Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

# Government of Canada White Paper: Data Sovereignty and Public Cloud

Published: 2018-06-25

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-213/2018E-PDF
ISBN: 978-0-660-27233-7

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Gouvernement du Canada Livre blanc : Souveraineté des données et nuage public

Government of Canada | Gouvernement du Canada

# Government of Canada White Paper: Data Sovereignty and Public Cloud

**From Treasury Board of Canada Secretariat**

The Government of Canada (GC) has a “cloud-first” strategy whereby cloud services are identified and evaluated as the principal delivery option when initiating information technology (IT) investments, initiatives, strategies and projects. Departments and agencies should consider cloud deployment models in the following order of priority:

1. public cloud
2. hybrid cloud
3. private cloud
4. non-cloud

The cloud-first strategy is reflected in recent updates to the Treasury Board Policy on Management of Information Technology (section 6.2.6).

The Treasury Board of Canada Secretariat (TBS), in consultation with key departments, [1] has determined that a commercial public cloud can, under certain conditions, offer sufficient protections for data up to and including the Protected B level. As such, “protected-cloud” procurement will be launched in 2018 in order to make commercial public cloud services available to departments for storage of data up to and including the Protected B level.

## On this page

# Purpose of this paper

The purpose of this paper is to provide an overview of the risk to data sovereignty [2] that is associated with using commercial public cloud environments. The risks to data residency [3] and security are also discussed. These risks are examined in the context of the GC's cloud-first strategy. By the end of this paper, the reader will understand these risks and the associated mitigation measures. The reader will also understand how cloud services can help the GC address other risks, such as:

- aging IT
- current security gaps
- not benefiting from emerging technology

# Outside of this paper's scope

This paper is not meant to provide a comprehensive overview of public cloud services or the GC's strategic direction regarding those services. Other documents, such as the Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021 and the Government of Canada Cloud Adoption Strategy, are available and provide information about cloud services and strategic direction.

# What is the cloud?

Cloud computing is the delivery of on-demand computing resources (from applications to data centres) over the Internet on a pay-for-use basis. Cloud services can be deployed using 3 different models: public, private and hybrid.

In the public cloud model, cloud resources (that is, hardware, software and infrastructure) are owned and operated by a third-party cloud service provider (CSP). Organizations consume IT services over the Internet from a shared pool of resources that are logically separated from one another. In the private cloud model, computing resources (that can be located on the premises or hosted by a third-party CSP) are dedicated to one organization and maintained on a private network. In the hybrid cloud model, both public and private clouds are used with data and applications communicating between the two.

# Challenges associated with the public cloud

**In this section**



Cloud computing is a fundamental shift in the delivery of IT services, and the GC needs to be ready to leverage this alternative service delivery model. However, because the nature of cloud computing results in an organization having a modified span of control over its information assets, a number of challenges related to data control, protection and privacy have been noted within the GC. These challenges relate to:

- data security
- data residency
- data sovereignty

## Data security

When data is moved to the cloud, security becomes a shared responsibility with CSPs. CSPs are responsible for the security **of** the cloud, and GC departments are responsible for security **to**, **from** and **in** the cloud. A simple analogy would be a rental building. Property owners or managers are responsible for the security of the building and common areas, but renters are responsible for the security measures within the units they rent. The modified span of control and shared responsibility often lead to fears that an organization's security posture may be degraded.

### Case study: the United Kingdom and a risk-managed approach

In 2013, the UK government introduced a "cloud-first" policy and a shift toward a risk-management approach to using cloud services. The UK government cloud strategy does not impose geographic limitations on public cloud services for information classified as official (there are limitations for information classified as secret and top secret). Rather, a risk-managed approach has been adopted and supported by the UK's National Cyber Security Centre with its 14 Cloud Security Principles for organizations to consider when evaluating a cloud service. Cloud security principle 2, asset protection and resilience, emphasizes the need for public sector organizations to understand:

- in which countries data will be stored, processed and managed, and how these locations will affect compliance with relevant legislation
- whether the legal jurisdiction(s) within which the service provider operates are acceptable to the organization

## Data residency

CSPs are typically hyper-scale providers, meaning that they have global deployment on a scale that eclipses the GC's own IT assets many times over. Although CSPs have the ability to move a client's data anywhere in the world, the client typically has the option to isolate their data to a given geographical region. This is an important feature because it allows the client to keep data under the laws and policies of a particular territory. Moving the GC's data outside of the geographic boundaries of Canada could impact the GC's access to data and services that are vital to its business continuity.

