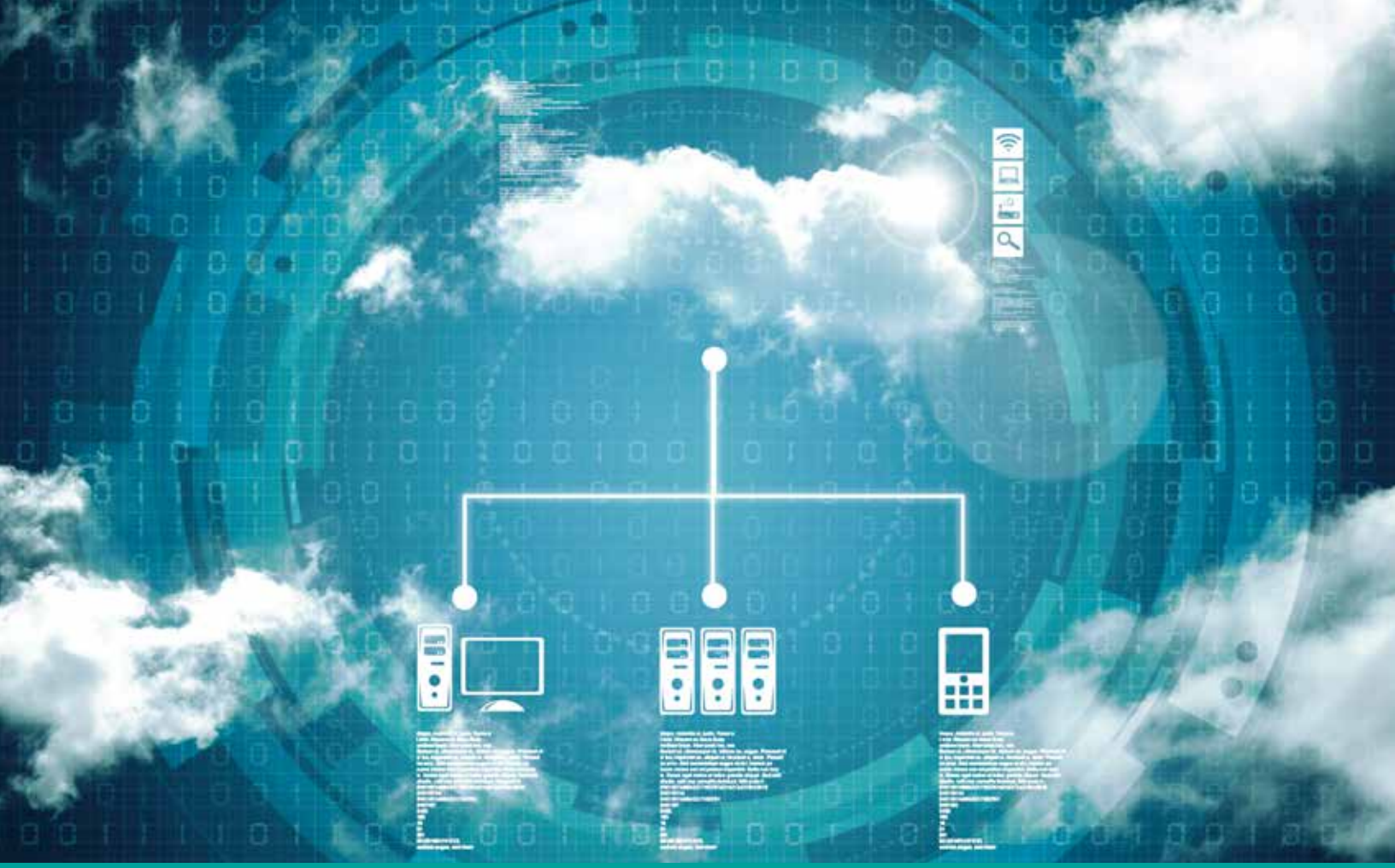

Thinking About Clouds?

Privacy, security and compliance considerations for Ontario public sector institutions

February 2016

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

CONTENTS

1. INTRODUCTION

The use of cloud computing services is increasing in popularity among public sector institutions due to the potential for cost savings and reduced administrative workload that the services entail. While cloud computing may be an attractive option for these and other reasons, the use of this type of service raises concerns about information security, privacy and legal compliance.

This guidance document has been prepared to help institutions evaluate whether cloud computing services are suitable for their information management needs. In particular, it seeks to raise awareness of the risks associated with using cloud computing services and outlines some strategies to mitigate those risks.[1]

2. WHAT IS CLOUD COMPUTING?

Cloud computing is a method of providing information and communication technology resources as a *service*. Rather than invest in traditional physical computing infrastructures, organizations with broad network access can quickly tap into a shared pool of virtually unlimited computing resources hosted elsewhere, whether maintained by them or by a third party, paying only for what software and other services are actually needed or used.

