open the door to a much broader audience and a faster and less costly implementation than a "traditional" enterprise GIS implementation (Ontario GeoPortal, 2011). For a detailed comparison of geospatial cloud and enterprise GIS solutions (e.g., applications and tools, computing infrastructure, content, security, costs, etc.), see Appendix 4.

2.5 Cloud Computing in Use

Two case studies – the Ordnance Survey in Great Britain and the Ontario GeoPortal – were conducted as part of the research for this primer. Lessons learned from these two case studies are incorporated into this primer.



Ordnance Survey GB is the National Mapping Agency of Great Britain. Since April 2010, Ordnance Survey has made a range of mapping data available for free to foster innovation and encourage government transparency. Ordnance Survey makes significant use of cloud computing as part of its online web mapping services, which serve Ordnance Survey's mapping data directly into customer websites or enterprise systems. Ordnance Survey chose to host these services on the public Amazon Web Services (AWS) platform, and is currently the largest UK public sector user of AWS. The experience with Amazon has led Ordnance Survey to also re-evaluate how they operate their internal data centres. Ordnance Survey has recently initiated a consolidation project that aims to use commodity hardware and virtualisation to build a more efficient private cloud infrastructure within their data centre.

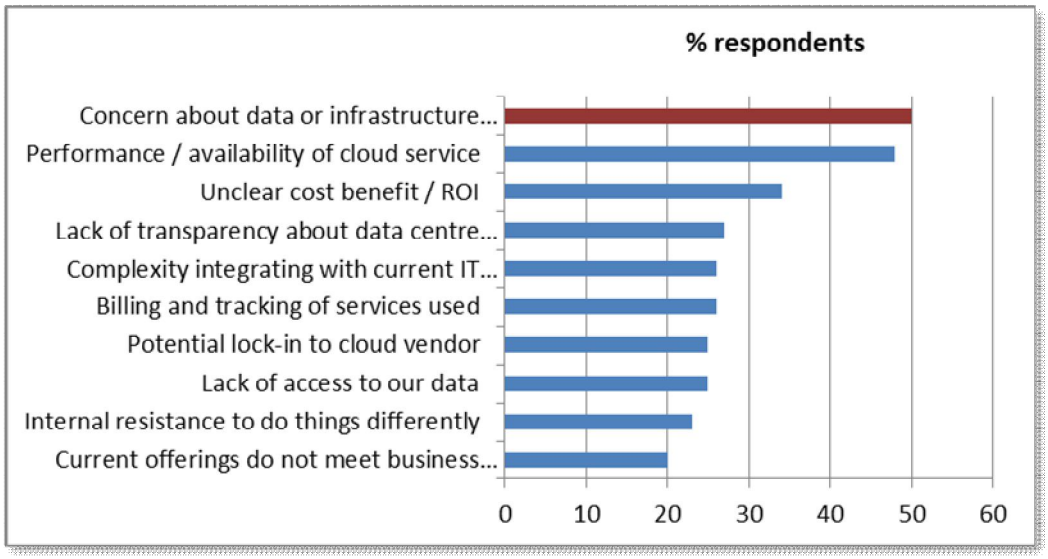
Ontario GeoPortal is a hosted data, software and infrastructure service of Infrastructure Ontario, a Crown corporation responsible for managing the province's real property assets – owned and leased buildings, lands and properties. Developed initially as an enterprise GIS to integrate data, documents and reports from a variety of databases within Ontario Realty Corporation (now Infrastructure Ontario), ORC decided in 2009 to migrate all the data, software and hardware to the "cloud" so that they could continue to grow the service while reducing internal ongoing IT requirements and costs. At its core, Ontario GeoPortal provides a geographic platform to integrate, publish and visualize tabular business data and non-structured content, and make this information securely accessible to users through a mapping interface. The service currently supports over 1,600 users within the Ontario government and has 14 corporate applications supporting a variety of business requirements.

3. Operational Polices and CC Implementation

Research conducted for the preparation of this primer clearly demonstrates that data security, and cloud service reliability and performance are the primary concerns of prospective users of cloud computing. Despite the rapid expansion of CC use, there remain concerns that are inhibiting CC adoption, as illustrated by Figure 5 (Trend Micro, 2011) (Gens, 2009). Therefore, cloud service providers face a significant challenge in building trust that: a) data will not be compromised; and, b) their service is always available and reliable.

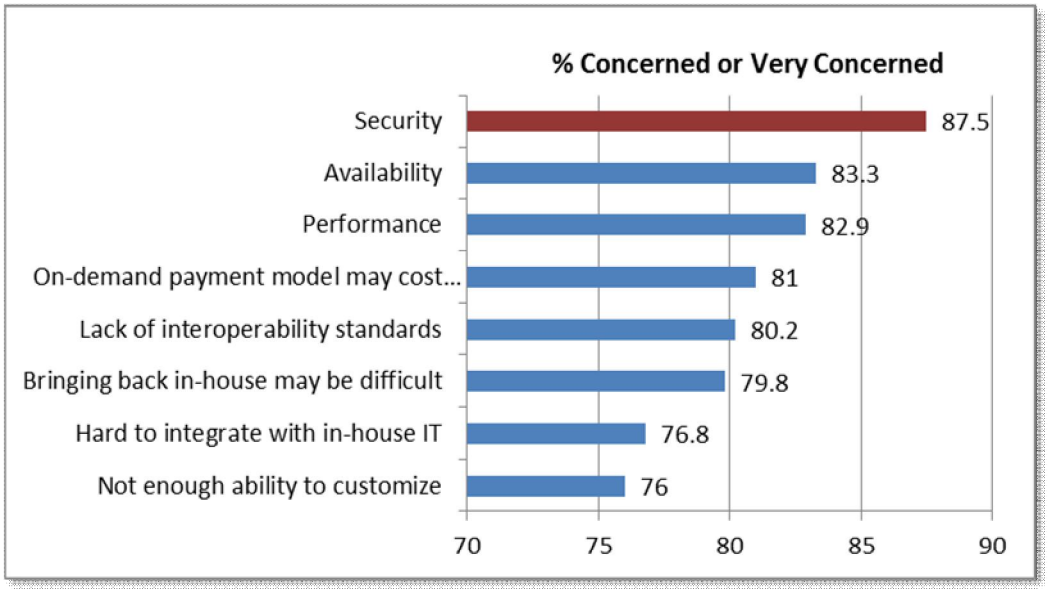
Figure 5: Potential Inhibitors to Cloud Computing Adoption

Q. What risks / barriers do you perceive in adopting cloud computing services?



Source: Cloud Security Survey Global Executive Summary (Trend Micro, 2011)

Q. Rate the challenges / issues of the cloud / on-demand model.



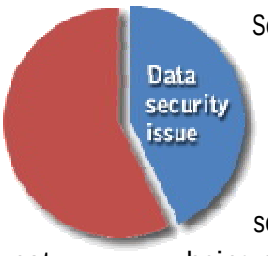
Source: New IDC IT Cloud Services Survey: Top Benefits and Challenges (Gens, 2009)

3.1 Security

3.1.1 Security Risks in the Cloud

Security is the top concern with cloud computing, both from the perspective of unauthorized data access and from the standpoint of the ability of the system to thwart malicious attack. **Security risks** include (Cloud Security Alliance, 2010) (Weech, 2011):

- *Abuse and Nefarious Use of Cloud Computing* – CC providers are targeted by spammers, malicious code authors and other criminals.
- *Insecure Application Programming Interfaces* – Weak interfaces and APIs expose CC users to confidentiality, integrity, availability and accountability issues.
- *Malicious Insiders* – Internal abuse can lead to brand damage, and financial and productivity losses.
- *Shared Technology Vulnerabilities* – Threats to the operations of one organization can affect many others that share the same resources.
- *Data Loss/Leakage* – Inappropriate use of or access to data can erode trust, have competitive and financial implications, and result in compliance violations and legal ramifications.
- *Account, Service & Traffic Hijacking* – Attackers using stolen accounts can compromise the confidentiality, integrity and availability of CC services.
- *Unknown Risk Profile* – Not doing a proper threat-risk assessment can leave customers vulnerable.
- *Complexity* – The complexity of the cloud infrastructure, as well as the integration with the organization's internal infrastructure, can provide more chances for security exploits.
- *Delegation of Authority* – Security is delegated to your vendor.
- *Encryption* – Becomes more difficult, with the lock and key stored off site.



Security concerns appear to be well founded. In the survey of 1,200 decision makers conducted by Trend Micro in May 2011, 43% globally (38% in Canada) who were using a cloud computing service reported a data security lapse or issue that year. In the same survey, 50% indicated data security concerns as a key reason for not adopting CC, and 40% of those with a CC solution felt their IT security requirements were not being met.

However, some CC users think the cloud offers *better* security potential because (Jackson, 2011):

- all systems receive security patches at the same time;
- fewer people are needed to update systems; and
- vendors are highly motivated to ensure the security of their service.

Experts such as the Cloud Security Alliance and the European Network and Information Security Agency have published helpful advice on managing the security risks in a cloud computing environment (Cloud

Amazon Web Services Customer Agreement

"**You are responsible** for properly configuring and using the [AWS] Service Offerings and taking your own steps **to maintain appropriate security, protection and backup of Your Content**, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving of Your Content."

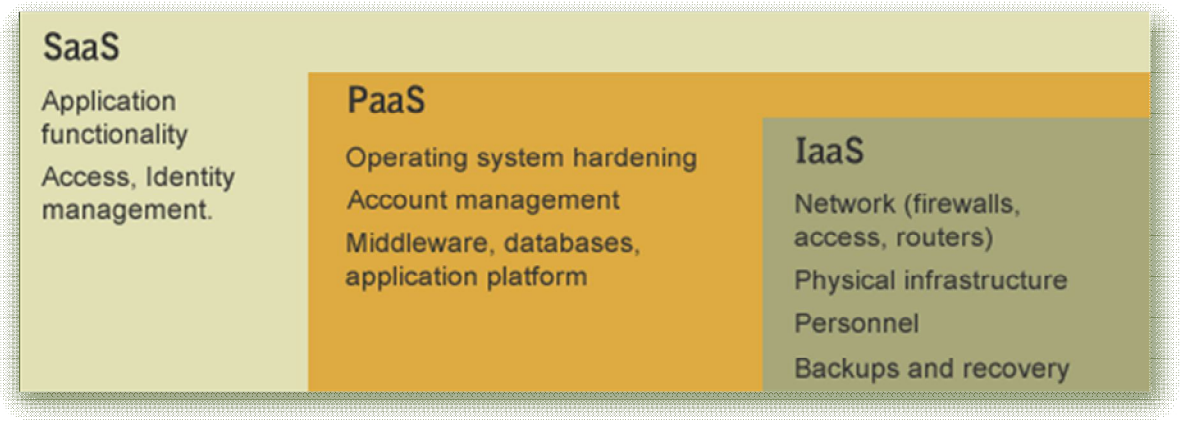
Security Alliance, 2011) and (European Network and Information Security Agency, 2009a).

