Workshops and Benchmark to support GC's Cloud Strategy

Consultation Report

Prepared for: Treasury Board of Canada Secretariat (TBS)

July 31, 2015

GARTNER CONSULTING

Project Number: 330026489

Gartner

Agenda

- Executive Summary
- Context of the Cloud consultation
- Analysis
  - Policy
  - Business
  - Procurement
  - Security
- Summary of recommendations
  - Before Cloud
  - Cloud inception
  - Cloud evolution
- Appendices

Executive Summary

Gartner

The GC and jurisdictional partners launched a pan-Canadian Cloud consultation to solicit industry perspective to inform the Crown's Cloud strategy. Gartner supported the Crown with RFI analysis, vendor interviews and recommendations.

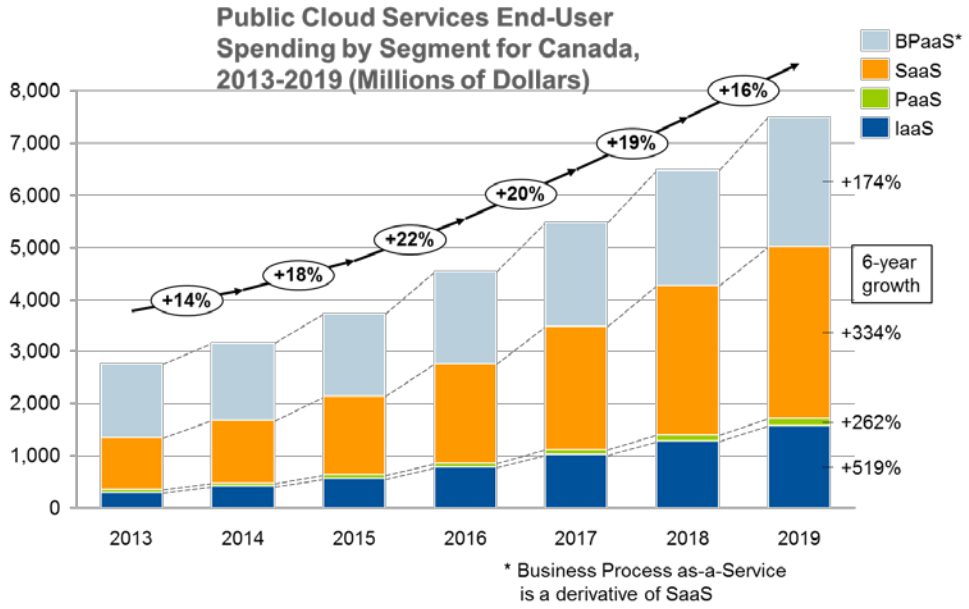
- The Government of Canada (GC), in partnership with Canadian provinces, territories and municipalities, led an industry consultation on Cloud computing.
- The consultation was launched on November 13, 2014 at an event attended by over 170 representatives from 82 companies.
- A request for information (RFI) was published on December 2, 2014 and focused on four key pillars: Business, Policy, Procurement and Security.
- Gartner supported TBS in the review and assimilation of information provided to the Crown with regards to go forward cloud approaches. In this effort, Gartner leveraged industry information, benchmark data and best practices to provide the Government of Canada with key information required to develop a Cloud strategy for all of government.
  - Gartner reviewed the 67 RFP responses received from a variety of organizations, including Canadian vendors, global vendors, systems integrators, non-profit organizations and Cloud industry organizations.
  - Gartner participated in 32 of the 64 one-hour One on One meetings, alongside Federal, Provincial and Municipal government representatives, to further understand the position of a significant sample of the RFI respondents.

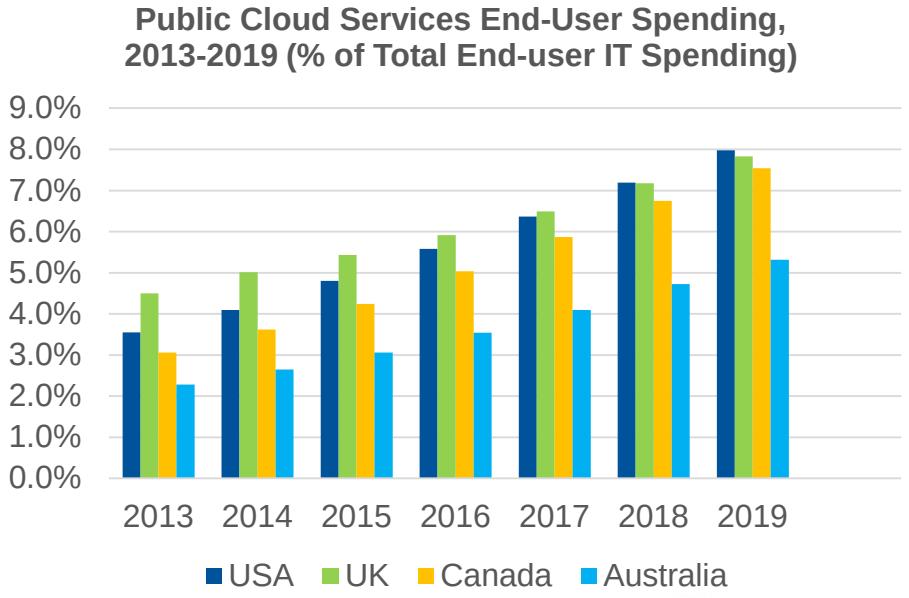
Significant Industry response (67 submissions) by international and Canadian Cloud Service Providers and related organizations reflects the strong interest in the rapidly growing Canadian Cloud economy.

High level profile of the 67 RFI respondents (categories are not mutually exclusive):

	Cloud Service Providers				
	IaaS	PaaS	SaaS	Cloud Broker	Other (technology, prof. svcs, …)
Canadian DC	11	7	7	1	13
DC Outside Canada	9	7	13	4	44
TOTAL	**20**	**14**	**20**	**5**	**57**

Data shows a rapidly growing Cloud economy in Canada that is catching up to the US and the UK.





Based on RFI questions across 4 pillars (Policy, Business, Procurement, and Security), Gartner combined input from respondents, best practices and experience from other jurisdictions to perform further analysis across 20 key topic areas.