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
>
> – NIST SP 800-145

Cloud computing is an attractive option for many organizations because it offers the possibility of reduced overhead and operating costs, improved operating efficiencies and enhanced services or performance.

The term "cloud computing" describes a range of technology components including servers, storage devices, networking components and specialized cloud software. Organizations can implement cloud computing services using their own components, or they can outsource some or all of these components to a third party cloud service provider. Depending on which type of cloud infrastructure is used, a large portion of the security arrangements and information management controls could be managed by a cloud service provider, potentially reducing the organization's workload and the costs associated with the storage and processing of information.

1 This guidance is not directed at health information custodians whose handling of personal health information is governed by the *Personal Health Information Protection Act, 2004*.

CLOUD INFRASTRUCTURES

There are four main infrastructure models by which cloud computing services are used, namely, public, private, community and hybrid clouds. Public clouds refer to cloud computing services that are owned and managed by one provider for multiple organizations that pay to use the service. A private cloud is used on an organization's own private infrastructure, with services used and managed internally. Community clouds are extensions of the private cloud that involve private networks, with services shared by multiple affiliated organizations. Hybrid clouds combine attributes of the public and private cloud services and are the most common infrastructure model used by organizations.

Public Clouds: Generally, public clouds provide services to anyone over the Internet. Most public clouds are run by third parties, who own and manage the infrastructure and applications on behalf of multiple customers. The use of a public cloud can relieve the customer of the costs associated with an in-house deployment.

Private Clouds: A private cloud can be hosted and operated within an organization's own infrastructure, or within infrastructure that has been leased from a third party provider. A private cloud is built for the exclusive use of the customer and provides the ability for the greatest control over the quality of service and security of data. In most cases, the organization owns the infrastructure and has total control over how the applications are installed and used. In some cases, third parties are retained to help manage operations. A "hosted private cloud" is more flexible than a public cloud, in that it allows an organization to configure, install and operate the infrastructure that best suits its business needs.[2]

Community Clouds: Community clouds are similar to private clouds, except that the cloud infrastructure is shared by several organizations, typically with common needs. A community cloud may be managed by the organization or a third party, and may exist on the premises of the organization or the third party.[3]

Hybrid Clouds: Hybrid clouds are a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized technology that enables data and application portability. Hybrid clouds provide greater flexibility, enabling organizations to move processes between the different cloud types as needs change. An example of a hybrid cloud is one where an organization has implemented a private cloud for its sensitive applications, but also participates in a community cloud for collaboration with business partners, while using generic office services from a public cloud. One of the main advantages of hybrid clouds is that they can be used to handle sudden workload increases (also known as "surge computing"). In instances where there is a workload increase, organizations can access additional computing resources across infrastructures, effectively increasing capacity and the speed at which tasks can be completed. Since hybrid clouds offer the greatest flexibility, many cloud providers are preparing their platforms to support more hybrid type models.[4]

---

2 Sun Microsystems, ***Introduction to Cloud Computing Architecture***, white paper, June 2009.
3 Ibid.
4 Arthur Cole, "**The Future Belongs to the Hybrid Cloud**," *IT Business Edge*, September 16, 2011.

CLOUD SERVICE MODELS

There are three primary models by which cloud computing services are delivered: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Each service comes with different benefits and limitations. The three models build upon each other in terms of the number and variety of services used in each model. IaaS is the foundation of all cloud services (the bottom layer) providing the largest number and variety of services, with PaaS (the middle layer) building upon IaaS, and SaaS (the top layer) upon PaaS.

Infrastructure as a Service: IaaS is a service model that delivers basic storage and computing capabilities over a network. IaaS clouds provide customers with processing power, network-accessible storage, network infrastructure components and other fundamental computing resources, such as servers, storage systems, switches and routers. In an IaaS environment, the user is able to run any software that can range from operating systems to high performance computing applications. IaaS can be used by system developers, system administrators and information technology (IT) managers to create, install, monitor and manage services and applications. Customers can be billed according to the amount or duration of the resources consumed, such as central processing unit hours used by virtual computers, volume and duration of data stored, network bandwidth consumed or the number of IP addresses used.

Platform as a Service: PaaS is a service model that allows customers to create and use their own applications within the cloud infrastructure of the PaaS provider. Some well-known examples of PaaS services include Google App Engine, Amazon Web Services and Microsoft Azure. PaaS customers can be application developers who design, implement and publish application software; application testers who run and test applications in a cloud-based environment; and application administrators who configure, monitor and manage applications deployed in a cloud.

IaaS is the foundation of all cloud services (the bottom layer) providing the largest number and variety of services, with PaaS (the middle layer) building upon IaaS, and SaaS (the top layer) upon PaaS.