3.1.2 Who is Responsible for What?

Understanding **responsibility** is a key part of managing cloud solution security. Figure 6 illustrates the types of security control in each of the predominant CC service model. Normally, the CC service provider is responsible for the overall system's security while the security associated with data content and access (who has access to what and how) is the client's responsibility.

CC providers are typically very secretive about their security capabilities. They will usually commit to a set of standards and processes to mitigate security breaches but will *not* guarantee that breaches will not occur. Depending on the type of cloud services, organizations may be responsible for the security of the data they put into the cloud, the applications they build and the operating systems they set up.

Figure 6: Security Control by Service Type



Source: Adapted from (Sawyer, 2011)

3.1.3 Threat Risk Assessment

Undertaking a **threat risk assessment** (TRA) is generally considered a best practice. However, some CC vendors may not permit the kind of probing that typically takes places within a TRA. The TRA identifies key assets (i.e., infrastructure components), services, and data that comprise the CC solution and its associated environments, determines the sensitivity of these assets, and assesses potential threats, vulnerabilities and safeguards. Risks are often "scored" as low, medium, high and severe. Recommendations

THREAT RISK ASSESSMENT

Prior to launching Ontario GeoPortal, an appropriate threat risk assessment (TRA) was completed. A professional consulting firm specializing in IT security was hired to conduct the TRA, and the issues identified in their report were subsequently addressed. The TRA report is available to new clients of Ontario GeoPortal as the basis for their own threat risk analysis of the solution.

are provided to assist in mitigating risks to meet defined targets and improve operational resilience and efficacy.

The TRA will consider such things as: the availability and continued operation of the service; confidentiality and security of the key data; linkages with other external services/systems; and trust and cooperation of partners and users. In so doing, the TRA looks at:

- The overall system and its deliverables
- The clients
- The components of the system
- Application architecture
- Network architecture
- User access control
- Security features of the hosting facility and the client facility
- The related IT standards and requirements in place

Based on this investigation, the TRA will then involve:

1. *Sensitivity assessment* – note and evaluate each asset with respect to confidentiality, integrity, availability.
2. *Threat assessment* – identify and describe threats to the system and the potential impact on the confidentiality, integrity, and availability attributes of the information and assets.
3. *Vulnerability assessment* – examine the system for weaknesses or safeguard deficiencies.
4. *Risk assessment* – quantify the degree to which a given risk is acceptable.

3.1.4 Risk Mitigation

Organizations can respond to security concerns by employing a variety of **risk mitigation** best practices. For example (Drake, Jacob, Simpson, & Thompson, 2011) (Escalante & Korty, 2011):

- Users that decide the risk of security breaches is so severe that they will not deploy applications on public clouds can opt instead for private clouds behind firewalls, on-premises, to control privacy, security and authentication issues.
- An organization can adopt public clouds, but insist that their data not be stored on servers located in jurisdictions where there are concerns about security breaches (e.g., either in US territory or under the control of a US-based or affiliated company, due to concerns about application of the Patriot Act).
- Organizations can take advantage of the reduced costs of public clouds while protecting sensitive information, for example, by stripping off some attributes from the geospatial data before sending them to the cloud.
- Organizations implement security everywhere (e.g., encrypted transport into the cloud, secure coding and access control inside applications, and encryption at rest), rather than the normal perimeter approach to security.

- Organizations can ensure that all APIs and data sources are checked with penetration tests[1] and thoroughly analyzed.
- Organizations can develop a policy statement and training materials covering the types of information allowed on CC services, and establish a process for conducting security reviews according to the policy.

[1] A method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders who do not have an authorized means of accessing the organization's systems, and malicious insiders who have some level of authorized access (Wikipedia, 2012)

3.1.5 Security Monitoring and Incident Response

ADEQUACY OF SECURITY MONITORING AND INCIDENT RESPONSE IN THE CLOUD

Organizations should ensure that security monitoring and incident response is well covered, by (Sawyer, 2011):

- **Asking CC providers for the highest possible level of access and control, or demonstrated acceptable levels of assurance by contract and SLA**
- **Asking CC providers for access to all the security logs available and plugging them into internal security monitoring processes**
- **Developing and following an incident response plan tailored to their needs and adaptable to the cloud**

Finally, there are two remaining critical aspects of security in the cloud from a user's perspective – **security monitoring** and **incident response**. The ability for an organization to monitor its data in the cloud may be limited because availability of security logs will vary by CC model and cloud service providers may also limit the different types of logs it makes available to customers. Incident response is more complicated in the cloud because there is no single physical machine from which data can be collected and analyzed, and there is additional time consuming coordination required to resolve an incident since the affected machines are in the cloud provider's premises, not those of the organization.

3.2 Privacy and Confidentiality

3.2.1 Privacy and Confidentiality Risks in the Cloud

Privacy and confidentiality risks run a close second to security as an issue that often discourages organizations from moving their data and applications into the cloud, and the privacy of personal information and the confidentiality of certain types of business or government information are obviously closely linked to the issue of data security. The main reason for these concerns is that CC service providers necessarily have access to all of the user's data and may disclose or use it, either accidentally or deliberately, for unauthorized purposes. Personal, confidential and sensitive data, in particular, need protection from inappropriate access or loss. The key privacy and confidentiality risks associated with CC can be summarized as follows (Gellman, 2009) (Office of the Privacy Commissioner of Canada, 2010):

- *Terms of service and privacy policy* – A user's privacy and confidentiality risks vary significantly depending upon the CC provider.
- *Disclosure of information to a cloud provider* – For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change with disclosure.
- *Legal status and protections* – Disclosure and remote storage may have adverse consequences for personal or business information.
- *Location of information in the cloud* – Location may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or

store the information, or information may have more than one legal location at the same time, with differing legal consequences.

- *Legal obligations* – Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters.
- *Legal uncertainties* – Assessing the status of information in the cloud, as well as the privacy and confidentiality protections available to users, are difficult.
- *Creation of new data streams* – CC providers may use data for purposes beyond those for which consent was originally given.
- *Intrusions into individuals' data* – CC providers or cloud-based applications may be able to access, mine or otherwise commoditize the data they hold, of which the individual never becomes aware.

PIPEDA IMPLICATIONS

Implications of the Personal Information Protection and Electronic Documents Act (PIPEDA) for the cloud computing environment in Canada include (Karn, 2011):

- **Cloud providers processing personal information must maintain security safeguards**
- **Cloud providers are not permitted to retain personal information indefinitely**
- **Cloud providers are not permitted to use personal information or its derivatives for new purposes**
- **Cloud users must pass along a number of other PIPEDA obligations to their CC providers**

3.2.2 Jurisdictional Considerations

Jurisdictional considerations are an important source of privacy concerns as well. For example, if data in the cloud is physically stored on servers located on US soil¸ service providers might hand over customer stored data and usage patterns to government agencies when they have not obtained proper authority (Weissberger, 2011c). Both the US Patriot Act and Canada's Security Intelligence Service Act have provisions that can compel CC providers to hand over data to the government. In addition, if data is stored on servers in multiple jurisdictions, management of the withdrawal of consent to data use becomes much more complex.

One of the requirements in the creation of the Ontario GeoPortal was that the chosen service provider must physically reside and store the data in Ontario, so that there would be no jurisdictional issues associated with hosted data. In Ordnance Survey's case, Amazon stores data on servers in Dublin, and the UK government does not tend to store personal data outside of the UK. While it is technically possible to ask for an exemption, they decided that it would be easier to build solutions in a way that did not require personal data to be stored in the cloud.

3.2.3 Cloud Vendor Obligations

As noted above in the context of security, depending on the type of cloud service being provided, the cloud provider may have a significant role to play regarding data confidentiality and privacy, or almost none at all. IaaS and PaaS providers typically have a more limited role in ensuring that privacy and confidentiality of data are maintained, except with respect to any third party access or non-permitted use of the data they are storing.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) requires that CC vendors processing personal information maintain security safeguards, and it prohibits cloud providers from retaining personal information indefinitely or using it for new purposes. Organizations should understand that if their CC provider is outside Canada and uses data illegally, it is likely that the organization will bear the brunt of any investigation or sanctions.

> Salesforce.com Customer Agreement
> "In accordance with the salesforce.com *Master Subscription Agreement*, **salesforce.com may access Customer Data only for the purposes of providing the services, preventing or addressing service or technical problems, at a Customer's request in connection with customer support matters, or as may be required by law.**"

Privacy legislation exists in most countries, but it has been suggested that the requirements have not always been reflected in CC providers' privacy policies (Ryan, 2011). Notwithstanding these privacy concerns, the success of companies like Salesforce.com has shown that many organizations are willing to trust the service provider with their most sensitive information.

3.2.4 Privacy and Confidentiality Risk Mitigation

Organizations can employ various methods to mitigate the risk of privacy and confidentiality breaches. For example, organizations that are moving to cloud computing can ensure that the person responsible for privacy is involved early in the process, to ensure that the privacy rights of individuals are identified and recognized and the potential risks when using cloud computing are addressed. The privacy staff should be involved in the evaluation of information moving to the cloud, the proposed service delivery model, the CC provider's proposal before a contract award takes place, and other areas of concern with specific legislation.

In addition, technologies can be used to ensure privacy protection. These include encryption of data prior to uploading it to the cloud, and hardware-based security initiatives such as the Trusted Platform Module, which are designed to provide a remote user with the confidence that data submitted to a CC provider is processed only according to an agreed policy. Services such as TRUSTe provide a privacy verification service to help CC vendors and clients deal with privacy and confidentiality concerns. Additional tips for addressing the risks of data privacy or confidentiality breaches in the cloud can be found in the Appendix 3.