## Data sovereignty

Regardless of where the cloud resources are physically located, when data is stored in a cloud environment, the stored data may be subject to the laws of other countries. As previously mentioned, CSPs are hyper-scale providers that have global deployment. A CSP with foreign operations could be required to comply with a warrant, court order or subpoena request from a foreign law enforcement agency seeking to obtain GC data. This means that Canada cannot ensure full sovereignty over its data when it stores data in the cloud. Lack of full data sovereignty has the potential to damage the GC and third parties. Sensitive GC data could be subject to foreign laws and be disclosed to another government. Under some foreign laws, disclosure of GC data could take place without notice to the GC.

### Case study: British Columbia and full data residency

The Office of the Information and Privacy Commissioner for British Columbia released Cloud Computing Guidelines for Public Bodies (PDF (Portable Document Format), 175 KB (Kilobyte)) (updated in June 2012) to provide guidance on how to apply British Columbia's Freedom of Information and Protection of Privacy Act (FIPPA). FIPPA applies to **personal information** that is **in the custody or under the control of a public body**. Strict data residency measures have been put in place to ensure that personal information is protected and adheres to FIPPA. According to the guidelines, subject to a few exceptions, British Columbia's public bodies are required to:

- ensure that “personal information is only stored in and accessed from inside Canada”
- “protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal”

# Addressing the challenges

**In this section**



The GC has made progress in its efforts to address the data security, data residency and data sovereignty challenges in order to enable the adoption of cloud computing.

## Data security

As previously mentioned, the shared responsibility for security in the cloud and the hyper-scale nature of CSPs mean that the GC needs to use different processes to meet policy requirements for managing security risks when using the cloud. CSPs do not assess themselves against GC guidelines, such as ITSG-33. [4] Instead, they meet internationally recognized certifications, such as the International Organization for Standardization’s ISO 27001. The GC has published the Government of Canada Security Control Profile for Cloud-based GC IT Services that cross-references ITSG-33 with prevalent cloud industry certifications. The GC has also published the Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) to support departments and agencies in their understanding of existing TBS security policy requirements in the context of cloud computing. SPIN highlights:

- the key security measures required to protect GC information and assets in a cloud environment
- which security controls are the responsibility of the CSP and which ones remain a departmental responsibility

## Data residency

The GC has published the Direction for Electronic Data Residency, which sets out the Canadian residency requirements for data at the Protected B, Protected C and Classified levels. These requirements are embedded in recent updates to the Treasury Board Policy on Management of Information Technology (section 6.2.7). However, limiting residency to Canada introduces 2 new risks:

1. Limiting data storage to Canada may limit the market availablility of solutions. At the time of writing, at least 5 of the largest CSPs have the ability to isolate data in Canada.
2. Limiting data storage to Canada may be viewed as being a barrier to trade. Trade considerations and the related legal risk have been the subject of legal advice prepared by the Department of Justice Canada in the context of the recent updates to the Policy on Management of Information Technology. When procuring their own cloud services, departments may wish to review this advice.

### Data sovereignty

As long as a CSP that operates in Canada is subject to the laws of a foreign country, Canada will not have full sovereignty over its data. This is because there remains a risk that data stored in the cloud could be accessed by another country. The issue of data sovereignty is complex and continuously evolving as foreign laws are being tested in foreign courts.