A total of 20 topics were retained for further research and analysis:

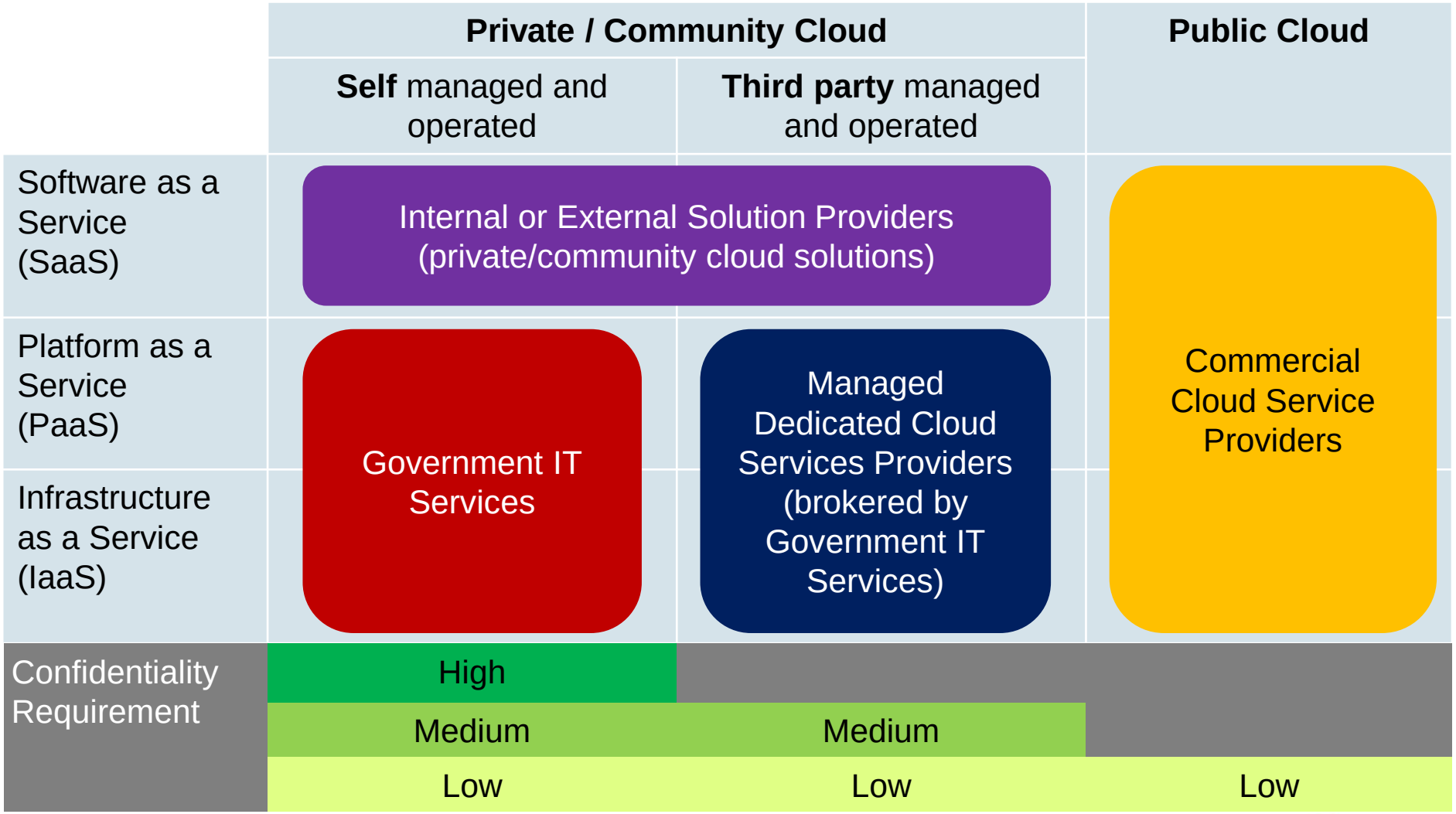
Policy	Business	Procurement	Security
Cloud council	GC Cloud	Cloud terms and conditions	Identity and Access
Canadian Cloud innovation	Cloud exit	Cloud program	Security and IM standards
Cloud workload	Service Level Agreements	Cloud taxonomy	Cloud security certification
	Accountability	Procurement vehicles	Security of public clouds
	Cloud brokers		Information confidentiality
	Launch strategy		Data residency
	Commitment		

The input from respondents was validated and combined with best practices, industry trends as well as experience in other jurisdictions to provide a complete view.

From this analysis emerged an action plan for Cloud within Government of Canada…

Before Cloud (3-6 months)	Cloud Inception (12-18 months)	Cloud Adoption (ongoing)
Establish Governance ▪ GC Cloud Council ▪ GC Cloud Center of Excellence **Define initial policies and guidelines** ▪ R&D tax credits and tax relief ▪ Cloud workloads decision tool ▪ Confidentiality-based information classification ▪ Data residency ▪ Data protection (encryption, risk-based guidance) ▪ GC Cloud definition ▪ Migration planning ▪ Cloud taxonomy **Plan Cloud inception phase** ▪ Initial Cloud workloads and Pathfinder projects	**Execute Cloud pilots** ▪ Potential cloud workloads **Gather insights** ▪ Cloud registry **Refine policies and guidelines** ▪ Cloud sprawl mitigation ▪ Cloud broker definition ▪ Define Cloud broker roles within GC ▪ Democratized procurement ▪ Cloud solutions security assessment **Establish procurement** ▪ SLAs definition and negotiation ▪ Cloud vendor prequalification ▪ Cloud Service Catalogue ▪ Collaborative procurement	**Expand cloud usage** ▪ Cloud Federated Identity ▪ Plan for the redistribution of IT and non-IT skills **Monitor and control for continuous improvement** ▪ Assessment approach

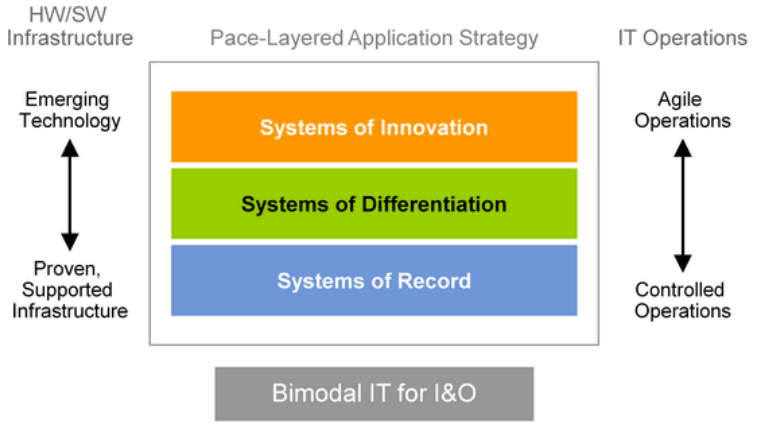
Including a proposal for an initial vision of Cloud workload segmentation with services requiring high and medium confidentiality delivered by Government IT, or Managed Dedicated Cloud Service Providers. Lower information confidentiality services are delivered on the Public Cloud.