3.3 Copyright and Licensing

Although no Canadian law cases have yet dealt with **copyright** in the cloud computing context, a number of questions are being posed in legal circles. These questions involve issues such as: when and where copies of works are being made and by whom; backup and transfer of copyrighted works from one server to another in the cloud; service provider and user ownership or licensing of rights to works; existence of copyright in the cloud or processed output from the cloud; and control of the communication of works across jurisdictional borders.

The cloud has also introduced some **licensing** complexities for CC users and providers. For example, conventional software licensing models are incompatible with the cloud and new models are evolving, such as retroactive charge backs based on resources or number of users serviced, or on-demand monthly charges based on historical patterns of how many users or requests were served. Software vendors such as Microsoft, Oracle, Esri and others have introduced pricing and access mechanisms defined for CC providers offering IaaS, PaaS, or even SaaS solutions.

In addition, providers of DaaS in the cloud may need to deal with the challenge of multiple licenses from third party data suppliers. If the licenses for the different datasets they want to provide as part of their service have conflicting terms, this must be resolved so that the DaaS provider's terms for licensing its data to users are workable. For example, in the case of the Ontario GeoPortal, means had to be found to provide different levels of access to data because of licensing restrictions on some datasets available through the portal.

LICENSING IN THE CLOUD

Infrastructure Ontario works with various data providers to ensure appropriate use and access to their data is maintained within the various client implementations of the Ontario GeoPortal. For example, the Ministry of Natural Resources already has a negotiated arrangement to make the Ontario Parcel (OP) – a spatial database with all the property boundaries in the province – available to other ministries, so Ontario GeoPortal is able to leverage the OP agreement. GeoPortal gives ministries that might not otherwise use the large and complex OP easy access and the ability to use this resource.

Software vendors vary in their approach to licensing on CC services and many have struggled to price appropriately. For Ordnance Survey (OS), the cost of using some of their existing commercial software on their CC solution was considered prohibitive, so they moved to Open Source software products. OS has paid close attention to the license models behind some of this software, to ensure that they are not compelled to make software, data or services available if they don't wish to.

3.4 Legal / Liability

There are a range of legal issues associated with cloud computing, several of which have already been referenced in Sections 3.2 and 3.3. However, most of the issues are not unique to the cloud, and prospective CC customers may be able to use the legal analysis applied to other Internet services as a foundation for the analysis of the security risks posed by cloud computing.

3.4.1 Cloud Computing Contracts

There is considerable criticism in the literature about the shortcomings in CC providers' standard terms of service and service level agreements (SLAs), and their general inflexibility to changes in those **contracts** (Bradshaw, Millard, & Walden, 2010), (MacDonald, 2010), (Karn, 2011). In Ordnance Survey's case, they approached the engagement of Amazon to provide cloud services in a manner similar to outsourcing any other element of IT services or infrastructure. This included consideration of a number of issues, including: safeguards against changes to the technical environment; IPR warranties and indemnities; security, back up and disaster recovery obligations; and data protection and confidentiality provisions, among others. However, they did encounter the reputed CC provider inflexibility to changes

in standard terms and conditions. OS has had to assume that any liability to third parties or its end users and costs or damages which it incurs as a result of any failure in the provision of the cloud service cannot be recovered from Amazon. SLAs often use vague language and narrow definitions regarding service guarantees, access to service quality statistics, dispute resolution, etc. OS encountered this problem and negotiated a customized SLA with their provider, Amazon.

A Federated Press workshop in 2011, Cloud Computing Law, provided some excellent insights into legal issues with cloud computing. In particular, presentations by two lecturers identified the following potential issues with CC **contract clauses**, which touch on several of the issues previously discussed (Lifshitz, 2011) and (Percival, 2011):

- *Data integrity* – Responsibility for preserving the integrity and confidentiality of the data usually rests with the user, and providers often disclaim any liability.
- *Data ownership and access* – It is important to specify that the user owns the data and what happens to the data upon contract termination; ensure that disputes on outstanding fees payment do not lock in data or result in data deletion; ensure that data is accessible and useable in case of interruption, litigation or bankruptcy and agree in advance on data formats and retrieval costs.
- *Licenses* – Users need to ensure that appropriate licensing exists to use IP and content accessed; beware that there is increased risk of IP infringement occurring in multiple jurisdictional situations.
- *Representations, warranties and liability limitations* – CC contracts often disclaim any warranties for quality of their services or service disruptions, which might result in data loss; broad sweeping limitation of liabilities clauses are common and should be avoided.
- *Indemnities* – These clauses are often equally broad and always in favour of the CC provider; users should seek remedies for any third party claims in respect of the provided software infringing IP rights of any third party.
- *Jurisdiction* – This may be an issue for resolution of disputes; export control laws may be a factor; location of data storage should be clearly specified.
- *Service Level Agreements (SLAs)* – SLAs often use vague language and narrow definitions regarding service guarantees and access to service quality statistics; it is important to request right to audit performance levels.
- *Loss of data* – Data inaccessibility when service is disrupted may not constitute a failure under SLAs; clarity is needed on who bears the cost of data replication and indemnification for lost or deleted data.
- *Data retention* – Laws or regulations may require data retention for specified periods in some jurisdictions; ensure that appropriate data retention and destruction policies are agreed upon.
- *Privacy* – The CC provider's privacy policy should state that personal information is stored in the cloud; compliance with PIPEDA should be in contracts; since protection of trade secrets and other proprietary information is not protected by PIPEDA (unless they do in fact contain personal information), contracts should deal with that accordingly; consider specific clauses in contracts for mandatory data breach notification, and indemnification for inappropriate access, use, disclosure or transfer of personal information.

- *Security* – Concerns may relate to CC providers' physical, operational or programmatic security measures; typically there is a great deal of secrecy about providers' security capabilities; providers usually commit to a set of standards and processes to mitigate security breaches but will not guarantee that breaches will not occur; divide responsibilities between yours and the CC provider's administrators so that no one organization has free access to all security layers.
- *Audits, certifications and inspections* – Users should request a right to audit clause; certifications should be based in ISO 27001 or SAS70; demand transparency of security and continuity management programs.
- *Contract changes* – Watch for terms that allow the provider to unilaterally vary the contract terms and conditions or to impose termination conditions based on criteria that it solely determines.
- *Dispute resolution* – Users should request specific terms on how disputes are to be resolved and the details of the issues escalation process; alternative dispute resolution (ADR) is a good tool if multiple jurisdictions are involved.

EDISCOVERY PLANNING

An eDiscovery plan between the CC user and provider is advisable, which includes (Selznick, 2011):

- **An eDiscovery Response Team with named individuals from provider and user organizations plus legal counsel;**
- **Definition of the provider's role in eDiscovery; and**
- **Details about**
  - **the types of data stored and storage locations**
  - **how data is to be accessed**
  - **procedures for indexing and searching data**
  - **procedures for demonstrating a clear chain-of-custody to data in question**
  - **turnaround times for data segregation**
  - **preservation and access procedures**
  - **the provider's ability to sub-contract, and**
  - **succession matters.**

3.4.2 eDiscovery and Litigation

Organizations considering use of CC services also need to consider documentary and records retention procedures, systems that support **litigation** readiness, and strategies for determining and defending eDiscovery processes (Selznick, 2011). It is important for prospective CC users to recognize that the determination of power, possession and control of information, in the legal discovery context, can be significantly impacted by the relationship with the CC provider, the terms of the service agreement and the provider's systems architecture. Users need to ensure that CC contracts contain clear wording to enable them to fulfill their legal obligation to produce documents in case of litigation (e.g., proper preservation processes, responsive search methodologies and selection processes, etc.).

When things go wrong, computer forensics are often required to figure out what happened, understand what portions of the system were affected, learn how to prevent such incidents from happening in the future, and collect information for possible legal actions. Such forensics can be more complicated in a cloud computing environment.

COMPUTER FORENSICS IN THE

Computer forensics can be more complicated in the cloud due to:

- **The ways that incident handling responsibilities are defined in SLAs**
- **Whether or not clocks are synchronized across data centers to help reconstruct a chain of event**
- **How data breach notifications laws are handled in different countries**
- **What data a cloud provider can look at when capturing an image of a shared hard drive**
- **What the user is allowed to see in an audit log (e.g., is information related to other cloud subscribers protected?)**
- **What responsibility a user has to report an incident in a PaaS model**
- **Whether or not a provider can legally intervene to stop an attack on an application in its cloud if it is only an indirect contractual relationship (e.g., three tiers of customers)**

3.4.3 Legal Jurisdictional Considerations

Many of the legal issues surrounding cloud computing are related to questions of **jurisdiction**, and several jurisdictional misconceptions are debunked in a recent white paper published by Fasken Martineau[2] (Kyer & Stern, 2011):

- *Misconception #1: Choice of law clauses solve the jurisdictional dilemma* – The choice of law does not mean that tort claims will be dealt with under that law, that intellectual property created by the parties will be assessed under that law or that consumer protection laws will be determined by that choice.
- *Misconception #2: There are separate rules for determining jurisdiction in Cyberspace* – While there are some special laws that have been passed dealing with the Internet, the general rule is that this method of doing business is subject to the same general rules and principles as other business methods that have an international or multijurisdictional element to them.
- *Misconception #3: Jurisdiction for e-commerce is determined by where the server is located* – This may or may not be a relevant fact to be taken into account in determining jurisdiction, but even if this were true, with CC it is difficult to determine definitively where the relevant servers are physically located.
- *Misconception # 4: There is a single set of rules to determine jurisdiction* – There is a not a single, applicable, international law nor is there one set of rules and principles applied around the world. Many countries are multi-jurisdictional like Canada (we do not have a single approach to conflict of laws). Even in a single jurisdiction, there are often separate rules and principles that govern conflicts in contract, tort, consumer protection and the like.

3.5 Archiving and Preservation

As suggested in the previous section, some legal issues are closely linked with issues surrounding data **preservation** in the cloud. For instance, legal requirements to preserve data for extended periods of time may exist in some jurisdictions, but such preservation can be complex in the cloud (e.g., retention timeframes may exceed SLA terms, downloading data in a forensically sound manner can be difficult, and there may be programmed data modification or purges). Users should protect themselves by ensuring that CC providers know what is important to preserve and can continue to store such

[2] The paper then proceeds to discuss the identification and management of jurisdictional risks

information for as long as required. As also mentioned above, eDiscovery requirements dictate that parties to a CC services contract also need to ensure that proper processes exist to defend the value, reliability and credibility of any documents to be produced.