Unlike the IaaS model, the customer has no control over the cloud infrastructure. PaaS provides an environment for developers and organizations to create, host and deploy their own applications, saving them from the complexities of the infrastructure side (setting up, configuring and managing elements, such as servers and databases). With PaaS, the customer manages applications and data, while the provider manages the cloud operating system, servers, storage and networking. PaaS customers can be billed according to the number of PaaS users, the processing, storage or network resources consumed by the PaaS application, and the duration of the platform usage.

Software as a Service: SaaS (also known as "on-demand" software) is a service model where a cloud provider licenses the use of on-demand applications to its customers. Common SaaS examples include web hosting, office productivity, document storage and online collaboration tools and services. Customers can interact with this type of service as end-users who directly use software applications (such as webmail), as organizations that purchase access rights for the use of existing software for its staff, or as organizations that customize web-based services for their own, or other, organizations. SaaS providers typically host the applications on their own infrastructure, but may also install the application on the customer's networks or devices.

SaaS customers can be billed based on the number of end-users, the time of use, the network bandwidth consumed, the amount of data stored or the duration of stored data. If the applications are uploaded onto the customer's infrastructure, they are disabled once the on-demand contract expires. In a SaaS environment, the customer has no control over the cloud infrastructure with only limited capabilities to configure applications.

ADVANTAGES OF CLOUD COMPUTING

Cloud computing offers the potential to use services and applications faster than traditional computing, reducing run and response times by leveraging the infrastructure of third party cloud providers.

Organizations that contract services out to a cloud provider can add functionality, while improving operational efficiency and reducing costs by off-loading the administrative responsibilities associated with deploying and maintaining services.

In some models, organizations do not need to concern themselves with equipment purchases, scalability issues or workload limitations; rather, as cloud customers, they can purchase the on-demand services that are needed to carry out their specific business requirements.

In addition, cloud computing can more effectively address surge computing, as workload spikes can be distributed among servers to alleviate the pressure on one machine.

Finally, cloud computing can provide enhanced security with respect to risks arising in the context of traditional computing. Cloud computing may be more flexible, with access to a greater number of computing resources, allowing it to address security issues more quickly and efficiently. Many kinds of security measures are cheaper when implemented on a larger scale. Therefore, the same amount of investment in security may buy better protection.[5]

There is a wide variation in the power and functionality of cloud services available to organizations. Organizations thinking about cloud services will need to satisfy themselves that the advantages discussed above are applicable to the services under consideration.

5 "This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, etc. Other benefits of scale include: multiple locations, edge networks (content delivered or processed closer to its destination), timeliness of response to incidents, threat management." See European Network and Information Security Agency (ENISA), ***Cloud Computing Security Risk Assessment***, special report, November 2009, p. 7.

3. RISKS OF CLOUD COMPUTING

Despite the opportunities for improved operational efficiencies and services, and for reduced overhead and other costs, cloud computing introduces its own privacy, security and compliance risks that must be addressed.[6]

The discussion that follows is not an exhaustive risk analysis. Ontario public sector institutions have obligations to manage the personal information in their custody and control in ways consistent with Part III of the *Freedom of Information and Protection of Privacy Act (FIPPA)* and Part II of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* (collectively, "the Acts") and their regulations.

Regulation 460, section 4 under *FIPPA* and Regulation 823, section 3 under *MFIPPA* include specific requirements relating to privacy and security. They state:

(1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

(2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.

(3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

It is an institution's responsibility to fully assess the risks and benefits of cloud services and, in most cases, it is advisable to consult with an IT professional and to obtain legal advice.

While a wholly private cloud, administered solely by an institution for its own uses, may reduce privacy and security risks, the costs associated with this approach make it challenging, if not impossible, for most institutions. As a result, many cloud services are outsourced to, or managed by, third parties. This may result in the introduction of new risks to the privacy and security of the information involved and risks to the institution that may result from non-compliance.

Before considering which cloud infrastructure and service model are right for your institution's needs, you must determine whether you intend to process personal information in the cloud and the nature of the personal information involved. If your institution is considering a cloud computing service to manage personal information, then you should conduct a privacy impact assessment (PIA). A PIA is a risk management tool used to identify the effects of a

> The potential loss of control of information is the chief category of risk associated with moving operations to the cloud.