Some workloads have been identified as potential candidates for Cloud pathfinder initiatives. The proposed Cloud Council will be a key source of innovative candidates based on real need.

- High potential Cloud workloads include the following, assuming a compatible security and risk profile:
  - PaaS/IaaS – Information Dissemination (e.g. web hosting (underway), Open Data, 311)
  - PaaS - Development and Test environments
  - SaaS – CRM/Case Management (for processes that are external and public-facing)
  - SaaS – Collaboration (with citizens, private sector organization or other governments)
  - SaaS/PaaS – Geo-spatial, Big Data, Business Intelligence and Analytics
  - IaaS – Project specific (unique requirements), through SSC

- In general, workload that belong in the systems of **innovation** category of the Gartner Pace-Layered Application Strategy are good candidates for Cloud delivery.



The recommendations are intended to advance the Crown's Cloud adoption maturity, in order to realize the potential benefits of Cloud.

	0 – Ad Hoc Cloud	1 – Elementary Cloud	2 – Specialized Cloud	3 – Streamlined Cloud	4 – Optimized Cloud
Organizational	Underground and Isolated	Sponsor and Define	Construct Organization	Train and Transform	Broker IT Services
Governance	Manual Definition and Assessment	Classify and Triage	Develop Decision Framework	Mitigate Risks	Broker Risk Management
Technology and Applications	First and Simple Solutions	Assess Portfolio and POC	Set Integration Foundations	Implement Strategically	Revamp Infrastructure and Services
Provider Selection and Management	Website and Sales Team Management	Create Master Criteria	Manage Providers Completely	Manage Providers Through Risk Decisions	Offer Self-Service Provider Management
Cloud Operations	Island of Management	Baseline Management	Integrate Manually	Operate With Agility	Operate Through Self-Service

Benefits


Increase Agility


Focus on core mission


Manage Cost


Leverage skills & knowledge


Reduce Complexity


Innovation

Context of the Cloud consultation

Gartner

List of RFI respondents

The following organizations submitted a response to the Cloud Consultation RFI:

2Keys Corporation	CloudLink Technologies Inc	Infor (Canada), Ltd	PricewaterhouseCoopers LLP
Adobe Systems Canada Inc	CloudMask Corp	Informatica Corporation	Red Hat Canada Limited
Akamai Technologies, Inc	CSC (Computer Sciences Canada Inc.)	Infosys Public Services, Inc	Rogers Communications Partnership
Alcatel-Lucent Canada Inc	Cybera Inc	Insight Canada Inc	RSA
Allot Communications	D and B (The D and B Companies of Canada ULC)	Intel Canada Ltd	Salesforce, Inc
Amazon Web Services, Inc	Day1 Solutions, Inc	iTMethods Inc	SAP Canada Inc
Apprenda Inc	Decisive Technologies Inc	KPMG LLP	Scalar Decisions Inc
Bell Canada	Deloitte Inc	KTI Data Center (Kihew Technologies LP)	ServiceNow (ServiceNow, Inc.)
Blue Coat Systems Canada Inc	Eclipsys Solutions Inc	Microsoft Canada Inc	Softchoice LP
BMC (BMC Software, Inc.)	EMC Corporation of Canada	NetApp Canada Ltd	Symantec Corporation
C2 Labs, Inc	Esri Canada Limited	Northern Micro	TELUS Communications Company
CA Technologies (CA Canada Company)	FTI Technology (FTI Consulting, Inc.)	OpenPlus.ca (Vurtur Communications Group Inc.)	TeraMach Technologies Inc
CenturyLink (CenturyLink, Inc.)	Fujitsu Consulting (Canada) Inc	OpenText Corporation	Thales Canada Inc
CGI Information Systems and Management Consultants Inc	General Dynamics Information Technology Canada, Limited	Oproma Inc	Trend Micro Canada Technologies Inc
Cisco Systems Canada Co	Hewlett-Packard	Oracle Canada ULC	Unisys Canada Inc
Cloud Perspectives	Hitachi Data Systems	Palo Alto Networks	VMware Canada (VMware Inc.)
Cloud Security Alliance Canada	IBM	PeopleInsight (QuIRC Qualitative Insights, Research and Consulting Inc.)	

One on One meetings

From April 28 to May 27, 2015, Gartner participated in 32 one-hour One on One meetings, alongside Federal, Provincial and Municipal government representatives, to further understand the position of the following RFI respondents, out of the 64 that participated in the industry consultation:

RESPONDENT NAME	MEETING DATE	MEETING TIME
Cloud Mask	2015-04-28	10:00 to 11:30
Centurylink	2015-04-29	12:00 to 1:30
IBM	2015-04-29	1:30 to 3:00
iT Methods	2015-04-29	8:30 to 10:00
ServiceNow	2015-04-29	3:00 to 4:30
KPMG	2015-04-30	1:30 to 3:00
Rogers Communication	2015-05-06	1:30 to 3:00
Salesforce	2015-05-06	12:00 to 1:30
TeraMach	2015-05-07	10:00 to 11:30
PeopleInsight	2015-05-07	12:00 to 1:30
NetApp	2015-05-07	1:30 to 3:00
Cloud Perspective	2015-05-07	3:30 to 5:00
VMware Inc.	2015-05-12	12:00 to 1:30
Cybera Inc.	2015-05-13	1:30 to 3:00
General Dynamics IT	2015-05-13	12:00 to 1:30
CA Technologies	2015-05-13	10:00 to 11:30

RESPONDENT NAME	MEETING DATE	MEETING TIME
PWC	2015-05-13	3:00 to 4:30
Oracle	2015-05-13	8:30 to 10:00
Infor	2015-05-14	12:00 to 1:30
SAP	2015-05-14	3:00 to 4:30
Intel Canada Ltd.	2015-05-14	8:30 to 10:00
RSA	2015-05-14	10:00 to 11:30
Microsoft Canada	2015-05-19	1:30 to 3:00
Telus	2015-05-19	3:00 to 4:30
CGI	2015-05-19	8:30 to 10:00
Eclipsis	2015-05-19	12:00 to 1:30
Symantec	2015-05-20	1:30 to 3:00
CSC	2015-05-20	3:00 to 4:30
CSA Canada Board	2015-05-21	3:00 to 4:30
HP	2015-05-26	1:30 to 3:00
OpenText	2015-05-26	12:00 to 1:30
Scalar	2015-05-27	10:00 to 11:30

This cross section included Canadian vendors, Global vendors, Systems integrators, non-profit organizations and Cloud Industry organizations. The value of respondent's contributions varied significantly and did not follow obvious patterns.

Analysis

Gartner

Gartner analysis

Gartner's analysis is summarized on the following pages, organized according to the four pillars of the Cloud consultation:

- **Policy**,
- **Business**,
- **Procurement** and
- **Security**.