Another issue that emerges with cloud computing is the potential **segregation** of different kinds of records (e.g., video clips, photos, E-mail, mapping data, etc.) between a number of different cloud providers. This scattering of data makes the task of finding all the information about a specific subject much more challenging, for example, in an Access to Information Act (federal legislation) or a Freedom of Information (provincial legislation) request situation. One solution to this preserving and archiving challenge is DuraCloud, an open source tool that allows CC users to make as many copies of their content as necessary and store those copies with several different cloud data storage providers. The application integrates directly with cloud storage providers, helps keep copies automatically synchronized, and allows users to verify the health of all of their content at any time (DuraSpace, 2012).

Cloud computing users may also benefit in the future from a research project in Europe, TIMBUS, which is examining the issues of preserving and future accessing of data in a cloud computing environment and will be completed in 2014 (Kepes, 2011) .

3.6 Regulation and Standards

3.6.1 Regulations

Compliance with a multitude of rules and **regulations** across multiple jurisdictions can be a particular challenge in the cloud. Since very few regulations were written for the cloud environment specifically, it can be difficult for a CC user to prove that their organization is in compliance without a cloud strategy that is based on a detailed understanding of the interaction between the regulatory environment and cloud computing. Regulations can limit an organization's range of cloud options because they may have to adhere to regulations around business continuity and disaster recovery, security standards (ISO 27001), logs and audit trails, and specific standards and governmental compliance requirements like Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA) in the US, and PIPEDA in Canada. For organizations to be compliant with the various regulations, they may have to adopt a hybrid or community cloud solution, potentially losing the full benefits of cloud use.

STANDARDS IMPLICATIONS

Without significant standards for cloud computing, there will be some level of lock-in to that service. In Ordnance Survey's case, they needed to modify their application to make use of some of the Amazon cloud service features, which has effectively tied them to Amazon.

Ontario GeoPortal's approach was to use best-of-breed technologies and components and have a Services Oriented Architecture to help ensure as much interoperability as possible. Ontario GeoPortal also had to respect the Government of Ontario's internal IT standards for account management, security and more.

3.6.2 Standards

Although clients care most about price, security, availability, and feature functionality,

standards can also be important. For example, without standards across the cloud community, clients can become "locked-in" to their chosen service provider because their implementation isn't transportable across cloud vendors should they want/need to change. However, despite the relative immaturity of cloud computing, recognition of the importance of standards has resulted in an array of cloud computing standards setting activities and bodies, as illustrated in Figure 7 (Cloud-Standards.org, 2010).

Figure 7: Organizations Involved with Cloud Computing Standards

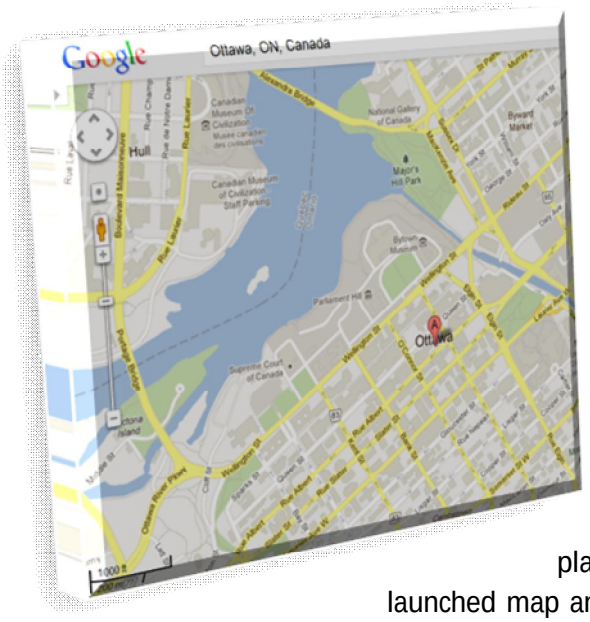
Some of the key initiatives of these organizations include:

- The National Institute of Standards and Technology (NIST) is identifying gaps in cloud standards and specifications and publishes the gaps on their portal.
- The Cloud Security Alliance (CSA) has several initiatives underway and has tools to assist cloud users and providers to assess and adopt cloud computing.
- The International Telecommunications Union – Telecommunications Standard Sector (ITU-T) has established a Focus Group on Cloud Computing (FG Cloud) to contribute to the aspects of cloud computing making use of telecommunication networks.
- The Open Management Group is focusing on modeling deployment of applications & services on clouds for portability, interoperability & reuse
- The IEEE Computer Society is working on cloud computing standards to help enable portability and greater interoperability.

The main standards setting organization in the geospatial domain, Open Geospatial Consortium (OGC), submits that its standards and the associated architecture are compatible with the cloud, since they are designed to provide interoperability across all platforms including the cloud (Ramage, 2011). However, a comparison of three PaaS platforms by University of Pretoria researchers found potential security pitfalls (e.g., malicious files on host machines and denial-of-service (DoS) attacks) when developing a Web Processing Service in a PaaS cloud (Ludwig & Coetzee, 2010).

4. Implications, Benefits and Risks

4.1 Implications for Canada's Spatial Data Infrastructure and its Stakeholders



As more and more geospatial cloud computing solutions appear, the need to address the fundamental requirement for base or framework data will be paramount. Most cloud computing solutions on the market currently do not include data. However, in the case of map-based solutions, geospatial data are always required, and there is a common core component of base data that virtually all clients need. Also, most cloud clients do not have the technical skills or staff capacity to build, acquire and/or maintain their own base geospatial data, and *therefore will rely on these data to be available as a service.*

Large commercial players that have launched map and imagery services, such as Google Maps and Bing Maps, have been meeting much of the online client community's base geospatial data requirements, providing visual locational reference and basic geospatial functionality. However, they do not typically address the need for thematic data such as resource management, agriculture, environment, demographic, economic, education, and more. When more clients are using maps for display, the need and opportunity for additional processing functionality will also grow.

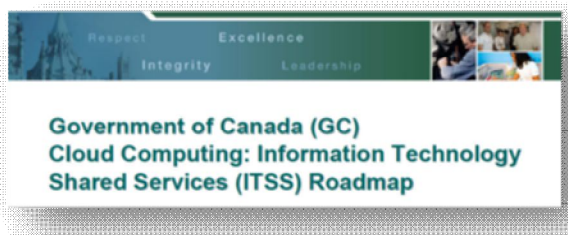
Canada's Spatial Data Infrastructure should be ready to encourage and respond to both these trends – the increased

requirement for geospatial data and the increased use of geospatial functionality. The CGDI can play a pivotal role in supporting the growth and adoption of geospatial cloud computing, particularly in this growing community of users who have no previous geospatial experience and capability, by being a source for: 1

a) geospatial data – with feature information – that can be easily acquired and consumed within an online application; and,
b) geospatial functionality that can be incorporated within SaaS solutions.

The map services that are accessible through the CGDI like GeoBase do not need to compete with the commercial base data providers. There is still significant demand for services to deliver the authoritative base data that government geospatial agencies make available through the spatial data infrastructure. CGDI will also find new opportunities for the delivery of thematic data services, particularly as more use is made of geospatial data and the cloud becomes a suitable delivery mechanism for applications that support its use.

Serious consideration is being given to cloud computing adoption at the federal level and, as discussed in Section 1, the evidence suggests that the provinces are also actively exploring CC potential. Government geospatial information organizations will be one of the most impacted, given the size of their data holdings, and will need to assess all of the operational policy considerations discussed in this primer as plans to migrate to the cloud are developed. Private sector data providers in Canada that adopt the cloud will also need to assess the operational policy challenges presented herein. In particular, legal issues such as protection of privacy and confidentiality and licensing will need close attention. CGDI stakeholders are already struggling with how to best preserve and archive digital geospatial data for research and possible eDiscovery purposes, and data migration into the cloud will make a complex task even more challenging.



Source: ITSS (Government of Canada, 2010)

4.2 Benefits

Along with the commonly associated benefits of cloud computing, *Geospatial* Cloud Computing offers the following *additional* benefits:

- *Lower cost of implementing* – acquiring a service, not server software, spatial data, and hosting.
- *Increased certainty* – lower risk; GCC helps simplify what is typically quite complex.
- *Geospatial data* – management and availability.
- *Capacity* – can be implemented without GIS expertise.

By extension, cloud computing can have beneficial impacts on the CGDI and its stakeholders. As more commercial geospatial cloud computing options become available on the market, organizations that previously had no or minimal experience with geospatial solutions will face lower barriers to adoption of this powerful technology. The resulting growth in the user community will increase demand for high quality geospatial data of all kinds, providing additional evidence of the value of the data being made accessible through the CGDI. Access to geospatial data via web services will increase as user demand shifts from professional geospatial organizations that typically download data into their own GIS systems to consumption of data by a much broader range of organizations, on an as-required basis. CGDI stakeholders will be challenged to meet the demand for high volume web access to patches of data on a daily basis.

4.3 Risks

As the technology and capability of the services and the underlying Internet infrastructure continue to improve, the primary risks associated with cloud computing generally are related to the operational policy matters addressed in this primer. However, one important technology risk for CGDI stakeholders is also relevant. As noted in the previous section, consumption of geospatial data via high quality web services is expected to grow quickly. The current capability of the CGDI and the stakeholder organizations that provide access to their data via the infrastructure to meet this demand is limited. While web service standards like WMS, WFS, etc. have been endorsed, most data access via the CGDI is still through data download. If this weakness in the infrastructure is not addressed, commercial data providers will fill this gap in the CGDI's ability to efficiently serve data for geospatial cloud computing applications.

The migration of hardware and software components of the CGDI (or other SDI in Canada) into the cloud will have a number of consequences. For example, the lack of internationally accepted cloud computing standards could present some problems of compatibility with standards-based SDI. Although the OGC standards adopted for the CGDI are intended to operate in cloud environments, as noted in Section 3.6.2, some research has suggested problems with web processing services in the cloud. Lack of CC standards also affects interoperability between data/applications in different cloud solutions and can result in vendor lock-in. This may affect SDI operations as well as have impacts on long term sustainability of certain SDI components in the cloud if a vendor ceases business or makes major changes in direction that are incompatible with the SDI model. And very critical assessments of the security offered by CC vendors will be necessary to make the best choice between public, private, community or hybrid clouds as a means of ensuring that private, confidential or sensitive information accessible through the CGDI is not compromised.

While addressing these operational policy issues will be challenging for CGDI stakeholders, the experiences documented in the two case studies (Ordnance Survey and Ontario GeoPortal) demonstrate that this challenge can be successfully addressed and overcome.

