Governments Embracing Cloud

An Opportunity for Modernization, Innovation and Transformation

ITAC
INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ACTI
ASSOCIATION CANADIENNE DE LA TECHNOLOGIE DE L'INFORMATION

Table of Contents

Executive Summary **3**

Introduction **4**

Understanding Cloud Computing **6**

- Why cloud computing is different 5
- Getting out of the data centre business 6
- One cloud does not fit all: public, private, and hybrid clouds 6
- The cloud market 7
- Key drivers of cloud computing 8
- Budgeting for cloud: shifting from CapEx to OpEx 10

Benefits of Cloud Computing **12**

- Eliminate technological debt 12
- Environmental impacts 13
- Support remote workers with cloud-based systems 13
- Improved agility and speed 13
- Cost savings 14

Dispelling the Myths **15**

- Data and borders: the CLOUD act explained 15
- Data sovereignty and control 15
- How secure is the cloud? 16

Developing Smart Cloud Policy: Considerations **18**

- Public cloud first 18
- Rethinking data classification 19
- Leverage existing data privacy and controls 19
- Security governance models 20

Recommendations **21**

1. Maintain alignment 21
2. Prioritize cloud education and training 21
3. Get out of the data centre business 21
4. Follow a Cloud First policy—but public cloud first of all 21
5. Explore cloud flexibility 22
6. Support cloud-native software development 22
7. Leverage existing security controls and accreditations 22
8. Enable transformation 22
9. Modernize data classification for cloud 22
10. Develop a step-by-step strategy to migrate seamlessly to the cloud—and operate successfully there 23
11. How ITAC can help 23

Executive Summary

While the vast majority of Canadians are connected, technologically adept, and comfortable accessing digital services, their government has not been keeping up.

In fact, governments' tremendously slow adoption comes at a considerable cost, in terms of wasted resources, technological debt, and missed opportunities to access better, greener, and more secure IT services.

In light of this, the Cloud Working Group of the Information Technology Association of Canada (ITAC) urges governments to begin the digital transformation that will move operations into a cloud environment.

Embracing cloud computing—in which software, platforms, and infrastructure are services accessed via the Internet—will allow governments to move away from its reliance on outdated, expensive data centres and traditional IT. Instead, it offers a huge opportunity for innovation and technological competitiveness, more robust security, and significant savings.

Best practices for moving toward a cloud environment have been established, and can be leveraged by Canadian governments. Holders of the most sensitive data in the world, including the CIA, NASA, financial institutions, and many international governments (including the US, UK, and Australia), have already adopted Cloud First policies and are reaping the benefits.

The paper makes the following nine recommendations to help governments make this important step forward:

1. **Maintain alignment** with transformation initiatives currently underway.
2. **Prioritize in-house cloud education and training.**
3. **Get out of the data centre business** and shift from a CapEx to OpEx model of IT services.
4. **Follow a Cloud First policy—but public cloud first of all**. Rethink and remodel data classification schemes and move up to 80% of government data to the cloud.
5. **Explore cloud flexibility** to make the best use of private and public cloud.
6. **Support cloud-native software development**. Ensure all future software development is designed *specifically* to take advantage of the cloud delivery model.
7. **Leverage existing security controls and accreditations**. Look to existing frameworks for best practices, guidance, and direction.
8. **Enable transformation**. Build an implementation strategy that optimizes the delivery of services through the most efficient and valuable delivery model; engage in innovative partnering arrangements between government, industry, and citizens.
9. **Modernize data classification for cloud**. Governments in Canada must undertake an assessment to match data security classifications, categories and requirements to commercial cloud security capabilities.
10. **Develop a step-by-step strategy to migrate seamlessly to the cloud—and operate successfully there**. Provide a cloud migration roadmap or policy plan to ensure agency and departmental cloud plans are aligned to key migration operational activities.

ITAC urges governments to begin the digital transformation that will move operations into a cloud environment.

Introduction

Ninety per cent of Canadian adults use the Internet or own a smartphone, making them the third most connected populous in the world, after only South Korea and Australia. But while citizens crave digital services, and are overwhelmingly adept at using them, the Canadian public sector has, to date, not risen to meet these demands.

The hesitation to move forward with progressive technological transformation is coming at considerable cost to Canadian governments, in terms of wasted resources, technological debt, and missed opportunities to access better, greener, and more secure information technology/information management (IT/IM) services.

Cloud computing, with its established capacity for innovation, security, standardization, and cost savings, should be fully embraced at the federal level as the cornerstone of a digital transformation strategy. This is not a new idea. Governments around the world, including in the United States, United Kingdom, New Zealand, and Australia have already successfully adopted and adhere to Cloud First policies, moving away from traditional IT/IM services. Their experiences offer valuable lessons learned about adoption, security, accreditation, and acquisition models that have delivered improved policy outcomes, enhanced efficiencies, higher levels of service quality, greater agility, and improved levels of trust with citizens and business. There is now an understanding that in order to drive cloud adoption, directives centred on enforceability and accountability are required to spur the move to cloud technology (for example, including language that makes budgetary funds conditional on cloud usage, and that oulines reporting requirements on cloud adoption).