6 For an excellent overview of cloud computing risks, see Office of the Privacy Commissioner of Canada, ***Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing***, research paper, March 2010.

proposed or existing information technology, process, system, program or other activity on an individual's privacy. By completing a PIA, you will be able to guide your institution through a process that will identify the privacy impacts and the means to address them.[7]

PRIVACY RISKS

The use of cloud computing may introduce or heighten a number of privacy risks, including the following:

New Data Streams: New Disclosures, New Uses

Cloud services have the potential to generate new types of data streams and information, including metadata, which may become available to the cloud service provider, subcontractors and other third parties. Although these data streams may not be relevant to the original cloud operation, there are risks that they will be used either by the institution, the cloud service provider or other parties for unauthorized purposes, such as profiling and marketing. As such, consideration should be given to whether these activities constitute uses or disclosures of personal information under *FIPPA* and *MFIPPA*. If they do, the institution must ensure that there is proper legal authority for them.

Unauthorized Processing/Secondary Purposes

Institutions should consider that cloud service providers may inappropriately access, manipulate or mine the information entrusted to them for purposes not specified or authorized in their contract or under *FIPPA* and *MFIPPA*.

Access and Correction Rights

FIPPA and *MFIPPA* include individual rights to access records and to seek correction of personal information. Institutions must ensure that their arrangements with cloud service providers will not negatively impact their ability to comply with their statutory obligations.

Institutions must ensure that their arrangements with cloud service providers will not negatively impact their ability to meet their access to information and correction obligations.

Covert Surveillance

If your institution uses a shared cloud infrastructure, law enforcement requests for access to information in the control of the cloud service provider could result in the inadvertent, or intentional disclosure of additional information beyond what is required to respond to the request, including information owned by other organizations. In addition, the cloud infrastructure increases the risk that individuals and the institutions with custody of their information will be unaware of these disclosures; that is, disclosures may take place without the knowledge or involvement of the institution.

7 For further information about how to conduct a PIA, see IPC, ***Planning for Success: Privacy Impact Assessment Guide***, May 2015.

INFORMATION SECURITY RISKS

Maintaining the confidentiality, integrity and availability of information is a significant concern when dealing with cloud service providers. Any scenario that results in the sharing of control of your institution's information holdings represents a potential threat, since the service provider's infrastructure and security safeguards may be insufficient. Security management is an ongoing challenge when outsourcing services to cloud providers.[8]

Security management is an ongoing challenge when outsourcing services to cloud providers.

For example, you may have no control or input into the operational and functional capabilities of your cloud service provider, or the security associated with safeguarding information. Information may be encrypted in transit and in storage, but processing typically requires working on unencrypted information. Consequently, the following security risks need to be considered.

Insider Threats

Greater and more frequent access to larger amounts of information increases the risks posed by insiders. Cloud architecture requires that certain administrative staff manage the data held within the cloud and the security of the cloud. These individuals have significant access and power, potentially increasing the risks of inappropriate access to or use and disclosure of information. The risks may be heightened in those cases where cloud service providers, their staff and any subcontracted agents have the ability to access information without detection or producing an audit trail.

Breach Detection, Remediation and Reporting

Cloud computing may compromise an institution's ability to detect unauthorized access, use or disclosure of information stored and processed with a cloud provider. This may increase the risks of failing to properly deter, contain and remediate breaches when they occur, and to comply with breach reporting requirements.

Backups

Information ownership questions may arise due to potential replication of information within cloud-based infrastructures. An institution may not know that copies of its information have been created, and this can become a significant issue if the cloud service provider claims ownership of the new copies of the information. Backups also increase risks of interception, unauthorized access, use and disclosure and insecure deletion or destruction. Conversely, in some cloud services, there may be no backups at all, which introduces different risks if the information becomes corrupted or otherwise unavailable.

8 Security management covers data protection, operational integrity, vulnerability management, identity management, business continuity and disaster recovery.

Remote Access

Remote access or browser-based interfaces between the cloud service and individual users may make information more vulnerable to attack, as more data is in transit than in traditional computing. Institutions must critically evaluate a cloud service provider's security practices to ensure that they meet required standards.

Multi-tenancy (Non-segregation)

Cloud computing's strength is founded on shared computing resources that can be instantly accessed in response to demand. This means that an institution's information will typically share storage, memory and routing with unrelated organizations, a situation called "multi-tenancy." However, multi-tenancy introduces risks that information may be accessed by unauthorized parties if not properly segregated. These risks are less significant in the case of private and community clouds.

Data Permanence

Data permanence is also a risk that institutions must consider. Information must be securely retained while held by the cloud provider, but must also be securely deleted in accordance with your institution's records retention requirements. Some cloud services may not be able to fully delete information. This may occur in cases where the cloud provider has stored extra copies of data in inaccessible locations or if the deletion will impact data of other cloud customers.

Loss of Access

Cloud computing services, being remote in nature, necessarily depend upon reliable, secure high-speed access between the institutional customer and the cloud service provider. Any interruption of access introduces risks of compromising operations and services. This is a risk factor regardless of the cloud infrastructure or service model that you may choose. Even if you do not know where your data is, a cloud provider should tell you what will happen to your information and service in case of a disaster.

"Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," says Gartner, Inc., a global IT research and advisory firm. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."[9]

OTHER COMPLIANCE RISKS

In addition to the need to comply with *FIPPA*, *MFIPPA* and their regulations, Ontario public sector institutions must verify that cloud service providers do not store and process information in a manner that may violate existing institutional policies, other legal requirements or contractual agreements. Certain compliance risks are increased whenever an institution hands over control to a third party.

Jurisdiction

One of the primary concerns with outsourcing to cloud providers is the risk that the data and/or applications offered by the cloud provider may be physically located and housed outside of

9 Jay Heiser and Mark Nicolett, Gartner, Inc., ***Assessing the Security Risks of Cloud Computing***, special report, June 3, 2008.

the institution's legal jurisdiction. In addition, information stored and processed with a cloud service provider may leave the jurisdiction when in transit from your institution to the cloud provider. Information transmitted or stored outside of the country or managed by a foreign owned provider could be subject to the laws of the country housing the data or that of the provider. These laws may be substantially different from Ontario laws. For example, in the event of a dispute with the cloud service provider, institutions may be forced to seek remedies under foreign regulatory regimes.[10] These risks may be compounded if the cloud service provider subcontracts processing to agents and partners located in other jurisdictions.

Audit/Certification

It may be difficult to audit your institution's information management practices in a cloud environment, particularly where other organizations share a common infrastructure. Cloud service providers may be reluctant to allow customers to directly audit their facilities and practices, and may insist that the institution accept their own assessments and reports or those of third parties chosen by the provider.

Lock in/Portability

Institutions run the risk of being "locked in" to a single cloud service provider. Without adequate guarantees of access to data, application and service portability, it may be difficult for the institution to migrate from one provider to another, or to migrate data and services back to an in-house IT environment. This introduces the risk of dependency on a particular cloud service provider.

Some cloud providers use contracts of adhesion, which means institutions that seek their services will not have the power to negotiate or modify the terms. This poses significant compliance and other risks.

Contracts of Adhesion

A "contract of adhesion" is a standard form "take-it-or-leave-it" contract drafted by one party. Some cloud providers use contracts of adhesion, which means institutions that seek their services will not have the power to negotiate or modify the terms. This poses significant compliance and other risks. The main risk is that the terms of service that govern the relationship with the cloud service provider may allow for the collection, use, disclosure and retention of information by the provider that is contrary to the Acts. Therefore, these standard contracts may not enable compliance with *FIPPA* and *MFIPPA*, their regulations and other relevant legislation or government policy guidelines. Moreover, the cloud provider may have the right to unilaterally change the contractual terms, making the evaluation of risks at the outset challenging.

Some cloud providers are reluctant to enter into customized contracts as they benefit from economies of scale associated with the delivery of identical services to their various clients. While larger institutions may have the ability to negotiate special arrangements, smaller institutions may not have that ability.

10 The IPC provides guidance on outsourcing in ***PC12-39: Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report***, June 2012.

4. RISK MITIGATION STRATEGIES

The following risk mitigation strategies should be considered if your institution is thinking about using a cloud service provider to process and store personal information. Consult with your privacy, security and legal staff about requirements and practices that may be specific to your institution and your project.

KNOW YOUR LEGAL AND POLICY OBLIGATIONS

There is no legal prohibition in Ontario against outsourcing computing services to a third party cloud service provider. This applies regardless of whether the third party stores personal information in a foreign jurisdiction. However, *FIPPA* and *MFIPPA* and their regulations do impose legal requirements that must be met regardless of where the data resides or is processed.

The critical question is whether your institution has taken reasonable steps to protect the privacy and security of the records in its custody and control.[11] Accountability for meeting legal and policy requirements to protect personal information rests with institutions, whether or not they choose to outsource to external service providers. As such, institutions must ensure that their arrangements with cloud service providers will not negatively affect their compliance with the Acts. Obtaining an appropriate solution requires prudence, diligence and vigilance on the part of the cloud customer. At a minimum, institutions should conduct feasibility assessments to determine if existing legal and policy requirements allow for the provisioning of external services of this nature.

The existence of relevant mandates, policies and standards adopted by the institution should also be acknowledged and considered at the outset. For example, your institution's procurement policies may specify additional requirements and conditions about engaging third party services, and standardized contract clauses may be required.

BUILD YOUR BUSINESS CASE

Is outsourcing to the cloud the best option? Institutions considering the use of cloud based services are strongly encouraged to develop a comprehensive business case for migrating to cloud services. A project management approach is recommended, involving the following actions:

- Engage your privacy, security and IT staff in the cloud project from the beginning to ensure that privacy and security issues are considered as early as possible.
- Consult with internal and external stakeholders, including end-users, to understand, document and communicate cloud project requirements, organizational capabilities and assigned roles.
- Review current information security management policies and processes to assess how these would be addressed or supported in various cloud infrastructures, service models and use case scenarios.