5. Conclusions

The use of cloud computing by public and private sector organizations is growing rapidly and geospatial information organizations are adopting this new computing model as well. Cloud computing provides a new means of delivering geospatial data, software and computing infrastructure as an online service, reducing the barriers to use of this powerful technology by non-GIS professional.

This primer was developed to highlight the key operational policy issues that organizations working with CC may face – particularly data security, privacy and confidentiality, legal, archiving and preservation, and regulatory and standards concerns. Information provided on policies and practices currently in use and key lessons learned by CC implementers is intended to serve as guidance to anyone wishing to initiate or improve their own cloud computing solution.

Appendix 1: Glossary

Acronym	Term	Definition
ADR	Alternative Dispute Resolution	Processes that can be used to resolve a conflict, dispute or claim, which are alternatives to having a court decide the dispute in a trial or other institutions decide the resolution of the case or contract (American Bar Association Section of Dispute Resolution, 2006)
	Applications	Computer software designed to help the user to perform specific tasks
API	Application Programming Interface	A source code-based specification (e.g., for routines, data structures, object classes, and variables) intended to be used as an interface by software components to communicate with each other.
	Archiving	Creating a collection of historical records (i.e., records that have been selected for permanent or long-term preservation on grounds of their enduring cultural, historical, or evidentiary value)
CGDI	Canadian Geospatial Data Infrastructure	The CGDI helps Canadians gain new perspectives into social, economic, and environmental issues, by providing an online network of resources that improve the sharing, use and integration of information tied to geographic locations in Canada.
CC	Cloud Computing	A model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
	Computer forensics	Computer investigation and analysis techniques to determine legal evidence (Lexbe.com , 2012)
	Confidential information	Information that is meant to be kept secret within a certain circle of persons and not intended to be known publicly, which is accessible only to those authorized to have access
	Copyright	The exclusive right to produce or reproduce the work or any substantial part thereof in any material form whatever, or to authorize such acts.
DoS	Denial-of-service attack	An attack on a computer where the attacker attempts to prevent legitimate users from accessing information or services,

Acronym	Term	Definition
		such as email, websites, online accounts (banking, etc.), or other services that rely on the affected computer (US-CERT, 2009)
eDiscovery	Electronic Discovery	The collection, preparation, review and production of electronic documents in litigation discovery. This includes e-mail, attachments, and other data stored on a computer, network, backup or other storage media, as well as metadata (Lexbe.com, 2012)
GCC	Geospatial cloud computing	GCC can be considered as a cloud service that incorporates maps and the use and manipulation of spatial data.
HIPAA	Health Insurance Portability and Accountability Act	American law controlling the use of personal health information.
	Infrastructure	Processing, storage, networks, and other fundamental computing resources
	Liability	Legal responsibility for one's acts or omissions; failure to meet that responsibility leaves one open to a lawsuit for any resulting damages
	Licensing	Authorizing by the licensor the use of the licensed material by the licensee
	Mobile app	A software application designed to run on smart phones and tablet computers
PCI	Payment Card Industry	Standards associated with payment card data security.
PIPEDA	Personal Information Protection and Electronic Documents Act	Rules of the Canadian govt. associated with the responsibilities a service provider must take with respect to information that it collects or stores about individuals.
	Privacy	The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively
	Seamlessly	The manner in which processing or storage capacity is added or removed without any express action from the user or even awareness by the user that such adjustment is taking place
	Security	The means of protecting information on computers from theft, corruption, or natural disaster, which allow the information to remain accessible and productive to its intended users
SLA	Service Level Agreement	A contract between a service provider and a customer that establishes a common understanding about services, priorities, responsibilities, guarantees and warranties, and details the nature, quality, and scope of the service to be provided, usually in measurable terms
	Tort	A civil wrong, other than a breach of contract, which the law will redress by an award of damages (Canada Legal Information Sources, 2012)

Acronym	Term	Definition
	Web browser	A software application for retrieving, presenting, and traversing information resources on the World Wide Web

Appendix 2: References

American Bar Association Section of Dispute Resolution. (2006). *What You Need to Know about Dispute Resolution: The Guide to Dispute Resolution Processes.* Retrieved February 15, 2012, from American Bar Association: http://www.americanbar.org/content/dam/aba/migrated/2011_build/dispute_resolution/draftbrochure.authcheckdam.pdf

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011, May). *DRAFT Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology.* Retrieved December 28, 2011, from NIST: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

Bailey, S. (2010, April). *Data Preservation and Retrieval*. Retrieved January 12, 2012, from JISC infoNet: http://www.jiscinfonet.ac.uk/infokits/cloud-computing/information-management

Bradshaw, S., Millard, C., & Walden, I. (2010, September 1). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. Retrieved March 3, 2012, from Social Science Research Network: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374##

Canada Legal Information Sources. (2012). *Introduction to "What is a TORT CLAIM? How is this related to expenses from personal injuries?* Retrieved February 16, 2012, from Canada Legal Information Sources: http://www.canadalegal.info/prov-bc/0-ref-library/personal-injury/personal-injury-bc-icbc-03.html

Cloud Security Alliance. (2011). *ECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0*. Retrieved January 2, 2012, from Cloud Security Alliance: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Cloud Security Alliance. (2010, March). *Top Threats to Cloud Computing V1.0.* Retrieved January 5, 2012, from Cloud Security Alliance: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud-Standards.org. (2010, May 17). *Cloud Standards Overview*. Retrieved January 2, 2012, from Cloud-Standards.org: http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview

Corley, R. (2011). NEGOTIATING AND DRAFTING CLOUD COMPUTING CONTRACTS: A CHECKLIST FOR CC DEALS. *Cloud Computing Law Workshop.* Toronto: Federated Press.

Danek, J. (2010, April). *Government of Canada (GC) Cloud Computing: Information Technology Shared Services (ITSS) Roadmap.* Retrieved January 23, 2012, from ICT Standards Advisory Council of Canada : http://www.isacc.ca/isacc/_doc/ArchivedPlenary/ISACC-10-43305.pdf

Drake, J., Jacob, A., Simpson, N., & Thompson, S. (2011, November). *Open Data Center Alliance Developing Cloud-Capable Applications White Paper.* Retrieved December 30, 2011, from Open Data Center Alliance: http://www.opendatacenteralliance.org/docs/Best_Practices_whitepaper.pdf

DuraSpace. (2012). *Preservation and Archiving*. Retrieved January 12, 2012, from DuraCloud: http://www.duracloud.org/preservation_and_archiving

Escalante, D., & Korty, A. J. (2011, July). *Cloud Services: Policy and Assessment*. Retrieved December 28, 2011, from EDUCAUSE Review, vol. 46, no. 4 : http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume46/CloudServicesPolicyandAssessme/231833

European Network and Information Security Agency. (2009a, November). *Cloud Computing Information Assurance Framework.* Retrieved January 3, 2012, from ENISA: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework?searchterm=Cloud+Computing+Information+Assurance+Framework

Gellman, R. (2009, February 23). *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*. Retrieved December 23, 2011, from World Privacy Forum: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Gellman, R., & Dixon, P. (2009, February 23). *Cloud Computing Privacy Tips*. Retrieved December 23, 2011, from World Privacy Forum: http://www.worldprivacyforum.org/pdf/WPF_Cloud_Tips_fs.pdf

Gens, F. (2009, December 15). *New IDC IT Cloud Services Survey: Top Benefits and Challenges*. Retrieved December 15, 2011, from IDC exchange: http://blogs.idc.com/ie/?p=730

Jackson, K. L. (2011, October 17). *It's Official! US Intelligence Community Is Moving To The Cloud!* Retrieved December 15, 2011, from Forbes.com: http://www.forbes.com/sites/kevinjackson/2011/10/17/its-official-us-intelligence-community-is-moving-to-the-cloud/

Karn, B. (2011, March 31). *Data Security — The Case Against Cloud Computing*. Retrieved January 2, 2012, from casselsbrock.com: http://www.casselsbrock.com/files/file/docs/Data%20Security%20-%20The%20Case%20Against%20Cloud%20Computing%20PDF.pdf

Kepes, B. (2011, September 19). *New EU Digital Preservation Project*. Retrieved January 23, 2012, from CloudAve: http://www.cloudave.com/14995/new-eu-digital-preservation-project/

Kyer, C. I., & Stern, G. M. (2011, March 30). *Where in the World is My Data? Jurisdictional Issues with Cloud Computing.* Retrieved January 2, 2012, from Fasken Martineau: http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf

Lexbe.com . (2012). *e-Discovery & Metadata Definitions*. Retrieved February 16, 2012, from Lexbe.com : http://www.lexbe.com/hp/define-e-Discovery-metadata.htm

Lifshitz, L. R. (2011). Understanding Cloud Computing: Legal Issues and Best Practices. *Loud Computing Law.* Toronto: Federated Press.

Ludwig, B., & Coetzee, S. (2010, August 26). *A Comparison of PaaS Clouds with a Detailed Reference to Security and Geoprocessing Services.* Retrieved December 23, 2011, from http://webmgs2010.como.polimi.it/presentations/2_LudwigCoetzee.pdf

McDonald, S. (2010, February 2). Legal and Quasi-Legal Issues in Cloud Computing Contracts. Retrieved December 28, 2011, from Educause: http://net.educause.edu/section_params/conf/CCW10/issues.pdf

Mel, P., & Grance, T. (2011, September). *The NIST Definition of Cloud Computing.* Retrieved December 20, 2100, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Messmer, E. (2009, March 12). *Best security questions to ask about SaaS*. Retrieved December 15, 2011, from Network World : http://www.networkworld.com/news/2009/031209-saas-security.html

Microsoft. (2011, July 11). *Ontario Government Sees Waves of Potential After Testing Private Cloud Solution*. Retrieved January 23, 2012, from Microsoft Case Studies: http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000011335

NEC; IPC Ontario. (2010, May). *Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach.* Retrieved January 6, 2012, from Information and Privacy Commissioner, Ontario: http://www.privacybydesign.ca/content/uploads/2010/07/pbd-NEC-cloud.pdf?search=search

Office of the Chief Information Officer. (2011, July 19). *IM/IT Enablers Strategy v1.5 for Citizens @ the Centre: BC government 2.0.* Retrieved January 23, 2012, from Office of the Chief Information Officer: http://www.cio.gov.bc.ca/local/cio/about/documents/it_strategy.pdf