The hesitation to move forward with progressive technological transformation is coming at considerable cost to Canadian governments...

The Information Technology Association of Canada (ITAC) strongly supports the adoption of a Cloud First approach to IT modernization. ITAC has established a Cloud Working Group (CWG) of private-sector industry leaders and providers of cloud-based services.

The CWG developed this white paper to encourage governments to develop and act on a cloud strategy.

This white paper provides:

- A general understanding of cloud computing, including its key drivers, market position, and what it could mean to the federal budget process;
- Key benefits of cloud computing;
- A critical examination of lingering myths about the cloud and data security, sovereignty, visibility, and transmission;
- Policy lessons learned from other governmental cloud initiatives; and
- Recommendations for a future operating model and key steps required to successfully transition to cloud services.

Understanding Cloud Computing

> "Cloud computing is 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."
>
> — *National Institute of Standards and Technology (NIST)*

Along with this definition, NIST lists five characteristics deemed essential for any service to be considered cloud:

- **On-demand self-service:** the end user can sign up and receive services without long delays;
- **Broad network access:** the end user can access the service via standard platforms including desktop, laptop, and mobile;
- **Resource pooling:** resources such as storage, processing, memory, and network bandwidth are pooled across multiple customers;
- **Rapid elasticity:** the system has the capacity to scale commensurate with demand; and
- **Measured service:** resource usage is monitored, controlled, and metered on a pay-per-use basis.

Cloud computing offers software, platforms, and infrastructure as services accessed via the Internet. It steeply reduces or eliminates the need for on-premises servers and equipment, and turns traditional models of IT provisioning, purchasing, and operation on their head—to great benefit.

Why cloud computing is different

It is crucial to understand exactly how cloud computing differs from traditional in-house IT before examining cloud policy considerations and best practices.

Traditionally, organizations purchased, operated, and maintained their own IT systems, including data storage. That meant acquiring physical servers, network equipment, racks, and cabling; installing everything in a secure, air-conditioned, climate controlled room; and then configuring, managing, monitoring, and maintaining it all. Upgrading services or scaling up data storage meant purchasing and installing additional hardware. All of the costs to power, maintain, and replace the infrastructure—and the IT team to oversee it—were borne directly by the organization.

Private industry and governments alike managed their IT needs this way for many years, developing the skills and knowledge necessary to operate large-scale technology infrastructure and data centres to support their needs.

This is the model followed, almost exclusively, by the Government of Canada in 2019.

Getting out of the data centre business

Cloud computing offers access to the same (or better) services, without buying and maintaining physical assets. Instead, organizations tap into powerful computing, data storage, networking, and other IT resources which are maintained and managed off-premises, and they pay only for the resources used.

Cloud computing is a utility-style model, loosely comparable to household electrical services: consumers of electricity do not build and maintain their own generators or power stations. Instead, the electric company—which is in the sole business of creating and distributing power—provides electricity at a massive scale. Customers use as much or as little as they need and pay only for the amount consumed in a given billing cycle.

Cloud computing is a utility-style model, loosely comparable to household electrical services...

Similarly, cloud service providers offer their services at massive scale, and customers tap into the resources they need, when they need them, and only pay for what they use.

The major cloud service providers are leaders in innovation and enterprise-level IT. They have built global businesses on offering the most sophisticated data storage and security, and their teams of developers are the world's best, tasked with continually upgrading and updating their services. The public sector cannot match these technological resources or expertise, nor should it try to.

Governments should not approach cloud policy and procurement as if they are purchasing physical assets. Quite the opposite: moving to the cloud means getting out of the data centre business. Cloud policy must consider how standardized utility-style services are budgeted for, procured, secured, and used, and it must present a strategy that is intentionally different from traditional IT—and intentionally designed to harness the benefits of the cloud delivery model.

Traditional IT, with all assets and data maintained in-house, does allow a high degree of customization and control, with significant up-front investment and ongoing maintenance and upkeep costs. Cloud computing services are owned and managed by off-site providers who offer standardized options with advanced scalability, elasticity, and resilience, and replace the lump-sum payment with ongoing subscription fees.

Understanding these fundamental differences help set expectations and delineate responsibilities for both cloud service providers and their government customers.

One cloud does not fit all: public, private, and hybrid clouds

Cloud computing can be deployed in three different ways:

Public cloud: All servers and storage are owned and operated by a third-party cloud service provider and delivered over the Internet. All computing resources—hardware, storage, networks, etc.—are shared with other organizations. Access is provided on an authorized basis.

Private cloud: An extension of the traditional data centre, in that computing resources are used by only one organization or business. All hardware is dedicated to a single organization and services and networks are maintained on a private network. The private cloud (i.e., servers) may be physically located on the organization's premises or hosted by a third-party cloud service provider.

Hybrid cloud: Offers the benefits of both private and public cloud. The lower-cost, more flexible public cloud can be used for high-volume and lower-security items; the private cloud can be reserved for highly sensitive data.

The CWG recommends a hybrid model, with a **public cloud first** mandate and goal of 80% of data to be housed on public cloud.