## Data sovereignty: risks and mitigations

**In this section**



In the public cloud environment, government data is entrusted to a third party that may be subject to the laws of a foreign country, even if the data resides in Canada. As such, the key risk to the GC with respect to data sovereignty is that foreign agencies can leverage laws in their home country to compel CSPs to turn over the GC's data. This could:

- damage the GC
- cause Canadians to lose trust in their government

It should be noted that many countries, including Canada, have laws that allow them to subpoena private organizations or obtain a warrant for information from such organizations to support legal investigations. The primary risk to data sovereignty is the US Foreign

Intelligence Surveillance Act (FISA) and the US government's ability to compel an organization subject to US law to turn over data under its control, regardless of the data's location and without notifying Canada. It is important to note that there are long-standing information-sharing agreements between security and law enforcement agencies in Canada and the US. Those long-standing agreements, as well as mutual legal assistance treaties, are other methods for the US to obtain access to information held in Canada.

There are a number of mitigations that the GC is recommending to reduce the risk of unauthorized access to sensitive information. They include:

- limiting the categories of data stored in the cloud
- encrypting the data
- using standard contract clauses

## Limiting the categories of data stored in the cloud

Following the lead of other countries, Canada will be limiting the categories of data that may be stored in the cloud. To date, major CSPs have asserted their ability to meet the GC's requirements for storing and processing Protected B data. This assertion will be tested by the GC as it procures cloud services for Protected B scenarios. For this reason, the GC has stated that only data up to and including Protected B may be deployed to a public cloud.

## Encrypting the data

When using cloud services, encryption can provide a high degree of segregation to protect personal and other sensitive information. Data that is encrypted using a strong cryptographic algorithm is protected from anyone who does not have the decryption key. The GC will be directing that:

- all protected data hosted in the cloud be appropriately encrypted while in transit and at rest
- the GC maintain exclusive control of the encryption keys

It should be noted that if the encrypted data is to be processed in the cloud by an application, the data would need to be decrypted before processing. As a result, an unencrypted snapshot of the data would be stored temporarily in the cloud before being overwritten. The GC will continue to investigate techniques available to mitigate this risk and prevent the exposure of data to unauthorized parties. Possible mitigation techniques include data anonymization and hardware-level isolation.

## Using standard contract clauses

Contracting authorities should ensure that all contracts with CSPs include clauses that compel the CSP to disclose all unauthorized access to data, including access made under court order, where applicable and unless the CSP is prohibited from doing so by law. There are some cases where such disclosure is forbidden under US law, such as in the case of an order by the US Foreign Intelligence Surveillance Court. The GC may request that CSPs provide their procedures for navigating the conflict between their contractual obligations and applicable laws.

# Balancing security risks with business benefits

**In this section**



So far, this document has focused on the most complex risks associated with public cloud adoption. At this point one might ask, with all of these risks, why would the GC adopt the public cloud? The simple answer is that there are substantial business benefits associated with using cloud services. When weighing the risks associated with the cloud, one must also consider the risks associated with the status quo and consider how the cloud can help the GC address those risks. The risks associated with the status quo include:

- aging IT infrastructure
- cyber hygiene gaps
- the availability of non-cloud solutions
- GC plans for a digital transformation

## Aging IT infrastructure

The GC's mission-critical IT infrastructure is aging and at risk of breaking down. It must be renewed. IT infrastructure transformation is proceeding more slowly than anticipated, in part due to the complexity and challenges of consolidating the data centres, networks and email systems of 43 departments. As stated in the Shared Services Canada Resource Alignment Review, cloud computing presents a significant opportunity to address these challenges and achieve cost savings. A key driver for cloud adoption is the need to move from managing aging assets to focusing on using commercially available services to deliver business value.

## Cyber hygiene gaps

The rising number of security incidents has demonstrated the inconsistent security posture of GC systems. Lessons learned have highlighted challenges in the GC's ability to quickly identify assets and perform timely patching and remediation of known vulnerabilities. These challenges leave the GC exposed to cyber threats. Moving to the cloud provides the GC with an opportunity to:

- deploy secure virtual environments rapidly
- change its approach to managing its assets and addressing security from the outset

CSPs have a significant budget to maintain, patch and secure their cloud infrastructure. This means that CSPs can:

- mitigate many common risks that government organizations often face
- provide a much stronger overall security posture

Leading CSPs also subject their services and processes to multiple third-party audits and meet numerous internationally recognized industry certifications, such as ISO 27001, to provide assurance to their clients.