Office of the Privacy Commissioner of Canada. (2010, March 29). *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing*. Retrieved January 2, 2012, from Office of the Privacy Commissioner of Canada: http://www.priv.gc.ca/information/pub/cc_201003_e.cfm#toc2c1

Ontario GeoPortal. (2011, June 1). *Ontario GeoPortal Comparison.* Retrieved March 3, 2012, from Ontario GeoPortal: http://www.ontariogeoportal.com/Documents/OntarioGeoPortalComparison.pdf

Open Data Center Alliance. (2011a, June 7). *Open Data Center Alliance Usage: Provider Security Assurance*. Retrieved January 2, 2012, from Open Data Center Alliance: http://www.opendatacenteralliance.org/ourwork/usagemodels

Open Data Center Alliance. (2011d, June 7). *Open Data Center Alliance Usage: Regulatory Framework*. Retrieved January 2, 2012, from Open Data Center Alliance: http://www.opendatacenteralliance.org/ourwork/usagemodels

Open Data Center Alliance. (2011b, June 7). *Open Data Center Alliance Usage: Security Monitoring*. Retrieved January 2, 2012, from Open Data Center Alliance: http://www.opendatacenteralliance.org/ourwork/usagemodels

Open Data Center Alliance. (2011e, June 7). *Open Data Center Alliance Usage: Standard Units of Measure for IaaS* . Retrieved January 2, 2012, from Open Data Center Alliance: http://www.opendatacenteralliance.org/ourwork/usagemodels

Open Data Center Alliance. (2011c, June 7). *Open Data Center Alliance Usage: VM Interoperability*. Retrieved January 2, 2012, from Open Data Center Alliance: http://www.opendatacenteralliance.org/ourwork/usagemodels

Percival, R. L. (2011). Cloud Computing: Due Diligence Considerations. *Cloud Computing Law Workshop.* Toronto: Federated Press.

Power, A. (2011). Privacy Concerns with Cloud Computing. *reventing Data Breach and Misuse Workshop.* Ottawa: Federated Press.

Ramage, S. (2011, January 5). *Standards for geospatial technology and services in cloud computing.* Retrieved December 23, 2011, from OGC: http://portal.opengeospatial.org/files/?artifact_id=42636

Ryan, M. D. (2011). Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM, Vol. 54 No. 1* , pp. 36-38.

Sawyer, J. (2011, June). *Spot Trouble in the Cloud: Adapting Security Monitoring & Incident Response*. Retrieved December 30, 2011, from InformationWeek: http://reports.informationweek.com/abstract/5/7376/Cloud-Computing/strategy-cloud-security-monitoring.html

Selznick, S. I. (2011). ADDRESSING E-DISCOVERY AND LITIGATION ISSUES. *Cloud Computing Law Workshop.* Toronto: Federated Press.

Spires, R. A. (2011, September 6). *Cloud Computing, Front and Center*. Retrieved December 21, 2011, from CIO.gov: http://www.cio.gov/pages.cfm/page/Cloud-Computing-Front-and-Center

Trend Micro. (2011, June 3). *Cloud Security Survey Global Executive Summary*. Retrieved December 15, 2011, from Trendmicro.com: http://es.trendmicro.com/imperia/md/content/uk/about/global_cloud_survey_exec_summary_final.pdf

US-CERT. (2009). *Understanding Denial-of-Service Attacks*. Retrieved Febraury 16, 2012, from United States Computer Emergency Response Team: http://www.us-cert.gov/cas/tips/ST04-015.html

Weech, M. (2011). GIS & The Cloud. Ottawa, ON, Canada.

Weissberger, A. (2011b, January 13). *What Should Cloud Computing Users and Providers consider for SLAs?* Retrieved December 23, 2100, from Viodi: http://www.viodi.com/2011/01/13/what-should-cloud-computing-users-and-providers-consider-for-slas/

Weissberger, A. (2011c, August 11). *Cloud Computing Issues: State of the Net West Conference – August 6, 2008, Santa Clara, CA*. Retrieved December 23, 2100, from Viodi: http://viodi.com/2008/08/11/cloud-computing-issues-state-of-the-net-west-conference-august-6-2008-santa-clara-ca/

Yang, C., Goodchild, M., Huang, Q., Nebert, D., & Raskin, R. (2011). Spatial cloud computing: how geospatial geospatial sciences could use and help to shape cloud computing. *International Journal of Digital Earth, 4:4* , 305-329.

Zients, J. (2010, November 19). *Driving IT Reform: An Update*. Retrieved January 3, 2012, from Office of Management and Budget: http://www.whitehouse.gov/blog/2010/11/19/driving-it-reform-update

Appendix 3: Good Practices

This appendix provides a summary of good practices that other organizations have adopted in their implementation of cloud computing, which CGDI stakeholders may wish to consider.

5.1 Security

Security of data and applications in the cloud appears to be the overriding concern for prospective users of cloud computing services. Good practices for dealing with this concern are summarized in the sections.

5.1.1 Security Questions for Vendors

Questions that potential purchasers of SaaS should ask include (Messmer, 2009):

- Which of the SaaS employees has root and database access, and will anything prevent them from getting access to your corporate data? What controls are in place?
- Is data held encrypted? How?
- Is the held data separated between clients or is it all stored on one huge database? How is data separated? How will the legal question of e-discovery be addressed should it arise as a business concern?
- Is the data flowing between the business and the vendor's cloud computing infrastructure secured in some way?
- What controls would prevent vendor insiders from downloading your data onto a USB stick and walking out the door?
- In terms of service availability, can your vendor to sign a service-level agreement?
- Is their data center in a location prone to hurricanes or earthquakes? What are their back-up plans?
- What information is captured in audit logs?
- Are there ways to limit where the SaaS vendor goes within the corporate network?

Security issues customers should raise with vendors before selecting their provider include (Brodkin, 2008):

- Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.
- Identify whether the cloud vendor is willing to be subjected to external audits and security certifications.
- Ask providers if they will commit to storing and processing data in specific jurisdictions, and make a contractual commitment to obey local privacy requirements on your behalf.
- Find out what is done to segregate data at rest and for evidence that encryption schemes were designed and tested by experienced specialists.

- Ask providers if they can do a complete restoration of data in case of a disaster, and how long it will take.
- Ask providers for a contractual commitment to support specific forms of investigation (e.g., of inappropriate or illegal activity), and evidence that they have already successfully supported such activities.
- Ask providers how you would get your data back if their company fails or is acquired, and if it would be in a format that you could import into a replacement application.

Yang, et al (2011) identified the following as security baseline elements:

- Cloud computing providers
  - ensure the functionality and availability of the cloud services
  - provide possible solutions to protect data loss due to failure of cloud services, and have back-up strategies when the cloud service fails to enable data transfers securely from one location to another
- Privileged users within cloud computing companies
  - have separating duties to prevent data leaks or access by other third parties (e.g., computing resource maintainers that have control over computing infrastructure cannot access user accounts, while user account staff should not be able to access the physical machine)
- End users
  - have their own level-based identity management system to control access to cloud data and resources
  - only have access to and control over their own jobs

5.1.2 Security Usage Models

The Open Data Centre Alliance (ODCA) has developed the following security usage models for cloud computing:

- *Open Data Center Alliance Usage: Provider Security Assurance* (ODCA, 2011a) – provides standard definitions of security for cloud services, details mechanisms for service providers to demonstrate compliance, and gives organizations the ability to validate adherence to security standards within cloud services
- *Open Data Center Alliance Usage: Security Monitoring* (ODCA, 2011b) – provides user organizations with a standard monitoring framework and relevant interfaces that will let them query the status of security and compliance within the services they procure from providers
- *Open Data Center Alliance Usage: Virtual Machine (VM) Interoperability* (ODCA, 2011c) – specifies actions and process to spur development of interoperable, VM management solutions aimed at lowering management complexity and costs, especially in heterogeneous, multi-vendor environments
- *Open Data Center Alliance Usage: Regulatory Framework* (ODCA, 2011d) – helps user organizations assess and monitor their regulatory obligations when engaging and acquiring cloud services

5.2 Privacy

Privacy and confidentiality risks run a close second to security as an issue that often discourages organizations from moving their data and applications into the cloud. The following sections summarize good practices identified in the literature to deal with this issue.

5.2.1 Cloud Computing Privacy Tips for Organizations and Consumers

The following cloud computing privacy tips will help organizations and consumers to ensure data privacy is protected (Gellman & Dixon, 2009), (Power, 2011):

- Beware of "ad hoc" cloud computing. Any organization should have standardized rules in place telling employees when and if they may utilize cloud computing and for what data.
- Don't put anything in the cloud you wouldn't want a competitor, your government, a private litigator or another government to see.
- Read the Terms of Service and privacy policy and ensure that you understand them.
- Make sure that you are not violating any law or policy, by putting data in the cloud, and think twice before putting any consumer data in the cloud.
- Consult with your legal, technical, security or corporate governance advisors about the advisability of putting data in the cloud.
- Request advance notice of any changes to the terms of service or privacy policy.
- Ensure full understanding of respective roles and responsibilities.
- Pay close attention if the cloud provider reserves rights to use, disclose, or make public your information.
- Check to see if the cloud provider still retains rights to your information once you remove it from the cloud. If so, consider whether that makes a difference to you.
- Build privacy into your cloud computing implementation design.