The analysis is based on observations collected from the review of RFI responses and participation in one-on-one meetings with RFI respondents, as well as industry research and insight from other public sector cloud initiatives across the world.

Analysis – Policy – Cloud Council

Description
The Government of Canada will face many significant decisions as it establishes and executes its Cloud Strategy. Multiple stakeholders including public sector service providers, consumers and industry groups will have valuable input into the way forward and a formal mechanism for continuing to solicit input and test assumptions will be valuable.

Viewpoint(s)		
Establish a combined public and private sector Government of Canada Cloud Council.	**Establish separate public and private sector cloud councils.**	**Establish a public sector council and collaborate with industry and other third parties through existing Cloud Computing Industry Working Groups.**

Analysis

- On-going input and feedback from stakeholders is critical to enabling an effective cloud ecosystem.
- Internal cloud service providers such as SSC will have a direct impact on strategy and execution.
- Vendors and other industry stakeholders will bring important perspectives on what works and doesn't work based on experience from other jurisdictions.
- Government departments as service consumers will be an important voice to ensure that the strategy developed provides the appropriate combination of agility and security to drive adoption.
- A number of Cloud Computing Industry Working Groups made up of representatives from private sector, government and academia exist within organizations such as the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA) to provide guidance for Cloud adoption.

Analysis – Policy – Cloud Council

Recommendation

- Establish a Government of Canada Cloud Council made up of public sector participants and manage on-going collaboration with industry and other third parties through existing Cloud Computing Industry Working Groups.
- Ensure that the GC Cloud Council includes participation from a cross section of departmental CIO's with varying needs based on security profile, service delivery profile, or size.
- Determine Pan-Canadian representation on Council.
- Consider establishing parallel internal working groups to assess and deliver recommendations to the Cloud Council regarding strategy and implementation.
- Favour alliances with Cloud Industry organizations that are global in nature, as Cloud innovation and learning tend to transcend regional boundaries.
- Leverage established channels such as PSCIOC for cross-jurisdictional collaboration and communication.

Analysis – Policy – Canadian Cloud innovation

Description
Respondents proposed several strategies to promote and encourage Cloud innovation in Canada to fuel the Canadian Cloud economy.

Viewpoint(s)		
Financial Incentives Grants or tax credits for Canadian companies investing in Cloud innovation.	**Training and incubators** Work with Canadian institutions to promote training related to Cloud and to establish incubators for Cloud start-ups.	**Procurement strategies** Implement a “Buy Canadian first” policy, require Industrial and Regional Benefits or use a Canadian Small and Medium Enterprise (SME) “Set-aside” approach for Cloud procurement.

Analysis

- Many private sector organizations do not fully understand tax benefits and liabilities associated with Cloud investments.
- In the US, federal, state and local tax credit regimes are in place; R&D credits are most commonly claimed. Australia and the UK also offer tax relief to offset R&D efforts.
- Startup funding for Cloud technology and incubator programs are commonplace and often backed by Private Investors.
- Trade Agreements may limit the Government’s ability to favour Canadian Cloud SMEs.

Analysis – Policy – Canadian Cloud innovation

Recommendation

- Investigate the expansion of R&D tax credits and tax relief for Canadian Cloud SMEs.
- Launch an effort to ensure that tax benefits and liabilities associated with Cloud investments are well understood.
- Monitor how market forces, such as competition, venture capital or corporate investments, shape the Canadian Cloud economy before considering any Government influence.
- Assess procurement mechanisms that could be used to encourage Canadian Cloud SME while respecting existing Trade Agreements.

Analysis – Policy – Cloud workload

Description
Respondents lobbied for clear guidance on the type of workload and data that can be migrated to the cloud.

Viewpoint(s)		
Cloud decision tool Departments self-assess the propensity of workloads for Cloud to determine optimal delivery and procurement strategy.	**Prescriptive workload** Departments are required to favour Cloud deployment for specific workloads that are known to be Cloud friendly.	**In-depth assessment** A mandated Architecture Review performs a one-of assessment of the optimal delivery for every workload.

Analysis

- For Cloud to gain significant momentum with the Government, it must be the norm, rather than the exception.
- The volume of IT Architecture Reviews necessitates a federated approach, which brings consistency challenges. Clear guidelines and established architectural patterns can alleviate these challenges.

Analysis – Policy – Cloud workload

Recommendation

- Publish a Cloud decision tool to provide guidance to departments in consistently identifying Cloud candidate workloads. A point-based assessment model with a minimum threshold would be optimal. See Appendix A for a sample cloud suitability checklist for SaaS that could be used as a decision tool.
- Collaborate with key departments to pre-emptively identify low-risk Cloud friendly workload with a focus on high impact and pervasiveness.
- Create a central Cloud registry to inventory workloads and Cloud providers in order to quickly identify bright spots, identify patterns and monitor adoption.
- Be mindful to consider cases related to new workloads as well as legacy workloads as the business case and drivers may differ significantly.

Analysis – Business – GC Cloud

Description

GC Cloud is defined as cloud infrastructure provisioned by Shared Services Canada for exclusive use by the Government of Canada comprising multiple departments and Agencies. It is owned, managed, and operated by the Government of Canada and it exists on premises. The industry has been asked to comment on the financial, technical and business implications of positioning GC Cloud as Canada's preferred approach for cloud services.

Viewpoint(s)

GC Cloud will provide all cloud services and SaaS providers will build their services on top of GC Cloud.	**GC Cloud will provide some cloud services** while Public Cloud will be leveraged for other services.	**Public Cloud will provide all cloud services**.

Analysis

- GC Cloud's on-demand scalability, security, elasticity, innovation pace, cost savings and business agility will be constantly outpaced by the public cloud. GC Cloud is essentially a data center provisioned and maintained by SSC in a traditional IT managed services approach, involving:
  - significant up front capital investment and ongoing Capex instead of Opex
  - reduced functionality, scalability and agility
  - limited supplier pool due to specialized requirements such as:
    - to provision and support SaaS/PaaS on top of a government managed platform
    - to comply with costly security certifications against GC Cloud specific requirements
    - to take on increased operational risk

Analysis – Business – GC Cloud

Analysis (continued)

- PaaS and SaaS on top of GC Cloud would be challenging and unlikely to be successful. To facilitate the management and troubleshooting of their solutions, SaaS and PaaS providers have either built out infrastructure platforms specific to their requirements or tailored their software and middleware to run on public commercial IaaS platforms. Requiring these providers to use GC Cloud as their IaaS platform will:
    - impact their ability to deliver at the quality levels they are able to commercially
    - increase the cost of their services due to higher operational risk (additional effort and tools will be necessary to remotely manage and troubleshoot their solutions or to perform a one-of-a-kind deployment of their offering)
    - restrict their speed and agility to roll-out upgrades or patches, respond to incidents and resolve problems
    - reduce benefits such as any price reductions resulting from economies of scale or technical innovation
- A hybrid GC Cloud/Public Cloud model is a feasible option that would allow Canada to benefit from the public cloud value proposition, while retaining full control over sensitive data.
    - Classified workloads that need to be under the full control of Canada's security requirements would need to exist within GC Cloud.
    - Where possible, GC should favor public Cloud usage in order to enable rapid and efficient adoption and best value.
- Leveraging the public cloud for all GC cloud needs raises data security and sovereignty concerns that are challenging to alleviate at this point.