The cloud market

> "Enterprises that do not fully embrace the public cloud will be marginalized in this renaissance of digital innovation"
>
> *— IDC Chief Analyst Frank Gens*

The IDC predicts worldwide public IT cloud services will exceed **$276.8 billion** in 2021—more than double the $129.7 billion revenue reached in 2017.

The International Data Corporation (IDC), a global provider of market intelligence and advisory services for the IT sector, views the cloud as the essential foundation of digital transformation and the launchpad for digital innovation. Cloud adoption has been steadily growing and will surge in the coming years—by 2021, IDC predicts, the cloud will be virtually everywhere, and adopted into almost every use case.

In this era of digital transformation and growth, enterprises of all sizes are shifting traditional IT to the cloud, taking advantage of new innovations. Not surprisingly, the public cloud market is growing in value, in step with its dramatic upshift in importance. The IDC predicts worldwide public IT cloud services will exceed $276.8 billion in 2021—more than double the $129.7 billion revenue reached in 2017.

The public cloud is also evolving. IDC calls it "Cloud 2.0," and it includes new cloud environment and configuration options:

Distributed cloud: interconnected cloud services, shared among different systems and different geographic locations. In practice, a distributed model means the cloud moves "out on the edge," or closer to the enterprises using it.

Specialized cloud: some enterprises have hesitated to move to cloud computing due to the perception (real or imagined) that the cloud cannot perform at the optimized level required for specific workloads. The specialized (non-general-purpose) cloud removes that issue.

Multicloud: this is the cloud model of the future, as over 90% of enterprises are predicted to adopt intensively multicloud environments by 2021. This could represent any of a number of on-premises, off-premises, public, and private cloud hybrids.

The ongoing explosion in innovation and the growing number of enterprises from virtually every industry moving to the cloud—each with its own set of expectations, requirements, and parameters—has led to fierce competition among the major cloud services players. This has driven down prices, raised the quality of services and support, and increased the options available to customers. As an added benefit, leveraging a multi-vendor cloud environment also addresses issues pertaining to vendor lock-in.

In 2019, cloud computing is undergoing huge growth and an exciting pace of innovation, but it is also an established, well-tested way of organizing secure and advanced IT services for businesses, organizations, and governments.

Competition among the major cloud services players has driven down prices, raised the quality of services and support, and increased the options available to customers.

IDC has released 2017-2021 cloud market predictions for the three cloud services product categories: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS):

- **SaaS** will continue to dominate public IT cloud services revenue. In 2017 it accounted for 67.4% of cloud services revenue and is predicted to grow at 17% (five-year compound annual growth) through 2021.
- **PaaS** will be the second-fastest growing (30.9% five-year compound annual growth rate) category of the three cloud services product categories, driven by the continuing surge in cloud-based database, application development software, and data analytics/AI.
- **IaaS** will remain the second-largest IT cloud services category (32.2% five-year compound annual growth rate), boosted in part by cloud storage and, more broadly, by the growth of PaaS and SaaS services that will continue to require underlying IaaS capacity.

Key drivers of cloud computing

"If a company fails to get digital right, it's out of business; if a government fails to get it right, it becomes out of touch. Our relevance to citizens is in jeopardy if we can't deliver world-class digital services and cloud is a critical piece of providing good digital services."

—Treasury Board of Canada President Hon. Scott Brison (July 2017)

Demand for public cloud-based services is increasing sharply in all sectors, and will continue to do so, driven by several critical factors. Opportunities exist for the government of Canada to take advantage of this momentum, and to take a leadership role.

Digital transformation

Digital transformation is a necessity for any enterprise that doesn't want to be left behind. The incorporation of digital technology at all levels of operations is revolutionizing the way organizations deliver value and it is the strongest driver for cloud adoption. IDC predicts that global spending on technologies and services that enable digital transformation will reach $1.97 trillion in 2022.

Virtually all digital transformation initiatives depend on cloud services for access to key technologies and supply and distribution networks.

ITAC and Bayview Yards, an Ottawa-based business accelerator, have proposed the establishment of a Govtech innovation centre in Ottawa to capitalize on this global market opportunity. Their vision is to create a centre of excellence for digital government and transformation to connect entrepreneurs, business, government, and academia, and to encourage the development of novel digital solutions for the Government of Canada. These innovative solutions would not only help modernize government and improve services and productivity, but also be available for sale internationally.

Migration from traditional on-site data centres to cloud-based storage has never been more streamlined.

Tech innovation is happening in the cloud

The leading public cloud service suppliers have introduced a steady stream of innovative new IT services over the past couple of years, with a focus on automation, encryption, blockchain services, artificial intelligence and machine learning, the Internet of Things, and many others. This pace of improvement and innovation will continue and accelerate.

Organizations seeking the most advanced IT services will find them on public cloud platforms. **Comparable options do not exist for traditional IT setups**—they're just not being developed any more. As IDC warns: "Organizations that don't aggressively leverage these public cloud developer services will quickly find themselves isolated from most IT innovation in the marketplace."

If government does not adopt a cloud environment, it will be increasingly difficult to access or leverage the latest software innovations—and that includes the latest in security services.