## Availability of non-cloud solutions

Increasingly, industry is providing only public cloud solutions or focusing their efforts on cloud services. The expression "born in the cloud" signifies that a particular solution has been designed to reside natively in a public cloud and that no software equivalent exists. Excluding cloud solutions from the GC's IT landscape would limit the solutions that are available.

## GC plans for a digital transformation

The GC's demand for IT capacity and capabilities exceeds the available supply. The GC wants to follow the global trend of improving digital services for its citizens, and this can be greatly enabled by cloud services. Many governments have put into effect "cloud-first" policies, including in the other countries that make up the Five Eyes: the United States, the United Kingdom, Australia and New Zealand. Canada is the only Five Eyes country without a cloud-first policy. Failing to make the cloud part of the GC's digital landscape will impact how quickly the GC's digital vision can be achieved.

# Summary

Recent updates to the Policy on Management of Information Technology reflect the GC's cloud-first strategy. Departments are therefore required to consider the use of cloud services as the principal delivery option for data storage based on business needs. When considering the use of cloud services, departments should keep in mind the following:

- At this time, only data up to and including Protected B level should be stored in a commercial public cloud environment
- If it meets their needs, departments will be able to use the protected-cloud contract (which is currently in the process of being procured) to access cloud services
- Departments that choose to procure their own cloud services should:
  - assess the inherent risks to data sovereignty, data residency and data security
  - apply relevant mitigation measures
- The use of cloud services is subject to the following:
  - Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)
  - Direction for Electronic Data Residency

# Next steps

**In this section**

- Develop data encryption guidelines for cloud
- Establish standard contract clauses for clouds
- Initiate protected-cloud procurement

The GC has the responsibility to:

- safeguard the confidentiality, integrity and availability of GC information and IT assets
- implement appropriate measures to ensure the protection of data

This responsibility remains the same whether the information and assets are located on the premises of a GC facility or off the premises within a cloud environment. Cloud computing does not change the responsibility, but cloud computing's global reach and shared infrastructure do pose new challenges. A balanced approach is required to:

- adopt cloud computing as an alternative service delivery model for IT services
- manage risks to data sovereignty

The GC Enterprise Architecture Review Board (EARB):

- sets the direction for enterprise IT across government
- will play a key role in managing the risks related to the adoption of cloud computing

The EARB's membership consists of organizations across the GC, including:

- business owners, such as the Canada Revenue Agency (CRA) and Employment and Social Development Canada (ESDC)
- service providers, such as Shared Services Canada (SSC) and Public Services and Procurement Canada (PSPC)
- lead security agencies, such as Communications Security Establishment Canada (CSEC) and the Treasury Board of Canada Secretariat (TBS)

The Board will begin reviewing all cloud requests from both an architecture perspective and a risk perspective in order to ensure that the risks identified in this paper are mitigated to the greatest extent possible.

In order to fully realize the benefits offered by cloud computing, while limiting the GC's exposure to risk, the following steps are being undertaken.

## Develop data encryption guidelines for cloud

This guidance will include how the GC will maintain control of the encryption keys for data hosted in a cloud environment in order to mitigate unauthorized access concerns (winter 2017 to 2018).

## Establish standard contract clauses for cloud

These clauses will compel the CSP to disclose all unauthorized access to data (including those made under court order) to the GC, unless the CSP is prohibited from doing so by law (fiscal year 2018 to 2019).

## Initiate protected-cloud procurement

SSC and PSPC will be in a position to use the Direction for Electronic Data Residency, the Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN), and the Security Control Profile for Cloud-based GC IT Services to launch protected-cloud procurement in 2018.

Departments and agencies will also use the Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) to secure the services they deploy to the cloud.