Analysis – Business – GC Cloud

Recommendation

- Choose GC Cloud for classified workloads requiring the level of security that can only be provided by SSC and maximize the use of public commercial cloud services for non-sensitive workloads.
- Broaden the definition of GC Cloud to also include private IaaS that has been pre-qualified by Canada and shown to meet security requirements. SSC may act as a broker for all IaaS workloads.
- Recognize that the PaaS and SaaS provider pool that will agree to tailor their offerings to meet the GC Cloud requirements will likely be very limited and that those providers who agree will adjust their prices and SLAs to reflect the increased risk, overhead and loss of full stack control.
- Recognize that solutions deployed on top of GC Cloud will more frequently include departmental applications and solutions built by System Integrators through larger procurements where T's and C's can be negotiated.
- Expect and plan for the redistribution of IT and non-IT skills that accompany the movement of workloads from an in-house delivery model to a Cloud delivery model.
    - Assess IT professionals technical and business skills and ensure these skills are developed to support key trends and technology options such as Cloud, particularly in IT planning roles (Business Analysis, Enterprise Architecture, Security and Risk Management, Sourcing, Strategy and Planning, etc.).
    - Prepare for an evolutionary shift in job titles and descriptions.
    - Prepare for important changes in the role of technical professionals, with an emphasis on roles that perform brokering, integration and negotiation for services with outside entities.
    - Plan for the subsidence of certain 'build' and 'run' roles such as infrastructure specialists, application specialists, system administrators and capacity planners as those functions increasingly become the responsibility of Cloud service providers.

Analysis – Business – Cloud Exit

Description
GC needs to assess cloud exit strategies available in the industry and mitigate vendor lock-in risk by ensuring that feasible options for data migration from one cloud provider to another, data holdings transfers between cloud solutions and data repatriation in specific circumstances can be contractually provided at a reasonable cost.

Viewpoint(s)	
Define data repatriation and migration strategies up front.	**Rely on common, widely adopted technologies and cloud interoperability standards** and address cloud exit risks through solution architecture.

Analysis

- The rapid technological advancement of migration tools and open standards supports the fact that data migration and portability are considered standard requirements in the cloud industry. Customer's full control and ownership of the data are also typical requirements that CSPs currently have to meet for their client base.
- The diversity of migration tools and approaches generates a lack of transparency around migration costs and cost reduction strategies.
- Depending on how the acquired GC cloud services stack is architected, the responsibility for extracting and migrating data may be shared with or allocated in full to a SaaS vendor but it will likely reside exclusively with GC for an IaaS platform.

Analysis – Business – Cloud Exit

Recommendation

- Provisioning for a feasible migration strategy starts with the vendor and service selection:
  - Choose a CSP that provides appropriate migration tools and associated best practices and validate portability whenever possible.
  - Favour public commercial cloud services and COTS offerings versus one-of-a-kind solutions custom-built to address unique requirements.
  - Select cloud platforms and solutions that support commonly used file formats and technologies and attempt to the greatest degree possible to utilize these standards.
  - Ensure that a healthy competition exists for services procured to minimize the risk of vendor lock-in and reduce potential switching costs.
  - Consider *hard exit* cases (e.g. due to provider insolvency or other issues), where time is of the essence and the collaboration of the Cloud Service Provider may not be at its usual level, in planning for a Cloud exit.
- Ensure service agreements include explicit contractual clauses specifying that:
  - the portability and migration requirements are core requirements; and
  - data ownership remains with Canada under all circumstances.

Analysis – Business – Service Level Agreements (SLAs)

Description

As a key component of the cloud service agreements, SLAs must reflect the most important and appropriate metrics to measure. Recognizing the diversity of vendor-provided SLAs available in the cloud market and the vendors' reluctance to allow clients to customize them, GC needs to decide on a service management strategy for cloud services.

Viewpoint(s)

Adopt the vendor-provided SLAs and KPIs.	**Focus on business outcome SLAs when possible.**

Analysis

- Depending on the type of cloud services provided, vendors approached the SLA topic differently:
  1. Cloud-native service providers and managed services providers who deliver solutions based on public cloud IaaS are reluctant to provide customized SLAs for the following reasons:
     - Cloud services are used by a significantly large user base and economies of scale are only realized when terms and conditions operate the same way for each customer and services are standardized.
     - Implementing customized SLAs would require customized data collection, data reporting and (if applicable) remedies, generating additional costs and complexity.
     - SLAs are a key component of the "value proposition" of a cloud offering thus cloud vendors are incented to offer SLAs that effectively measure the performance of the salient elements of their service delivery; SLAs are typically refined over long periods of time, based on thousands of interactions with the provider's customers and a deep understanding of their clients' common needs.

Analysis – Business – Service Level Agreements (SLAs)

Analysis (continued)

- Public commercial cloud solution providers have made it clear that they may have no choice but to forego an opportunity to provide their services to GC if customized SLAs are required.

2. Managed services providers who deliver solutions in the traditional IT outsourcing model agreed to customized SLAs and KPIs, but the costs incurred by GC will be higher. However, overly prescriptive metrics may reduce the pool of providers who could otherwise deliver value to GC.

- NIST has identified "Measured Service" as one of the five fundamental characteristics of the cloud computing model. A "measured service“ is described by the cloud service properties that have to be measured and their associated standards of measurement or metrics.
- The diversity of the SLAs that are currently common practice in the cloud industry creates a lot of ambiguity due to inconsistent technical terminology when defining what is being measured. GC will need to evaluate and compare these highly diverse SLAs.
  - SaaS SLAs should focus on business metrics, while IaaS SLAs should focus on technical metrics.
  - Business outcome based SLAs will help GC move towards managing outcomes and consuming services instead of constructing them. These outcome-based measurement should reflect the business needs that GC is looking to meet when selecting a specific cloud offering, such as:
    - reduce infrastructure and application TCO costs;
    - increase speed and agility in procuring and provisioning infrastructure;
    - foster innovation through access to continuously evolving technology platforms;
    - benefit from the constantly shrinking cost of technology;
    - deliver high customer and end-user satisfaction; and
    - optimize quality of application delivery.