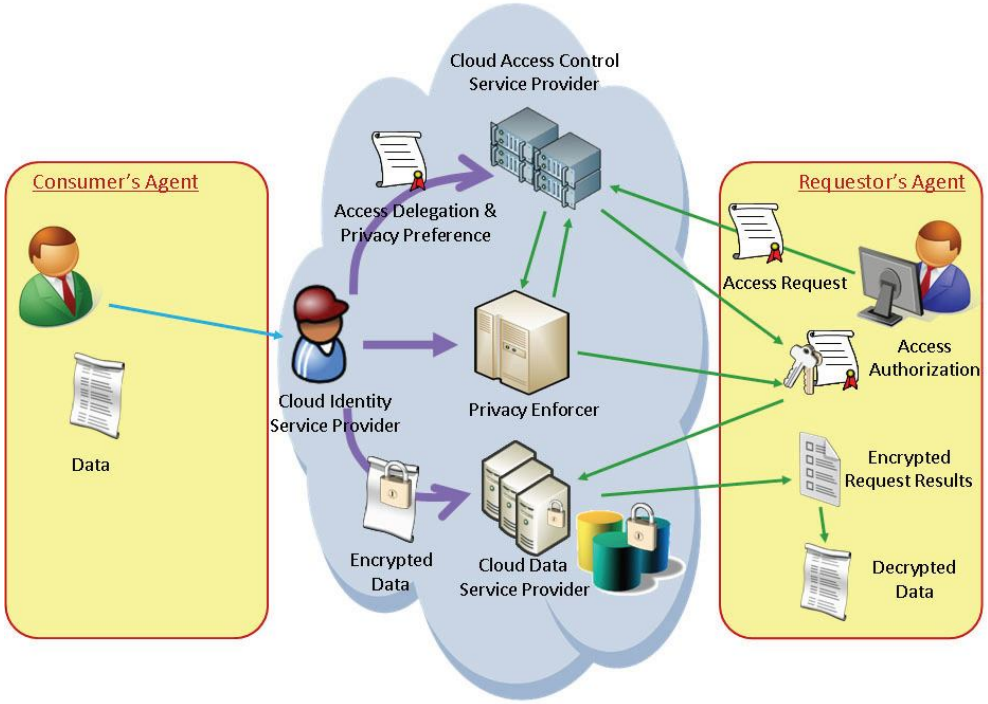
5.2.2 Protecting Data Entering the Cloud

A paper on the use of the Privacy by Design (PbD) principles for cloud computing provides suggestions for a data protection scheme for data that enters the Cloud and maintaining appropriate access to this protected data (see Figure 8) as follows (NEC and IPC Ontario, 2010):

- Develop an architecture that requires collaboration between two agents – the consumer's agent and the requestor's agent – three service providers – the Cloud access control service provider, the Cloud data service provider, and the Cloud identity service provider – and a privacy enforcer.
- The consumer's agent would encrypt data prior to sending it to the Cloud and issue access delegation to the Cloud access control service provider that will handle data utilization requests from the requestor
- The architecture would mandate that the requestor's agent must contact the Cloud access control service provider for access authorization

- The Cloud identity service provider would help the consumer in identity management, under the protection of secure and manageable pseudo identities, and provide pseudo identities to the consumer
- The Privacy Enforcer would match the requestor's stated purposes against the consumer's privacy preferences
- The authorization message would consist of three components: i) it would indicate to the Cloud access control service provider that the requestor had been authenticated; ii) it would indicate the subset of data to be released to the requestor; and iii) it would also contain a decryption key for the released data.

Figure 8: Cloud Computing Architecture for Privacy-Preserving and Usable Data Outsourcing



Source: Modeling Cloud Computing Architecture without Compromising Privacy: A Privacy by Design Approach (NEC and IPC Ontario, 2010)

5.2.3 Protecting Data Stored with Third Parties

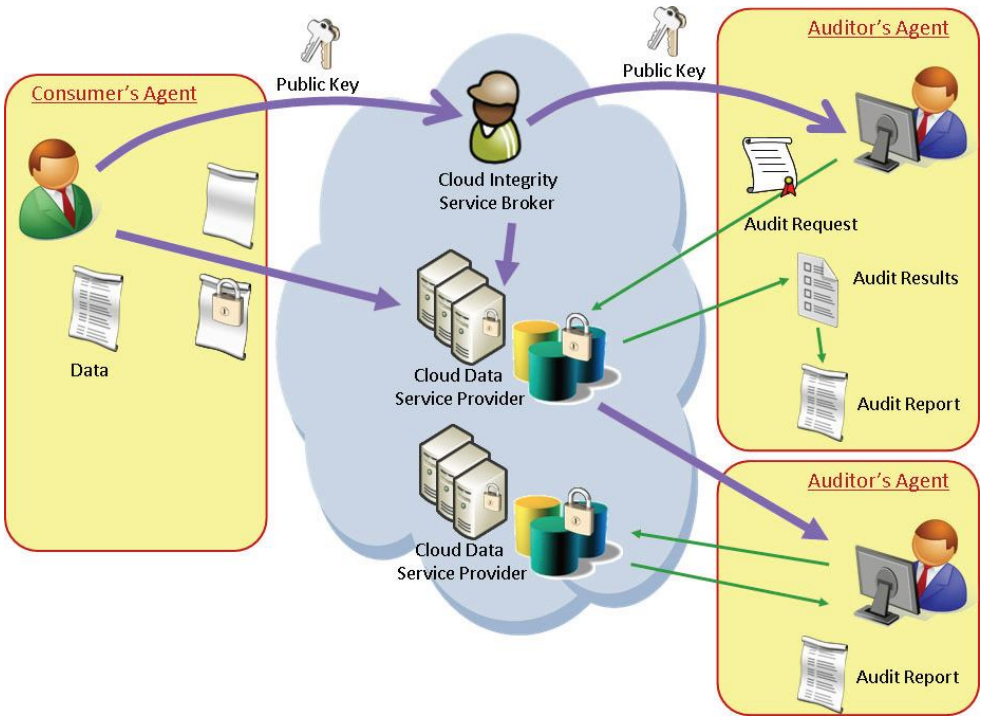
Suggestions for ensuring the integrity of protected data, without losing privacy, when the cloud data service provider uses other Cloud data service providers for backup purposes (see Figure 9) include (NEC and IPC Ontario, 2010):

- Develop an architecture that requires collaboration between two types of agents – the consumer's agent and auditor's agents – a (re-engineered) data service provider, and a Cloud integrity service broker

- The consumer's agent would outsource encrypted data to the Cloud data service provider, while now additionally contracting an auditor (either internal or external to the consumer) to handle integrity audits
- The Cloud integrity service broker would help both the consumer and the Cloud data service provider in contacting auditors and relay the consumer's public key to the auditors and Cloud data service provider
- The auditor would send audit requests to the Cloud data service provider, which would reply with an audit result; the auditor would then release an audit report on data integrity
- Crucial to this architecture design is that the consumer uses a public key rather than the encryption key so, even if both the Cloud data service provider and the auditor's agent are compromised, the consumer's data, and thus privacy, remains safe
- For an enhanced level of privacy protection, a Cloud identity service provider could be included in this audit architecture, allowing the consumer to find an auditor anonymously or pseudonymously and preventing a malicious auditor from obtaining any advantage towards privacy invasion simply by being contracted to audit a consumer's data

These architectural design ideas are intended to meet security, usability, data integrity and privacy requirements simultaneously – the 'positive-sum' that adherence to the PbD principles is designed to achieve.

Figure 9: Cloud Computing Architecture for Privacy-Preserving, Trustworthy, and Available Data Outsourcing



Source: Modeling Cloud Computing Architecture without Compromising Privacy: A Privacy by Design Approach (NEC and IPC Ontario, 2010)

5.3 Legal / Liability

Suggested good practices for dealing with contracts and service level agreements with cloud service providers are provided in the following sections.

5.3.1 Contracts

Considerations for entering contracts with cloud computing vendors include the following (McDonald, 2010), Badger, et al (2011) and (Corley, 2011):

- *Privacy and confidentiality*
  - Ensure, through specific contractual clauses, that the vendor will not use the data for any purpose other than providing the outsourced service (such as data mining for the vendor's own benefit) or re-disclose it to others without appropriate authorization.
  - Analyze SaaS and PaaS vendor's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet your confidentiality and compliance requirements.
- *Data security*

- Specify an actual, specific, independent security standard and require that it be updated, and perhaps audited (e.g., SAS 70, Type II audit) regularly, and require the vendor to give notice of any security/data breaches.
- Require that vendors offer a mechanism for reliably and securely deleting data on a subscriber's request.
- Require that SaaS vendors employ strong encryption using a robust algorithm with keys of required strength for Web sessions whenever the subscribed application requires the confidentiality of application interaction and data transfers. Also require that the same diligence be applied to stored data.
- Ensure that a PaaS application can be configured to run in a secure manner and can be integrated with existing enterprise security frameworks such as identification and authorization.
- Ensure that IaaS vendors have mechanisms in place to protect virtual machines from attacks (a) from other VMs on the same physical host (b) from the physical host as well as (c) network originated attacks.
- Require vendors to offer methods that the subscriber can use to assess whether or not their data protection requirements continue to be met.
- For encryption of data at rest, require vendors to make available the strength of the encryption algorithm suite, the key management schemes a provider supports, and the number of keys for each data owner (individual or shared keys).

- *Location of data*
  - If important, include language prohibiting "extraterritorial" storage (e.g., in the United States).
- *Access to data*
  - Consider contractual terms related to guarantee and testing of data integrity, data formats, frequency of backups, storage of backed up data, access to data if provider disappears, single points of failure, etc.
- *Responsibility for end users*
  - In order to comply with normal vendor requirements that any end users comply with their acceptable use policy, terms of service, or similar provisions, require end users to agree directly with the vendor to comply with any such provisions.
- *Unauthorized or inappropriate use*
  - Provide only that you will not "authorize" or "knowingly allow" any "unauthorized" or "inappropriate" use of the vendor's service by others and will notify them of only "material" such uses.
- *Suspension of end-user accounts*
  - Permit suspension of end users rights only if there are "material" violations of the vendor's acceptable use policy, terms of service, or similar provisions, or violations that "significantly" threaten the security or integrity of the vendor's system.
- *Emergency security issues*
  - The standard for what constitutes an emergency suspension of use should be clearly defined, should not give the vendor much if any discretion or flexibility in its application, and, preferably, should incorporate a "materiality" or similar threshold.
- *Suspension and termination of the service*

  - Provisions for termination of services should be limited in scope to only truly significant matters, provide for an opportunity for you to cure the alleged violations or some form of escalation rather than instantaneous implementation (except in the case of true emergencies), and give you adequate time to make alternative arrangements for your data or service.
- *Data ownership*
  - The contract should expressly state that all data belongs to your organization (and/or your users) and that the vendor acquires no rights or licenses to use the data for its own purposes by virtue of the transaction and does not acquire and may not claim any security interest in the data.
- *Service level agreements*
  - Spell out clearly the amount of guaranteed "uptime," the process and timeline for dealing with "downtime," and the consequences for any failures to meet those requirements.
  - Formulate remedies that are commensurate with damage that might be sustained.
  - Specify compliance with appropriate laws and regulations governing subscriber data.
  - Ensure there are no disclaimers relating to security or critical processing.
  - Search for provider recommendations regarding independent backup of data stored in their cloud.
- *Disclaimer of warranty*
  - Warrant in the contract that the service conforms to and will perform in accordance with its specifications (which should themselves be as detailed as possible, to avoid misunderstandings and disagreements) and that it does not infringe any third-party intellectual property rights.
- *Indemnification by vendor*
  - The vendor should indemnify you for all of its acts and omissions, and especially for infringement of third-party intellectual property rights and inappropriate disclosure or data breach.
- *Contract modifications*
  - Limit vendor service modification rights to commercially reasonable modifications to the Service, provided that they do not materially diminish the nature, scope, or quality of the Service.
- *Incorporation of URL terms*
  - In respect of references in the contract to additional terms and policies posted to the vendor's website, attempt to require the vendor to provide direct, individual notice sufficiently in advance of the effective date of any amendments to incorporated terms, along with the right to terminate if such amendments are unacceptable or materially detrimental to the customer's interests.
- *Automatic renewal*
  - Ideally, the contract should renew automatically (so you don't have to renegotiate every time), but also allow termination for convenience on some reasonably short period of notice.
- *Termination*

- Ensure that the contract describes the circumstances and terms under which a party can terminate the agreement before it expires, and the rights and liabilities of the parties in each circumstance.