11 For additional details see section 3 of Regulation 823 under *MFIPPA* and section 4 of Regulation 459 under *FIPPA*.

- Identify privacy and security risks associated with the proposed project design and operation and identify which cloud solution, if any, best matches the institution's needs. Conducting threat and risk assessments (TRAs) and PIAs is considered to be a privacy and security best practice. They will help identify risks and mitigation strategies.
- Get executive buy-in and sign-off to ensure accountability for all project-related decisions that impact privacy, security and compliance.

MINIMIZE PERSONAL INFORMATION

Data minimization refers to the practice of reducing the amount of personal information collected, used or disclosed to the minimum extent necessary. This practice supports privacy and security and reduces risks, as there is less information to protect against loss, theft or misuse. Good privacy and security design ensures that institutional programs, computing processes and end-users collect, use and disclose personal information only when necessary and for narrowly defined, legitimate purposes.

In the context of cloud computing, one strategy is to segregate personal information for local "in-house" processing, perhaps in the form of a non-hosted private cloud, while using other cloud computing services to handle public and non-sensitive data processing. According to statements made by the Ontario government, this is the approach it has taken to date.[12]

Encryption tools and methods can minimize information exposure and risk. Encrypting personal information at rest and in transit is a best practice that helps ensure effective organizational control of information in the cloud.[13] In some circumstances, encryption may even be used during processing.[14] In all instances, it is essential that encryption and decryption keys be securely generated and managed, and remain under the exclusive control of the institution.

Tokenization is a promising area of security-enhancing technology, where identifiable data is replaced with a random surrogate value. Tokenization methods allow cloud customers to use some cloud computing services, but to effectively retain personal information "in-house."[15]

Good privacy and security design ensures that institutional programs, computing processes and end-users collect, use and disclose personal information only when necessary and for narrowly defined, legitimate purposes.

12 The Ontario.ca website contains only publicly-available information and has been moved to Amazon's cloud servers while high sensitivity data such as personal information is stored in government-run data centres. See Andrew Brooks, "**Ontario data centre shutdown will save $20 million, province says,**" *IT World Canada*, May 13, 2014 and Jesse Ward, "**Ontario closing 20 data centres as it moves to cloud computing,**" *Global News*, May 7, 2014.

13 IPC, ***Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach***, May 2010.

14 For example, homomorphic encryption. See Erica Naone, "**Homomorphic Encryption: Making cloud computing more secure,**" *MIT Technology Review*, May/June 2011.

15 For a discussion of tokenization in the context of cloud computing services, see Office of the Information and Privacy Commissioner for British Columbia, ***Updated guidance on the storage of information outside of Canada by public bodies***, June 16, 2014.

De-identification techniques and re-identification risk management procedures are some of the strongest and most important tools to protect the privacy and security of personal information.[16]

Comprehensive PIAs will help identify where to best apply data minimization methods in order to reduce risks.

KNOW YOUR CLOUD SERVICE PROVIDER

It is a prudent business practice to carefully consider all service providers and agents and their services before entering into contractual relations with them. Cloud service providers are no exception. In fact, they should be subjected to additional scrutiny, commensurate with the scope and scale of the functions they may perform on behalf of your institution and the sensitivity of the information involved. In your review, obtain answers to the following questions:

- Is the cloud provider solvent and reputable, and does it have a credible performance record, especially regarding security and privacy compliance issues? Ideally, your cloud service provider will never become insolvent or be acquired by another company. You must be sure your information will remain available even after such an event, including rights to application source code needed to access the information. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application."[17]
- Do you fully understand the cloud provider's product and service offerings? Does the cloud service provider adhere to recognized standards? What are the standards and how do they relate to the cloud provider's services?[18]
- Are the cloud provider's information management policies and practices documented, available and described in sufficient detail? Knowing the cloud service provider means knowing how they run their business and having confidence that their operations will be a good fit with that of the cloud customer.
- Where will your information be processed and stored? You should understand the implications of processing and storing information in other jurisdictions. You should also understand any available options and remedies for the negative effects, if any, arising from processing and storage methods.
- Does the cloud provider subcontract any part of its operations? If so, to whom and under what circumstances does subcontracting occur and do you have any input into or say over these practices?

16 IPC, ***De-identification Protocols: Essential for Protecting Privacy***, June 2014.
17 Gartner, Inc., ***Assessing the Security Risks of Cloud Computing***.
18 For a good discussion of relevant cloud standards, see National Institute of Standards and Technology (NIST), ***SP 500-293: US Government Cloud Computing Technology Roadmap, Vol II***, special publication, October 2014.