Analysis – Business – Service Level Agreements (SLAs)

Recommendation

- For services delivered by **cloud-native service providers**:
  - Ensure a strong understanding of key business and technical performance requirements.
  - Be cautious when attempting to customize commercial public cloud SLAs and don't make custom SLAs and custom KPIs mandatory requirements in public cloud procurements without first assessing the appetite of the market.
  - To mitigate risk, evaluate the vendors' SLAs as part of the overall cloud service response (e.g. rated requirement).
  - Capture service level expectations specific to GC as mandatory non-functional requirements in RFPs.
- For services delivered by **managed services providers** who operate in the traditional IT outsourcing model and are willing to meet custom SLAs and KPIs.
  - Define a set of specific and critical performance criteria tied to service level penalties/credits.
  - Avoid overly prescriptive metrics as this will increase the cost of the offering and the degree of vendor lock-in, while limiting the interest of potential providers.
  - GC Cloud should offer SLAs that are comparable to the private sector SLAs.
- Use standard Cloud Metrics developed by NIST to assess and compare vendor-defined SLAs and KPIs or to define custom SLAs and KPIs *(Reference: Cloud Computing Service Metrics Description, NIST Special Publication 500-307).*

Analysis – Business – Mitigating Cloud Sprawl

Description
With a mandate to provide flexible and agile consumption of IT services through on-demand cloud offerings to its stakeholders and promote cloud adoption, GC must have a strategy in place to mitigate the risk of cloud sprawl.

Viewpoint(s)			
Governance	**Chargeback Mechanisms**	**Broker Oversight**	**Automation**

Analysis

- Given that data governance is not new to GC, it would not be difficult to bring it to the next level of maturity and align it with a cloud context. A formalized cloud governance strategy would provide the oversight and the mechanisms necessary to address scenarios such as:
  - multiple separate environments or solutions catering to the same business needs
  - duplicate data repositories
  - data without retention policies.
- A chargeback models that can be attributed and presented to individual users and departments would increase accountability and control sprawl.
- The broker oversight option has the potential to create a burdensome and time consuming process for the business, impacting the very benefits that GC is looking for in cloud service deployments (increased flexibility and responsiveness to business needs).

Analysis – Business – Mitigating Cloud Sprawl

Analysis (continued)

- Automation relies on one or multiple technology solutions for monitoring the cloud usage, generating real time analytics, providing reporting capabilities as well as alerts and notifications when preset threshold are reached, and preventing users from consuming additional cloud computing when predefined conditions are met. This option could prove to be very expensive – the more diverse the cloud computing platforms and solutions selected by GC are, the more diverse the monitoring tools required by this option. In addition, automation creates ongoing costs through operation maintenance overhead.

Recommendation

- The most effective solution is a combination of governance and automation.
  - Consistent platform interfaces would support common operations management tools, reducing the overall automation costs.
  - Governance would provide a flexible mechanism that could be adapted as the cloud adoption evolves within GC – stricter, more rigorous and federated governance policies and mechanisms for the initial phases, but more decentralized, team-led policies as internal cloud competencies and cloud usage increase. A Cloud business broker may help enforce governance in this area.

Analysis – Business – Cloud Brokers

Description

To deliver cloud services to its internal and external users, GC will rely on an ecosystem of public cloud vendors, managed services providers, system integrators and subject matter experts providing diverse solutions and services at different price points and meeting GC's business, compliance and service requirements to various degrees. A cloud broker is a third-party acting as an intermediary between the GC demand side and the available supply. The industry has been asked to comment on the business value and role of a cloud broker.

Viewpoint(s)

Cloud brokers are not needed.	**GC should build their own cloud broker.**	**GC should contract only one cloud broker who can not be a CSP.**

Analysis

- GC will have a complex cloud landscape with multiple and diverse types of systems, solutions, vendors and integrators, which will demand a highly integrated management approach. The majority of the vendors agreed on the necessity of a broker role.
- However, as an emerging role in this industry, the cloud broker function was inconsistently described and analyzed by the vendors – a cloud broker could be:
  - An entity such as:
    - A distributor - procures cloud computing through a reseller, system integrator or consulting firm as part of a comprehensive solution versus procuring directly via a CSP.
    - An integrator of cloud services – provides integration services between different cloud platforms, between different layers within the same cloud or between on premise and cloud solutions.

Analysis – Business – Cloud Brokers

Analysis (continued)

        - A cloud vendor manager – pre-vets and evaluates providers to accelerate the selection of cloud services for the various government business units.
        - An expert A-Team comprising different skillsets, such as procurement, business, architectural and technical.
    - A solution such as:
        - A cloud management platform - provides a single and unified management solution to help customers view, manage and govern their consumed cloud services through a ‘single pane of glass’.
        - An intelligent subscription engine - compares, selects and subscribes to best in class cloud services based on workload characteristics.
- No broker
    - Adding a broker has the potential to add delays, cost and complexity to cloud services delivery, eliminating one of the most fundamental benefit of public commercial cloud services: fast, on-demand self-service.
    - Brokers are costly and the funds are better spent on training the internal GC staff to fulfill brokerage roles as needed.
    - It is premature – first, generate sufficient demand for cloud adoption and manage the supply with internal resources before considering a cloud broker.
- GC should build their own cloud broker
    - GC should learn how to use the cloud themselves to their advantage via direct experience as this option provides full ownership and control over cloud service choices, governance and performance management as well as a holistic view of the cloud needs across all of GC .

Analysis – Business – Cloud Brokers

Analysis (continued)

- Most importantly, this option will provide GC with a first-hand understanding of the challenges, opportunities and risks associated with its cloud decisions.
- Expert teams providing cross-functional skillsets (technical, business, architecture, legal, procurement) will be required to ensure the success of this approach; GC will have to consider the training costs associated with this option.

- GC should contract only one cloud broker who cannot be a CSP
  - In this scenario, GC should retain architectural control over the technical and service management layers and avoid leveraging a CSP (or a vendor partnered with any other downstream cloud services provider) as a broker, to ensure fair equal access to all cloud vendors and eliminate any risk of the broker becoming an entrance barrier for public cloud services in the GC.
  - The advantage of this option is that GC will benefit from cloud experienced resources from the vendor community, able to provide the advanced cross-functional skillsets required of a successful broker.