# Appendix A: government responses to data sovereignty

In examining the issue of data sovereignty, it is relevant to look at what mitigations other governments have implemented. The following table provides a general overview.

| Mitigation | Pros | Cons | Who is doing it? |
|---|---|---|---|
| **Require data residency**<br>Require that certain data be stored within a country's geographical boundaries | Data residency helps maintain:<br>• access to GC data<br>• public trust | • Data residency does not mitigate against the application of foreign laws | British Columbia: data must be stored in Canada<br>France and Germany also have data residency requirements |
| **Use data encryption**<br>Make Canada's data opaque to the cloud service provider (CSP) | • Canada's data is opaque to the CSP | Encryption:<br>• can result in reduced functionality<br>• makes the GC responsible for managing encryption keys | The UK has published guidance regarding encryption |

1 ISO stands for "International Organization for Standardization."

2 ITSG stands for "Information Technology Security Guidance."

3 SOC stands for "System and Organization Controls."

| Mitigation | Pros | Cons | Who is doing it? |
|---|---|---|---|
| **Use data masking**<br>Protect sensitive data by storing it on the premises of a GC facility; the data stored in the cloud would be structurally similar but not authentic | • Canada's sensitive data is anonymous | Masking:<br>• can result in reduced functionality<br>• makes the GC responsible for managing masking infrastructure | Unknown |
| **Ensure that CSPs meet security certifications**<br>Ensure that the CSP meets internationally recognized certifications such as ISO 27001 [1] | • CSPs are compliant with GC security and privacy controls | • Security certifications do not mitigate against foreign laws | Canada: ITSG-33 [2] controls have been mapped to ISO 27001 and SOC 2 [3]<br>UK: ISO 27001 is appropriate for data classified as official |

1 ISO stands for "International Organization for Standardization."

2 ITSG stands for "Information Technology Security Guidance."

3 SOC stands for "System and Organization Controls."

| Mitigation | Pros | Cons | Who is doing it? |
|---|---|---|---|
| **Use standard clauses in contracts with CSPs**<br>Include clauses that require the CSP to maintain confidentiality | • Canada has mechanisms to enforce compliance with Canadian laws and retain data ownership | • It is unclear as to how a CSP would resolve a conflict between its contractual obligations and foreign laws | Canada: the CSP must be compliant with the Privacy Act<br>The EU has started issuing model contract clauses for the protection of personal data |
| **Entrust a Canadian company with the data**<br>Ensure that the CSP uses a Canadian-based company to control access to the cloud | • CSP access is controlled by a Canadian company | • Only one CSP in one country has adopted this model<br>• GC is not aware of this mitigation having been tested in court | Germany: Microsoft has created a sovereign cloud and a German telco controls access to it |

1 ISO stands for “International Organization for Standardization.”

2 ITSG stands for “Information Technology Security Guidance.”

3 SOC stands for “System and Organization Controls.”

| Mitigation | Pros | Cons | Who is doing it? |
|---|---|---|---|
| **Rationalize data categories**<br>Align data categories to commercial security capabilities | • Data categories are modernized for today's cyber environment<br>• Canada can determine where commercial controls are sufficient | • Rationalizing data categories does not mitigate against foreign laws | The UK has rationalized 6 categories into 3 categories<br>The UK has also decided that data classified as official can be secured with commercial controls |
| **Limit the categories of data stored in the cloud**<br>Consider data of non-national interest as appropriate for the public cloud | • Canada understands what level of data is appropriate for the public cloud | • Not applicable | Canada: the cloud can be used for data up to and including Protected B<br>UK: the cloud can be used for data classified as official |

1 ISO stands for "International Organization for Standardization."

2 ITSG stands for "Information Technology Security Guidance."

3 SOC stands for "System and Organization Controls."

# Footnotes

1 The key departments are Shared Services Canada, Public Services and Procurement Canada, and the Communications Security Establishment Canada.

2 In relation to Canada, “data sovereignty” is Canada’s right to control access to and disclosure of its digital information subject only to Canadian laws.

3 “Data residency” is the physical or geographical location of an organization’s digital information.

4 ITSG stands for “Information Technology Security Guidance.”

---


ISBN: 978-0-660-27233-7

**Date modified:**

2018-07-13