- Can you carry out site visits and audits and, if so, under what circumstances? According to Gartner, Inc., "cloud services are especially difficult to investigate because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."[19] If the cloud provider adheres to recognized privacy, security and accountability standards, then institutions can sometimes rely on independent audits, evaluations, assessments and certifications to enhance confidence and trust in the provider.
- Do the cloud provider's standard contractual terms and conditions, and service-level agreements (SLAs), satisfy your compliance requirements?

NEGOTIATE COMPREHENSIVE AND ENFORCEABLE CONTRACTS

Contract provisions are critical for ensuring the cloud service provider's compliance with an institution's privacy, security and access obligations. Contracts should have provisions that address:

- information ownership,
- limits on information collection, use and disclosure,
- limits on the jurisdictions in which the information may be stored,
- treatment of confidential information (including personal information),
- employee awareness and training,
- limits on subcontracting,
- security management including logging and auditing,
- breach incident response, management and notification,
- information retention and destruction,
- periodic vulnerability assessments,
- the availability of audit results,
- governing law and jurisdiction and
- enforceable remedies for non-compliance.[20]

Contractual terms should include specific measurable criteria for judging whether privacy and security standards are being met. Industry standards, corporate guidelines or any other information management obligations should be reflected in contracts and SLAs to ensure that cloud providers adhere to business requirements. Cloud services should be regularly monitored and evaluated to determine whether they should be continued. Cloud service providers should also be able to supply the appropriate documentation to validate that their infrastructure and service models meet your institution's requirements.[21]

---

19 Gartner, Inc., ***Assessing the Security Risks of Cloud Computing***.

20 For a discussion regarding contractual provisions related to outsourcing, see IPC, ***PC12-39: Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report***, June 2012, pp. 7-9

21 For example, ISO 27001 security framework standard and associated controls (e.g. 27002, 27018). See International Organization for Standardization, **"ISO/IEC 27001 - Information security management."**

Standards

It may be easier to evaluate the nature and quality of the cloud services being offered when the provider has been assessed or certified as adhering to one or more industry standards. In these circumstances, institutions have an independent basis on which to conduct their evaluation of the services.

Understand the limits and applicability of relevant standards.

Up-to-date, relevant cloud-related security, performance, interoperability and portability standards are important to the successful design, deployment and operation of cloud computing projects. Widely agreed-upon standards, verifiable by third parties, can be cited in contracts and SLAs to demonstrate effective accountability.

A number of third party audit/reporting frameworks and certification schemes exist to help customers evaluate the security controls in place for a given cloud service provider. Some frameworks focus on accountability and transparency, in addition to security and assurance.

The International Organization for Standardization (ISO), the US National Institute for Standards and Technology (NIST), and some private-sector organizations, such as the American Institute of Chartered Public Accountants (AICPA) and the Cloud Standards Alliance (CSA), have developed standards applicable to cloud computing services that provide some degree of assurance about the services offered by providers that meet those standards.

ISO/IEC 27018 — *Code of practice for personal information (PI) protection in public clouds acting as PI processors* (ISO 27018) — is a voluntary international standard that establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personal information processed in a public cloud computing environment. ISO 27018 includes guidelines that are based on the information security standard ISO/IEC 27002.[22] Implementation of the standard by cloud providers may vary. Therefore, institutions need to ensure that their contract with a cloud provider is comprehensive and satisfies their legislative and other requirements.

Service Organization Control (SOC) evaluation reports are based on the AICPA AT 101/SSAE 16 *Trust Principles*,[23] and examine operational controls, including security and privacy. Type I reports examine the design of operational controls for a specified point (or "snapshot") in time, while Type II reports include testing the effectiveness of those controls and their likely efficacy over a specified period of time.[24]

22 ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems.

23 For more information, see American Institute of CPAs (AICPA), "**Trust Services Principles and Criteria**."

24 For more information, see American Institute of CPAs (AICPA), "**Statements on Standards for Attestation Engagements**."

The CSA Security, Trust and Assurance Registry (STAR) is a cloud service assessment and assurance program intended to help cloud service providers demonstrate security controls and maturity.[25] STAR is based on several widely recognized reporting and certification standards.[26]

In addition, it may be worth noting that authorities in some other jurisdictions have mandated government-wide "Cloud First" policies that require public institutions to evaluate safe, secure cloud computing options before making any new investments.[27] To this end, national regulators have prescribed standards and other criteria to be observed when public institutions outsource to the cloud. These criteria vary by jurisdiction. For example, the US Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization and continuous monitoring of cloud products and services for US government institutions.[28] Unlike some cloud service adoption models, FedRAMP requires that assessment and authorization be based on independent review and evidence. In the UK, the GOV.UK Digital Marketplace (formerly CloudSpace) offers similar "G-Cloud" evaluation services for the benefit of UK government customers.[29]

Some standards only specify what issues need to be addressed, but not how they are resolved. Institutions must understand the limits and applicability of these standards when engaging cloud providers who claim to be or are certified compliant.