Analysis – Business – Cloud Brokers

Recommendation

- Define and address the success factors of a brokerage approach. Whether insourced or outsourced, a broker will require:
  - standardized procurement policies across GC and practical guidance for vendor and service selection;
  - common data classification principles, data taxonomy and cloud workload decision framework across GC;
  - formalized governance and enterprise architecture policies, tools and structures; and
  - a GC service catalog based on common standards for the description and consumption of cloud services.
- Define what a cloud broker means for GC with a focus on a small set of cloud broker functions in the context of the first phase of cloud adoption. As the cloud adoption increases and the GC's own skillsets and level of comfort with cloud services build up, refine and expand the required cloud broker functions through an iterative approach to discover and validate the true business value and role of a broker in the GC space.
- Leveraging this iterative approach:
  - Position and refine the role of SSC as the GC's Private/Community IaaS and, eventually, PaaS broker. Ensure the role is focused on facilitating services and responding to business needs with agility in order to position SSC as a Cloud enabler.
  - Democratize SaaS procurement for departments, possibly through the use of a pre-vetted Cloud solutions marketplace.
  - Consider outsourcing the cloud security access broker role (see Appendix D – Cloud Security Access Brokers).

Analysis – Business – Launch Strategy

Description
Respondents included recommendations for “Getting Started” with Cloud. Two approaches were suggested. The first approach recommended an extensive **Requirements Analysis** phase to determine the strategy followed by a traditional procurement phase. The second and dominant recommendation was for an agile **Prototyping and Pilot** approach to “Learn by Doing”.

Viewpoint(s)	
Full Requirements analysis first.	**Establish foundational strategy and refine through prototyping and pathfinder initiatives.**

Analysis

- Cloud adoption will require new ways of thinking about IT Service delivery and will change the way the GC approaches sourcing, governance and security.
- Cloud offerings are evolving rapidly, with a myriad of complex options and factors to consider for acquisition, use, and management with associated learning curves.
- Risk management is essential for sensitive workloads and will require measured analysis to determine acceptable models for deployment with a near term bias towards private cloud for sensitive workload. Less sensitive use cases could benefit from rapid experimentation.
- Experimentation is the best way to determine what works and doesn’t work in order to refine the implementation strategy based on real world experience.
- A series of pathfinder projects would provide the ability to test approaches for both quick win scenarios and more complex needs to determine what works in the Canadian context.

Analysis – Business – Launch Strategy

Recommendation

- Establish a set of Pathfinder projects to develop an experience base from which to refine the strategy.
- Look for a mix of projects that:
  - Provide visible quick wins and momentum for the Cloud initiative
  - Include pilots that test multiple Service Models (IaaS, PaaS, SaaS) and Deployment Models (Public, Private, Hybrid and Community Clouds).
- For IaaS, with SSC as broker, explore projects for on-premise and off-premise Private Cloud, and Public Cloud.
- Engage the GC Cloud Council to propose pathfinder projects based on departmental need.
- Potential workloads include the following, assuming a compatible security and risk profile:
  - PaaS/IaaS – Information Dissemination (e.g web hosting, Open Data, 311)
  - PaaS - Development and Test environments
  - SaaS – CRM/Case Management (for processes that are external and public-facing)
  - SaaS – Collaboration (with citizens, private sector organization or other governments)
  - SaaS/PaaS – Geo-spatial
  - IaaS – Project specific (unique requirements), through SSC

Analysis – Business – Length of Deal Commitment

Description
Some respondents recommended avoiding long term commitments while others favoured a minimum 3 year commitment. Direction will be required on length of commitment to ensure sufficient term to realize benefits and gain pricing leverage while avoiding lock-in for a rapidly evolving technology segment.

Viewpoint(s)	
Avoid long term commitments	**Introduce a minimum 3 year commitment.**

Analysis

- Three year deals are increasingly standard at least for SaaS but would usually give more leverage than 1 or 2 years deals if available[1].
- Five year deals typically provide even more leverage and may translate in an RFP scenario into improved overall pricing.
- For significant SaaS deals, a minimum 3 year commitment is not unreasonable as this may be a suitable term to establish the service and assess value and benefits in the public sector before considering termination.
- UK Cloud Adoption experience limiting contracts to 2 years was viewed by some vendors and consumers as too short given project implementation timelines[2].

Recommendation

- Consider establishing or accepting a minimum 3 year commitment for SaaS procurements.

[1]: Source: Gartner Research Toolkit: Negotiating Optimal SaaS Contract Terms and Conditions, Alex Bona et al, G00271157

[2]: Source: Gartner Research - U.K. Government G-Cloud Learns Lessons for Better Catalog-Based Procurement, Neville Cannon, G00265652

Analysis – Procurement – Cloud Terms and Conditions

Description
Respondents noted that Cloud Terms and Conditions for **Public** offerings typically do not bend to individual client's requirements. Understanding the extent to which T's and C's can be negotiated will be critical to ensure best value for Canada.

Viewpoint(s)	
Terms and Conditions for public offerings are non-negotiable and consumer must accept provider's terms.	**Some Terms and Conditions are negotiable.**

Analysis

- Many SaaS providers represent contracts as entirely standardized and state unequivocally that they cannot be altered at all.
- The SaaS business model is predicated on tremendous standardization to drive economies of scale. This applies to both the technology and the contracting models.
- Gartner's experience suggest some negotiation is possible as consumers attempt to get to a more balanced and less one-sided contract but negotiation is less flexible than in traditional outsourcing or on-premise software deals.[1]
- Contract managers may have leverage for beneficial terms when negotiating initial deals but bargaining power is eroded at renewal time when switching costs become a factor[2].

[1]: Source: Gartner Research Toolkit: Negotiating Optimal SaaS Contract Terms and Conditions, Alex Bona et al, G00271157

[2]: Source: Gartner Research Toolkit: Avoid Risks in IaaS Contracts by Understanding the Most Common Terms, Daniel Barros, G00265846

Analysis – Procurement – Cloud Terms and Conditions

Recommendation

- Plan to negotiate terms and conditions but recognize that negotiation is more limited than in traditional outsourcing or on-premise software situations.
- Identify key negotiating items and develop a Plan B if mandatory items cannot be negotiated.
- Recognize that deal size and negotiation flexibility are related and understand that smaller deals may have limited to no negotiation room.

[1]: Source: Gartner Research Toolkit: Negotiating Optimal SaaS Contract Terms and Conditions, Alex Bona et al, G00271157

Analysis – Procurement – Cloud Program

Description
Cloud adoption is a major shift in how organizations procure, deliver and manage services to clients. Canada would benefit from a multi-disciplinary Centre of Excellence and PMO to support adoption, value assurance and end user satisfaction.

Viewpoint(s)	
Establish a GC Cloud COE and PMO	**Rely on local departmental coordination**

Analysis

- Cloud Computing introduces a significant change in the way IT services are delivered and the move has impact on internal IT operations and security staff, procurement staff, and service consumers.
- Best practices and operational procedures must be developed to shift IT delivery from a focus on hands on technical skills to management planning, orchestration and control.
- A shift to Cloud Computing will introduce a dramatic change management requirement within the GC with requirements for targeted communications to multiple and varied stakeholders.