Support for enterprise-size workloads and complex deployment

Not only is the variety of services offered by cloud providers increasing, but the support systems accompanying them are too. Migration from traditional on-site data centres to cloud-based storage has never been more streamlined. Professional, managed services are increasingly available in both the public and hybrid arenas, facilitating complex, multiple cloud environments.

Workloads once considered too heavy to be moved to the cloud can now migrate with ease. Complex deployment scenarios are now simpler and more coherent. As the perceived barriers to migration to the cloud continue to crumble, the movement away from private data centres to shared cloud environments will accelerate.

Budgeting for cloud: shifting from CapEx to OpEx

IT spending, like most public or private sector spending, falls into two general categories: capital expenditures (CapEx) and operational expenditures (OpEx).

CapEx refers to money directed toward property, equipment, or other fixed assets (in the IT world, these could be servers, power systems, air conditioners, and backup generators). CapEx usually require a large one-time upfront investment. Planning and budgeting for CapEx requires future forecasting: when it comes to IT infrastructure, in particular, changing needs and technological advances must be taken into account—capital assets are designed to last multiple years while gradually depreciating, not become quickly obsolete.

Technology as CapEx	Technology as OpEx
Large up-front investment	Regular subscription-type payments
Guesswork to estimate future capacity needs	Pay only for capacity used
Static hardware/software with an ongoing refresh cycle requiring access to labour resources	Agility and regular (often automatic) updates, access to innovations and on-demand access to elastic resources
Potentially lengthy process to estimate budget and seek approval for big-ticket items	Accelerated budgeting process due to lower short-term spending requirements
Updates, when possible, require additional investment	Immediate access to latest updates and technology
In-house IT team responsible for operations management (including backups, upgrades, repairs)	Higher levels of IT automation and enforcement of security compliance

OpEx offers a new way to manage an IT budget. OpEx, the day-to-day costs of running a business, can be more stable than CapEx. Adopting an OpEx model for IT services replaces a large lump-sum payment with recurring fees, smoothing out cash flow. This model brings other benefits too, including immediate access to new technology, and the elasticity to adapt to changing needs without additional cash outlay.

Perhaps most relevant in the government context, using an OpEx model for IT services means **additional free cash flow** for capital investments in other projects that drive the delivery of public services to federal employees, citizens, and businesses.

OpEx is the perfect fit for the changing technological landscape. The private sector has overwhelmingly embraced cloud-based IT, and it is reaping the benefits. Many businesses now dedicate fewer resources to obtaining, maintaining, and updating hardware and software than they did just a few years ago. Users no longer pay for underutilized components, and they aren't left scrambling to purchase and physically add additional servers if usage unexpectedly spikes.

Many government agencies worldwide have also moved toward cloud computing: instead of purchasing technology based on long-term projections decided years ago, the government departments only pay for required IT services.

OpEx offers space for innovation, and a path for growth. Cloud computing can save taxpayer money through economies of scale, but also it scales cost-effectively as government needs grow. Additional cloud storage can be added at a fixed monthly cost, with the assurance that new applications and employees are connected, without adding operational human resources.

Selecting CapEx or OpEx is not an either/or scenario. Governments and other organizations can choose to adopt an OpEx approach in certain areas while choosing CapEx for others. In all cases, though, the trade-offs must be understood. CIOs/CTOs/IT leaders must collaborate with finance leaders within their public sector organization to develop the cloud enterprise OPEX subscription model to transition from CAPEX.

Benefits of Cloud Computing

Transitioning to cloud computing offers many benefits, several of which are examined thoroughly below and throughout this paper. In brief, adopting cloud computing can:

- Eliminate technological debt
- Reduce environmental impacts
- Reduce infrastructure deployment costs
- Decrease maintenance costs
- Create standardization
- Increase utilization
- Lower overall service lifecycle costs
- Reduce government's carbon footprint
- Boost productivity
- Smooth out budgets
- Spark innovation
- Improve agility and speed

Eliminate technological debt

Organizations fall into technological debt when they don't keep pace with technology. The concept can be roughly compared to financial debt: if an organization doesn't repay its tech debt, it will fall further and further behind, making it more difficult to implement changes (get out of debt) later on. **Being in tech debt means IT departments spend most of their time putting out fires—not finding new and more efficient ways to deliver services.**

Moving to cloud computing requires a shift in mindset and careful planning, but it is the most direct route out of tech debt.

Tech debt often stems from retaining ageing technology rather than keeping up with upgrades or new methodologies. According to IDC, **Canadian datacentre administrators spent 74% of their time "keeping the lights on"** in 2018, up from 70% just three years earlier. Old equipment and the old way of doing things is so far behind the cutting edge that operations suffer. Resources are wasted, productivity plummets, and opportunities are missed. Clawing out of that debt takes resources, planning, and a will to embrace change.

This is the situation the Government of Canada is in while it clings to traditional IT methods, including in-house data centres, and delays adopting a hybrid or full cloud-based system.

Moving to cloud computing requires a shift in mindset and careful planning, but it is the most direct route out of tech debt.