Ensure that legal, technical and organizational mechanisms are in place so that actual or suspected privacy breaches are reported and acted upon in a timely manner.

HAVE AN INCIDENT MANAGEMENT PLAN

- Develop plans to address potential problems such as interrupted access to cloud computing resources or privacy breaches.
- Retain the ability to access personal data at any time, make corrections and investigate any allegations of non-compliance.
- Ensure that legal, technical and organizational mechanisms are in place so that actual or suspected privacy breaches are reported and acted upon in a timely manner.

25 See Cloud Security Alliance, "**CSA Security, Trust & Assurance Registry (STAR)**."
26 See Cloud Security Alliance, "**Cloud Controls Matrix Working Group**."
27 For example, see Vivek Kundra, United States White House CIO, ***Federal Cloud Computing Strategy***, special publication, February 8, 2011 and UK Cabinet Office, "**Government adopts 'Cloud First' policy for public sector IT**," press release, May 2013.
28 FedRAMP draws upon NIST SP 800-53 as a basis for controls. See National Institute of Standards and Technology (NIST), ***Security and Privacy Controls for Federal Information Systems and Organizations***, special publication, April 2013.
29 See UK Digital Marketplace, "**Digital Marketplace**" and "**Digital Marketplace guidance G-Cloud framework**."

- Ensure that your institution can take control of the notification and investigation procedures in the event of a real or suspected breach. Cloud service providers should be required to:
    - notify the institution promptly of any theft, loss or unauthorized use or disclosure of personal information,
    - notify the institution of any request for disclosure of personal information by a law enforcement authority, when legally permitted to do so,
    - deny requests for personal information that are not legally binding and
    - consult the institutional customer, when legally permitted to do so, before disclosing personal information.

An incident management plan should anticipate the privacy risks and the key steps needed to mitigate those risks.[30] The plan must go further than simply seeking to contain breaches, and should allow for the full termination of the contract with the cloud service provider in appropriate cases.

30 See IPC, ***Privacy Breach Protocol Guidelines for Government Organizations***, May 2014.

5. CONCLUSION

There is growing interest in and use of cloud computing services by public sector institutions across Ontario.

However, the expected benefits of migrating internal operations to the cloud need to be tempered by an acknowledgement of the privacy, security and compliance risks associated with "outsourcing" personal information to third parties for processing and storage.

The IPC advocates an informed, principled approach under *FIPPA* and *MFIPPA* when considering cloud computing services. This should include appropriate planning, consultation and co-ordination, project documentation, risk analyses, data minimization, due diligence, effective contracts and a credible incident management strategy.

The intent of this paper and the recommended mitigation strategies is to ensure that Ontario public institutions remain effectively in control of, and fully accountable for, the personal information entrusted to them by Ontarians under *FIPPA* and *MFIPPA*.

Institutions should consult legal and other relevant expertise whenever undertaking significant cloud-related initiatives that may have an impact on the privacy of Ontarians.

RESOURCES

RELEVANT LEGISLATION:

Freedom of Information and Protection of Privacy Act

- **Freedom of Information and Protection of Privacy Act**
- **Disposal of Personal Information — RRO 1990, Reg 459**
- **General — RRO 1990, Reg 460**

Municipal Freedom of Information and Protection of Privacy Act

- **Municipal Freedom of Information and Protection of Privacy Act**
- **General — RRO 1990, Reg 823**
- **Institutions — O Reg 372/91**

ONTARIO GUIDANCE:

Government of Ontario

Ontario.ca e-Business Toolkit. "**Cloud Computing**" (2015)

Office of the Information and Privacy Commissioner of Ontario

PC12-39: Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report (June 2012)

Planning for Success: Privacy Impact Assessment Guide (May 2015)

GUIDANCE FROM OTHER JURISDICTIONS:

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia

Cloud Computing for Small and Medium-sized Enterprises: Privacy Responsibilities and Considerations (joint publication — 2012)

Office of the Privacy Commissioner of Canada

Fact Sheet: Introduction to Cloud Computing (October 2011)
Reaching for the Cloud(s) (March 2010)

Office of the Information and Privacy Commissioner for British Columbia

Cloud Computing Guidelines for Public Bodies (June 2012)

KPMG

Exploring the Cloud — A Global Study of Governments' Adoption of Cloud (2012)

Dentons

Privacy and Cybersecurity Guidance: Cloud Computing in the MUSH Sector (July 2015)

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three Acts, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction,**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations,**
- **Conducts research into access and privacy issues,**
- **Comments on proposed government legislation and programs and**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

February 2016