- *Governing law and jurisdiction*
  - It is preferable to either: (a) specify the law and jurisdiction of your own jurisdiction; (b) provide that disputes must be brought in the defendant's jurisdiction; or (c) delete the standard vendor contract provision and leave the question open for later argument and resolution if and when needed.
  - Consider the potential impacts of contractual, legislative or regulatory requirements (e.g., mandatory data disclosure, potential for data seizure, etc.), the provider's ability to adapt to new regulations or other required changes, and the potential for the provider to move into new jurisdictions.
- *Transitioning in and out*
  - Transition-in provisions should specify how the data and services will be moved to the provider in an orderly and efficient manner and for adequate provider support.
  - Transition-out provisions should allow for an orderly and efficient transition back to the customer or another provider, ensuring service continuity and data integrity.

5.3.2 Service Level Agreements

According to the ITU Focus Group on Cloud Computing, service level agreements (SLAs) should address the following (Weissberger, 2011b):

Service User Perspective

Component	Description
Responsibilities	Cloud service users should be responsible for limits on system usage and restrictions on the type of data that can be stored
Business continuity and disaster recovery	Cloud service users should ensure their cloud providers have adequate protection in case of a disaster.
System redundancy	Cloud service users moving data and applications that must be constantly available should consider the redundancy of their provider's systems.
Maintenance	Cloud service users should understand how and when their providers will do maintenance tasks
Location of Data	Cloud service users must be able to audit the provider to prove that regulations are being followed if a cloud service provider promises to enforce data location regulations,
Security	Cloud service users must understand their security requirements and what controls and federation patterns are necessary to meet those requirements.
Transparency	Cloud service users bear the burden of proving that the provider failed to live up to the terms of the SLA under the SLAs of some cloud providers.

Component	Description
Certification	Cloud service users might have the certification requirement that their cloud provider be ISO 27001 certified.

Service Provider Perspective

Component	Description
Security	Provider must understand what they must deliver to the service users to enable the appropriate controls and federation patterns.
Data Encryption	The details of the encryption algorithms and access control policies should be specified in the SLA.
Privacy	An SLA should make it clear how the cloud provider isolates data and applications in a multi-tenant environment.
Data Retention and Deletion	Cloud providers must be able to keep data for a certain period of time and delete data after a certain period of time.
Hardware Erasure and Destruction	Cloud providers should offer the added protection of zeroing out memory space after a consumer powers off a VM.
Regulatory Compliance	Cloud providers must be able to prove their compliance if regulations must be enforced.
Transparency	Cloud providers must be proactive in notifying consumers when the terms of the SLA are breached for critical data and applications.
Certification	Cloud provider would be responsible for proving their certification and keeping it up-to-date.

Common Requirements

Component	Description
Terminology for key performance indicators	A set of industry-defined terms for different key performance indicators would make it much easier to compare SLAs in particular (and cloud services in general).
Monitoring	Trust issue need to be considered during SLA enforcement. For example consumers may not completely trust the certain measurements provided solely by a service provider and regularly employ a neutral third-party organization. The neutral third-party organization is responsible for monitoring and measuring the critical service parameters and reporting violations of the agreement from both consumer and provider. This can eliminate the conflicts of interest that might occur if providers report outages at their sole discretion or if consumers are responsible for proving that an outage occurred.
Auditability	It is vital the service users be able to audit the provider's systems and procedures. Thus, an SLA should make it clear how and when those audits take place.
Metrics	Monitoring and auditing require something tangible that can be monitored as it

Component	Description
	happens and audited after the fact. The metrics of an SLA must be objectively and unambiguously defined.
Machine-Readable SLAs	A machine-readable language for SLAs would enable an automated cloud broker that could select a cloud provider dynamically. One of the basic characteristics of cloud computing is on-demand self-service; an automated cloud broker would extend this characteristic by selecting the cloud provider on demand as well. The broker could select a cloud provider based on business criteria defined by the consumer.
Human Interaction	Although on-demand self-service is one of the basic characteristics of cloud computing, the fact remains that there will always be problems that can only be resolved with human interaction. These situations must be rare, but many SLAs will include guarantees about the provider's responsiveness to requests for support.
Cloud Brokers and Resellers	If a cloud provider is actually a broker or reseller for another cloud provider, the terms of the SLA should clarify any questions of responsibility or liability if anything goes wrong at the broker, reseller or provider facilities.

5.4 Regulation and Standards

The Open Data Centre Alliance (ODCA) has developed the following standards-related usage models for cloud computing:

- *Open Data Center Alliance Usage: Virtual Machine (VM) Interoperability* (ODCA, 2011c) – specifies actions and process to spur development of interoperable, VM management solutions aimed at lowering management complexity and costs, especially in heterogeneous, multi-vendor environments
- *Open Data Center Alliance Usage: Regulatory Framework* (ODCA, 2011d) – helps user organizations assess and monitor their regulatory obligations when engaging and acquiring cloud services

5.5 Change Management

Change management challenges that Chief Information Officers (CIOs) can expect to face in adopting cloud computing solutions include (Spires, 2011):

- CIOs must work closely with acquisition, procurement, and finance communities to address the new CC business paradigm represented by cloud computing, because the bigger change management issues lie in the business and contracting models.
- CIOs will need to address changes to the workforce; as the cloud transforms IT service delivery, they must provide leadership to address the updating of existing personnel skills and the recruitment of new staff.
- CIOs must assess the tradeoffs between the benefits of public CC with security risks associated with managing and storing sensitive data.

- CIOs will need to address their governance and management models in response to the CC leverage of the rest of the IT organization.

5.6 Reliability and Performance

The Open Data Centre Alliance (ODCA) has developed the following performance usage model for cloud computing:

- *Open Data Center Alliance Usage: Standard Units of Measure for IaaS* (ODCA, 2011e) – provides subscribers of cloud services with a framework and associated attributes used to describe and measure the capacity, performance and quality of a cloud service

Appendix 4: Geospatial Cloud Compared with Enterprise GIS

Geospatial Cloud Computing Solution	Traditional Enterprise GIS Business Solution
Overall	
Generic, non-specific to any single organization. Fast to implement. Easy to learn and use. Proven with multiple clients and implementations. Typically for non-expert users – however access to data for GIS staff and desktop applications.	Solution designed and built is specific to meet the needs of the organization. Can be difficult to design to enable growth and change. Design, build and implement process can take months / years. In-house solutions are unproven, therefore high risk. Reliance on corporate resources or hired resources for maintenance and management.
Applications and Tools	
Core software: All core and application software are included. **End User Functionality**: Usually only generic tools with basic map-based access, integration, visualization and core set of spatial analysis. **Management Functionality**: May contain other business functionality such as document management; business database reporting. Browser based so almost always available (except for planned or emergency outages). Management functionality for accounts, setup, security, built in.	**Core software**: Need to acquire appropriate software licenses for database management, GIS, O/S, Web Services, etc. **End User Functionality**: Custom applications built and/or customized to meet needs. **Management Functionality**: Need to deal with software maintenance, versioning and upgrades as they come - often from multiple vendors. Need to customize to meet specific management needs. Need to build management / maintenance capability for user account management, security, etc.
Computing Infrastructure	
Computing infrastructure is included. Guaranteed system performance with ample computing resources provisioned for growth and high use requirements. Changes in usage requirements can be handled immediately.	Computing infrastructure is bought/leased, set up and managed by internal dedicated resources. System performance and capacity are usually not configured for high use / spikes / changes in service demand. Changes in usage and resource requirements are hard to accommodate.
Content	
Will almost always include base spatial data. Often incorporates / integrates related 3rd party web information services for added value.	Generally, the data are up to the organization to manage and maintain, which can be a significant effort and cost. May supplement corporate data with a DaaS-based service. Spatial data require specialized software and staff.

Geospatial Cloud Computing Solution	Traditional Enterprise GIS Business Solution
	May require negotiations with data owners to access content.
Security	
Robust security features in place – or the vendor risks losing their business. Security typically audited and documented, although this information may be difficult for users to access. In some implementations, the "distributed architecture" enables business data to remain behind client firewall.	Security must be built into the application. This includes user account management and rules-based access. Security is critical to the system's success especially if the system is accessing data across domains and with varying levels and degrees of access. Highly specialized skills required.
Business Continuity	
Most CC vendors have several components to ensure business continuity such as: • Redundancy in the computing infrastructure for high availability with no single point of failure. • Continual backup of data and software. • Enterprise-class maintenance agreements with underlying software/ hardware vendors. • Continual monitoring and testing of systems.	Business continuity plan needs to be developed and put in place to ensure appropriate availability of all aspects of the system (application, infrastructure, and data). Need dedicated professionals to provide and manage. Can be very expensive to provision a high availability solution. Expensive and time consuming to create / maintain.
Client Support	
Usually a clear incident management process. Defined Service Level Agreement (SLA) should be put in place. Can be an issue to ensure clear lines of communication with single point of contact. However, one vendor deals with all issues.	Internal client support procedures and key performance indicators need to be defined, established and enforced. Often multiple vendors and therefore no single point of responsibility. Customer service is often an issue. Often unclear customer support / relationship management.
Cost	
Often a subscription model. Predictable. Typically is affordable or can be designed to be affordable based on requirements.	Unknown / unpredictable costs at start-up and ongoing. Multiple vendors and multiple bills can lead to errors, discrepancies, higher costs and administration.