Environmental impacts

Data centres are a monster in the federal government's energy closet. Large data centres can use enough energy in a day to power 65,000 homes—and only 6 to 12% of that energy is actually used in computing. The majority of it is used to run backup servers and maintain cool climactic conditions within the data centre. As of 2019, hundreds of data centres are spread across the federal government's portfolio, many operating 24/7 at full capacity, regardless of demand.

As of the release of this paper, most major cloud brands have committed to achieving 100% green energy for their data centres.

As of the release of this paper, most major cloud brands have committed to achieving 100% green energy for their data centres. In the same way that cloud technology helps reduce financial costs through economies of scale, it also helps tackle energy inefficiencies by facilitating increased server allocation rates. Instead of every organization hosting its own in-house servers, the cloud approach welcomes multi-tenancy solutions and resource sharing, boosting energy efficiency.

Researchers at Lawrence Berkeley National Laboratory and Northwestern University have developed a Cloud Energy and Emissions Research Model, which estimates the energy savings of shared cloud storage models. They produced a case study that suggested that if all American businesses moved all their network applications and software to off-site cloud servers, the country's overall computing energy footprint would shrink by 87%—enough to power Los Angeles for an entire year.

Moving to cloud computing will allow the government to reduce hardware requirements, power consumption, and resource redundancy while supporting green initiatives.

Support remote workers with cloud-based systems

Remote working means less vehicles on the road, smaller offices, less consumption, and, in most cases, increased productivity. The cloud environment, with its mandate of shared tools and resources, supports working from home. Communication and collaboration are two of the great cloud advantages, and tools to facilitate this way of working are getting better, cheaper, and easier to use virtually by the day.

Improved agility and speed

In a cloud computing environment, new IT resources can be accessed with just a few clicks, sharply reducing the time it takes to make those resources available to those who need them. This is a dramatic increase in agility for government customers, in three key ways:

Scaling to meet capacity needs: In traditional IT models, capacity predictions have to be made before deployment, often resulting in idle resources or limited capacity. Cloud computing allows customers to scale up or down with just a few minutes' notice, based on actual demands. This is particularly valuable in departments that see a spike in demand during certain times of the year.

Availability and resilience: The geographic distribution of public cloud infrastructure protects against natural or man-made disasters, power failures, or

spikes in service demands that would negatively impact the service availability of on-premise systems. Data is transmitted, stored, encrypted, and replicated intelligently to protect the integrity of data and maximize efficiency and security for users. Most cloud service providers offer uptime service levels in excess of 99%.

Continual technology refresh: Unlike physical assets, the cloud model facilitates the dynamic evolution of infrastructure and services. Many updates can be automated. Staying at the leading edge of technology change ensures government investments in IT do not go toward paying off tech debt but directly benefit the mission.

Cost savings

Government cannot keep pace with private-sector innovation simply by updating or refreshing on-site infrastructure every few years. Moving toward cloud computing and minimizing this capability gap offers clear savings to government simply by not investing in outdated technology.

Other cost savings come from:

- Paying only for the resources being consumed.
- Taking advantage of economies of scale: being in a shared environment means sharing data centre costs, improving operational efficiency, and reducing overall power consumption.
- Improving transparency: the cloud environment allows for precise tracking of usage, making it easy to target efforts to optimize resources.
- Technological competitiveness: accessing the latest technology offers more capability for less investment, allowing governments to do more for less.

Dispelling the Myths

Data and borders: the CLOUD Act explained

In 2018, the US government passed the Clarifying Overseas Use of Data (CLOUD) Act. The Act changed how US law enforcement accesses data that is stored overseas. Prior to the CLOUD Act, US officials could only access data held in a foreign country through a mutual legal-assistance treaty, which generally required several months or longer to achieve, often rendering the data obsolete in the meantime.

The CLOUD Act, however, means tech companies must comply with any qualified request from a US law enforcement official for data in its control, no matter where the data is stored. This is particularly important in today's digital landscape, in which data can move instantly and seamlessly across borders and reside in servers in places other than its country of origin.

While the CLOUD Act is generally considered a win for safety and law enforcement, it also helps preserve data security and privacy, and the ability of cloud service providers to legally protect that privacy. The CLOUD Act does not give US officials unrestricted access to data; any data request must be accompanied by a warrant in accordance with US criminal procedures.

"The cloud has made the role of tech companies on privacy issues a practical necessity," says Microsoft President Brad Smith. "The CLOUD Act preserves and expands this role with legal certainty. It creates a responsibility for tech companies both to help protect public safety and preserve personal privacy."

It is a myth that all data must be stored within Canada's borders for the federal government to maintain digital sovereignty.

When moving into the cloud it is important to understand that the location of data does not guarantee security or limit access by foreign governments. It is crucial to work with an established provider that will ensure that specific security requirements and encryption standards are met; the exact location of data or cloud services, however, is not as important.

Data sovereignty and control

It is a myth that all data must be stored within Canada's borders for the federal government to maintain digital sovereignty. Ultimately, data residency is a jurisdictional issue—not a security one. Encrypting data or leveraging blockchain/cybersecurity measures to limit unauthorized access to data are better alternatives to requiring residency.

Governments naturally want to assure citizens that their personal data is safe. This has led some governments to develop public policy that mandates data reside within a country's borders, believing that doing so provides an additional layer of security and protection. It does not.

Requiring that Canadian data be stored on Canadian soil is a simplistic political approach to appeasing the need for security. In fact, the physical location of data has little to no impact on threats propagated over the Internet: Internet-connected systems expose an organization to a broad threat space, which can be propagated from any location in the world. Whether data is housed in Canada, Iceland, or

Romania makes little difference to hackers. The difference comes in the security measures put in place.

Localizing data leads to a weaker data security posture. Public cloud services operate globally, using geographically distributed infrastructure to encrypt, transmit, and store data intelligently between data centres and across borders in order to protect the integrity of the data and maximize efficiency and security for users. Requirements to localize data not only give hackers more defined targets to attack, but also limit competition of cloud services and the availability of best-in-class cybersecurity solutions.

Attempting to keep data within political borders is not a useful endeavour.

The Internet is routed via exchanges throughout the world, seeking the shortest possible track between two points. Most Domain Name System (DNS) routers, resolvers, and hosts are housed in the US—and Canada's Internet infrastructure is intimately linked to US networks. Many networks favour north-south connections, pushing Canadian data flow toward key US routing hubs. Canadians may be surprised to learn that when accessing Canadian sites, their data often flows through the US.

This is the reality of our globally connected world. Attempting to keep data within political borders is not a useful endeavour.

How secure is the cloud?

Tech companies have had to assume a key role in protecting data security as information has moved to the cloud. As a result, secure cloud computing that meets government's high standards in assurance, governance, security, and compliance is available—and it can be measured, ranked, and verified. The leading cloud service providers do secure data for multiple customers. Their business success depends on offering the highest-level security and confidence.

Stringent international and national security and privacy standards for cloud providers have been developed, including ISO, FedRAMP (Federal Risk and Authorization Management Program), ATO (Authority to Operate), GDPR (EU Global Data Protection Regulations), the NIST Cybersecurity Framework, and many more. Top cloud service providers certify their products against these standards and work with governments to ensure all guidance is met.

The cloud provides an automated environment that enables governments to reliably execute established standards and regulations and implement enforceable security and compliance. Other security-related benefits include:

- Greater visibility of resources
- Streamlined, real-time auditing
- Automated security and governance controls
- The ability to create forcing functions that cannot be overridden without authorization
- Continuous hardware upgrade

- Established compliance; many certifications already in place
- Significant protection against DDoS attacks
- Access to the world's leading security expertise

Precedents have long been set: holders of the most sensitive data in the world, including the CIA, NASA, financial institutions, health service providers, and many international governments, have shown their trust and understanding of the benefits of the cloud by inking major deals with top cloud service providers.

Letting the experts—the cloud service providers—focus on meeting compliance and security requirements means that governments can spend more time and resources in other areas.

The Australian Government's Secure Cloud Strategy astutely confronts the myths around cloud security:

> "Cloud security fears are often overstated as specific to cloud where the risks to an environment apply equally, whether it is a provider cloud or an in-house implementation. Sound risk management practices to prevent and detect cyber security attacks can be as successfully implemented in cloud as they can in traditional data centres. The automation cloud minimises human error. Cloud providers often implement and manage better IT security controls that internal IT teams as it is a core part of their business and reputation.
>
> "Cloud services are not inherently more or less secure than any other device with an Internet connection."

Developing smart cloud policy: Considerations

Smart cloud policy not only saves money but creates value by spurring innovation, boosting speed and agility, and increasing security, compliance, and standardization.

Moving to a cloud-centred approach does not mean simply migrating existing data and applications from an in-house data centre to a shared cloud and expecting to reap the benefits of an agile, scalable model. Applying a traditional IT vision to the cloud environment will not work.

Governments cannot consume the cloud as a service without significant groundwork—a complete digital transformation is required.

Fortunately, governments around the world have already modernized and migrated many of their operations to the cloud. Examining their successes and lessons learned provides a solid foundation from which to create a well-defined and well-implemented policies specific to Canadian governments. Below are some key considerations exemplified by successful cloud policies.

Public Cloud First

The first step is a government-wide commitment to public cloud as the default choice for government IT. A Cloud First policy sends a clear message that cloud is the new normal, with capabilities and efficiencies that traditional data centres cannot match. Cloud First sets out an order of preference when selecting a cloud deployment model but still recognizes that no one deployment model meets all of the government's needs.

As stated in the Government of Canada's Strategic Plan for Information Management and Information Technology 2017 to 2021, "Public cloud services will be the priority choice for departments when choosing a cloud deployment model," and "[d]epartments will use private clouds where needs cannot be met by public clouds (e.g., secret information)."

Implementing a successful Public Cloud First policy involves:

1. Examining the existing IT modernization strategy. This is the take-off point to understanding how the cloud can be used to work with the strategy.
2. Going beyond technical implementation considerations to including drivers that incentivize cloud adoption. Mandating that any use of non-cloud technology be justified.
3. Supplementing cloud-native policies with policy implementation directives that seek to stimulate and accelerate the use of cloud technology. Understanding any policies and legislation that could accelerate or inhibit cloud adoption, including security and data privacy policies and standards.
4. Designing a strategy for true hyper-scale cloud and taking advantage of the substantial benefits in agility, scalability, and reliance this brings.
5. Developing goal-setting and reporting requirements on progress, including the sharing of best practices between departments and agencies. Tying pay incentives for senior executives to the proportion of acceleration to the public cloud.

Cloud First policies have been developed and adopted by major governments around the world, including the US (2011), Australia (2014), United Kingdom (2014), Singapore (2016), and Philippines (2017).

Rethinking data classification

Canada currently has nine levels of data classification, resulting in systemic over-classification of data.

Many governments tend to believe that all the data they host is classified, thereby requiring storage in a private cloud environment. But building large-scale private clouds can be cumbersome, bearing many hidden security, lifecycle, and additional maintenance costs. Ultimately, a hybrid cloud model is likely the most cost-efficient model for government entities requiring the security of private clouds, but also the flexibility of public clouds.

But what data belongs in the public cloud?

In 2014, the UK government reduced its six levels of data classification to three: official, secret, and top secret. Cabinet Office Minister Frances Maude called the new system "fit for the digital age." He suggested the simpler classification scheme would make it easier to share information and save money, noting, "There has been a tendency to over-mark documents rather than manage risk properly." After the reduction, 90% of UK government data was marked "official," meaning it could be stored in the public cloud. The remaining 10% required private or hybrid set-ups.

A similar rethinking of data classification should take place in Canada. Federally, Canada currently has nine levels of data classification, resulting in systemic over-classification of data. Reducing this number and reassigning data accordingly will help the Government of Canada evaluate where and when public cloud services can be used, and where and when it is best to leverage a private cloud or hybrid cloud strategy

It will be critical to make this cloud approach known to internal decision makers and external suppliers, ensuring all parties are clear on which path they must follow.

Leverage existing data privacy and controls

Security and accreditation of cloud service providers reflects the massive growth of cloud adoption in major enterprises and global government—and provides guidance for evaluating the ability of vendors to manage different types of data.

Globally supported security standards such as ISO/IEC 27001 (Information Security Management) and NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) are excellent starting points for evaluating cloud vendors.

Instead of starting from scratch, governments may wish to leverage existing approaches to security standards. The US Federal Risk and Authorization Management Program (FedRAMP) is one government-wide program that provides a standardized approach to security assessment, authorization, and

continuous monitoring for cloud products and services. The Government of Canada may wish to develop a like approach to accreditation, thereby ensuring all cloud suppliers are openly aware of Canadian government requirements.

Part of the issue is that small and medium-sized (SME) cloud players can't afford to keep up with the varying certification requirements that the Government of Canada often asks for. Leveraging ISO standards would allow SMEs to comply with a single set of requirements for all clients, public or private.

Security governance models

Security and compliance can be made more efficient and expansive in the cloud. This cloud-centric approach to security helps government customers:

- Establish reliable and repeatable operation of controls
- Enable continuous and real-time auditing
- Script governance policies
- Create forcing functions that cannot be overridden by unauthorized users

The result is an automated environment that meets or exceeds assurance, governance, security, and compliance requirements. It enables governments to execute reliable implementation of what was previously written in policies, standards, and regulations, and create enforceable security and compliance, which in turn creates a functional reliable governance model for IT environments.

Recommendations

The Cloud Working Group urges governments to begin the digital transformation that will move operations into a cloud environment. Below are our recommendations to drive efficiencies and savings, protect the interests of citizens, and spur innovation as government becomes a cloud-enabled enterprise.

1. Maintain alignment

A number of transformation initiatives are currently underway within the federal government—all designed to innovate internal government and external client service delivery. It is imperative that governments develop and execute all transformation initiatives in a manner that will align with its cloud strategy.

2. Prioritize cloud education and training

Addressing cultural resistance to transformation, change management, and transformation and workforce development is crucial. Human resource managers should be inspired by the cloud and allow their team to be part of a growing and evolving IT ecosystem. Government should take a leadership position in training federal officers in new technologies, instead of paying hundreds of millions of dollars each year on consulting services or suffering from poor performance.

3. Get out of the data centre business

Government must stop thinking about digital services as physical assets that it must procure, own, and manage. By shifting from a CapEx to OpEx model of IT services, government leaves data centre management to the data centre experts, and frees up resources it can deploy elsewhere.

The government has made long-term investments of up to 25 years in colocation and in building data centres. As noted in the section on technological debt, further investment in on-premise data capacity is akin to investing further to support sunk costs. A business exit strategy should be developed to migrate out of data centre ownership, similar to governments' migration out of building management in the early 1980s.

4. Follow a Cloud First policy—but public cloud first of all

The primary benefits of the cloud for government come when a public cloud model is employed. Unless data classification requirements dictate the need for a private, controlled data centre, ITAC CWG encourages the Government of Canada to adopt a "Public Cloud First" strategy (i.e., before private cloud). This will be facilitated by a new data classification scheme and will operate under the assumption that the selected cloud service provider can meet the relevant security requirements using a public cloud.

Looking to the UK as a precedent, ITAC CWG suggests that a target of 80% of government data be moved to the public cloud. Any agency or department choosing a model other than the public cloud must provide its rationale for doing so, including a value-for-money business case.

5. Explore cloud flexibility

Given the complex nature of government operations, the number of legacy systems, and the extreme sensitivity of some data, some services will require delivery using private cloud. It will be important to determine how to balance public cloud with private cloud. Government should therefore select service providers who have the ability to establish interoperability across multiple clouds and leverage open-source systems. Government should also require that cloud service providers detail their capabilities for portability and workload migrations.

Cloud computing allows IT organizations within government to drive new business initiatives.

6. Support cloud-native software development

All future software development should be cloud-native, meaning new software must be designed specifically to take advantage of the cloud delivery model, and be agile, elastic, and marketable. This does not mean dumping traditional IT applications into the cloud. Cloud-native applications reside in the cloud, not in an on-premises data centre.

7. Leverage existing security controls and accreditations

Precedents have been set for establishing security standards, compliance, and guidance for government services in the cloud. Leveraging industry best practices regarding security, privacy, and auditing provides assurance that effective physical and logical security controls are in place, preventing overly burdensome processes or approval workflows that may not be justified by real risk and compliance needs. Use ISO, SOC, PCI, etc. as the starting point.

8. Enable transformation

Transforming the Government of Canada into a cloud-enabled enterprise requires a complete understanding of key challenges, a well-defined strategy, and a roadmap to execution. As outlined above, changes need to be made to business, operational, and IT delivery models and processes, governing IT and security policies and procurement processes.

Implementing a cloud environment is about innovation—and therefore, cloud computing allows IT organizations within government to drive new business initiatives. Rather than concentrating on operations, IT personnel should focus on building an implementation strategy that optimizes the delivery of services through the most efficient and valuable delivery model. This requires innovative partnering arrangements between government, industry, and citizens. The Govtech citizen accelerator proposal is just one way to support this.

9. Modernize data classification for cloud

Governments' data is often subject to stringent requirements governing data residency, security clearances, and departmental security controls. These requirements are often incompatible with the supply of public cloud solutions.

International experiences do not display a reckless approach to security or privacy protections. Rather, governments who have successfully adopted cloud have often

undertaken a careful assessment of their data classifications systems and matched data categories to commercial security capabilities. In short, this approach enables the implementation of digital government services, while also protecting citizens' security and privacy.

It is open for governments in Canada to make similar policy changes and doing so is often a necessary step to digitally transform service delivery, while also protecting the security and privacy of Canadians.

10. Develop a step-by-step strategy to migrate seamlessly to the cloud—and operate successfully there

There is no one-size-fits-all way to move to the cloud; however, a cloud migration roadmap or plan can be provided at a policy level (such as the New Zealand government has done) to help ensure agency or departmental cloud plans are aligned to key migration operational activities.

Cloud migration roadmap patterns that have become apparent in the last decade include:

- Look to **development and test** workloads as a learning path to cloud adoption.
- Use cloud for **entirely new applications**. Building new applications on the cloud provides all of the advantages of cloud right from the get-go, free of legacy concerns or hindrances, and no need for migration plans.
- As cloud skills and maturity develop, consider **moving websites** and digital properties, analytics, and mobile applications to the cloud.
- Move **business-critical applications** to the cloud and ensure that the cloud is leveraged for its enhanced disaster recovery capabilities.
- **Migrate entire data centres to the cloud** and go **"all-in."** Cloud adoption plans should consider whether data centres coming up for lease in 6, 12, or 18 months (or that require a significant technology refresh) will be needed. Can these workloads be moved to, or built on, the cloud instead? And can all future development and workloads be cloud-native?
- **Adopt open data policies:** Cloud computing enables government to leverage data analytics, artificial intelligence, and machine learning to streamline processes, gain valuable insights, and improve citizen services. Enabling greater access to open government datasets, supporting open data principles, and enabling data sharing initiatives will open up more possibilities for greater innovation and promote more competition from technology providers.

11. How ITAC can help

ITAC is happy to facilitate an industry 'Cloud Day' so that governments might better understand what the cloud avails the public sector.

ITAC ACTI

INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ASSOCIATION CANADIENNE DE LA TECHNOLOGIE DE L'INFORMATION

About the Information Technology Association of Canada (ITAC)

For more than 60 years, ITAC has served as the leading voice for Canada's information, communications and technology (ICT) industry, championing the development of a robust, competitive and sustainable digital economy in Canada.

As a prominent advocate for the expansion of Canada's innovation capacity, ITAC provides a vital connection between business, academia and government. ITAC also offers its members advocacy, networking and professional development services that help them to thrive nationally and compete globally.

Our role as a trusted and authoritative voice has expanded significantly over the years, as technology plays a more significant and important role in all sectors of our economy. That's why ITAC prides itself on its efforts around shaping public policy that supports the growth of talent and access to ICT professionals with diverse experience and backgrounds, better reflecting Canada's population.