Recommendation

- Consider establishing a multi-disciplinary team to serve as a Centre of Excellence and Program Management Office for the Cloud program to develop and communicate the strategy and best practices across procurement, security, integration, cloud service management and change management.

Analysis – Procurement – Cloud Taxonomy

Description
A cloud taxonomy that is understood and adopted by both Canada and the industry is a fundamental building block for a cloud decision making framework. The GC cloud taxonomy provided in the RFI has been adapted from the National Institute of Standards and Technology (NIST) standards, but the definitions provided include certain areas of ambiguity that might create confusion across the entire sourcing cycle (evaluating and selecting vendor services, understanding and comparing price structures, defining or agreeing to vendor SLAs, managing and measuring service performance, etc).

Viewpoint(s)	
GC Cloud will provide its own cloud taxonomy.	**GC Cloud will adopt the NIST taxonomy.**

Analysis

- The NIST taxonomy comprises broadly accepted definitions and standards, used by most cloud service providers and vendors to describe, package and price their services. NIST's mission is to develop, publish and maintain cloud computing standards and guidelines as the industry evolves.
- Opting for the custom cloud taxonomy means that GC will have to continuously manage (update and publish) the terms and definitions, becoming a taxonomy provider instead of a taxonomy consumer.
- The cloud definitions included in the RFI show a number of inconsistencies with NIST (see next slide).

Analysis – Procurement – Cloud Taxonomy

Analysis (continued)

Reference	GC Definition	NIST Definition
Private cloud	The cloud services are provisioned for exclusive use by the Government of Canada comprising multiple departments and agencies. It is owned, managed, and operated by a private company and exists off premises. *(Ref: ABES.PROD.PW_EEM.B033.E28243.EBSU000, pg 34)*	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. *(Ref: The NIST Definition of Cloud Computing, NIST Special Publication 800-145, pg 7)*
Hybrid cloud	The cloud services are a composition of two or more distinct cloud infrastructures (GC, private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). *(Ref: ABES.PROD.PW_EEM.B033.E28243.EBSU000, pg 34)*	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). *(Ref: The NIST Definition of Cloud Computing, NIST Special Publication 800-145, pg 7)*

Recommendation

- Use the NIST taxonomy for the entire sourcing cycle as well as for any formalized internal policies (governance, enterprise architecture, procurement standards, service catalogs, etc).

Analysis – Procurement – Procurement Vehicles

Description
Respondents suggested different procurement approaches to acquire Cloud services. A well defined procurement approach will have a dramatic effect on time to market and benefits realization for Cloud adoption.

Viewpoint(s)	
Pre-qualify vendors and make offerings available through a Service Catalogue or "Cloud Store"	**Follow a Collaborative Procurement approach to select vendors for specific service types.**

Analysis

- The Gartner 2014 CIO Survey indicated the most significant reason for adopting Cloud was agility. Efficient procurement for Cloud services in the Government of Canada will be a major contributor to improvements in agility for departments.
- Vendors indicated a pre-qualification approach with offerings made available through a Service Catalogue or Cloud Store would be the most effective approach.
- This follows a model similar to the SLSA in Canada and that of the Digital Marketplace (formerly G-Cloud CloudStore) in the U.K.
- Other jurisdictions such as Australia and the U.S. are also following a Service Catalogue approach to speed up procurement.
- The U.K. approach had provision for Pan Government acquisition through the Digital Marketplace but uptake beyond the Central government was limited[1].
- Collaborative procurements will be valuable in cases where the Cloud service is only a subset of a larger total solution being acquired (e.g. ERP solution through a System Integrator) or GC is looking to down-select for commonly procured segment (e.g. IaaS, ERP, CRM).

[1]: Source: Gartner Research U.K. Government G-Cloud Learns Lessons for Better Catalog-Based Procurement, Neville Cannon, G00265652

Analysis – Procurement – Procurement Vehicles

Recommendation

- Implement a pre-qualification approach for Cloud solutions and make them available to consumers through a Service Catalogue.
- Recognize that the breadth of platform functionality, pricing models and other standard terms and conditions will make it exceedingly difficult to compare SaaS offerings directly and look to empower departments to determine best value when acquiring services.
- Explore the approaches from the U.K., U.S. and Australia to understand lessons learned as input to the design and delivery of an effective Cloud Service Catalogue.
- Use collaborative procurements when the Cloud service is part of a larger service or major project involving significant professional services or when looking to down-select vendors in an often-procured market segment.

Analysis – Security – Identity and Access

Description
Comprehensive and controlled Identity and Access has been identified by respondents as a prerequisite for successful Cloud deployment.

Viewpoint(s)	
Cloud service specific Identity Each cloud provider has built-in identity and access.	**Federated identity** Government sets up a Federated identity framework such that a user's identity is shared across multiple Cloud services, from various service providers, in addition to traditional IT systems.

Analysis

- Federated identity, in all its forms, is a foundational capability in the age of Cloud and Digital.
- As systems become increasingly distributed, federation can enable trusted authentication for employees, partners and citizen and minimized risks related to onboarding and offboarding, redundant identities and access management.
- As federation implementations become more common, intelligent and distributed, it will be important to manage the proliferation of federated user stores and federation access policy configurations.

Analysis – Security – Identity and Access

Recommendation

- Federated Identity will facilitate Cloud initiatives by securing access to Cloud services by any user, anywhere.
- Until Federated Identity is available, be mindful of the source of identity for each Cloud workload.
- Because of the foundational nature of identity in establishing the security of Cloud services, multifactor step-up authentication capabilities should be strongly considered.

Analysis – Security – Security and Information Management

Description
Under the shared responsibility model, data management has significant security implications for both the vendor and GC: data classification is the driver for security settings, data residency locations, data encryption, monitoring and audit requirements, backup and recovery procedures, retention policies as well as privacy requirements. The industry has been asked to assess the impact of data management on their offerings and provide pragmatic approaches to data management challenges.

Viewpoint(s)	
Departments should determine their own security, privacy, audit and data residency needs for each cloud solution.	**A consistent data classification structure driving standardized security, privacy, audit and data residency across the entire GC should be used.**

Analysis – Security – Security and Information Management

Analysis

- Clear data classification and robust data governance are key GC responsibilities, with a significant impact on the cloud providers' ability to successfully protect Canada's data. The vendors have indicated they can meet advanced security requirements, provide Canadian data storage, apply data encryption when necessary and provide auditing and monitoring functionalities, as long as the right cloud solution is selected for the right dataset and workload.
- A common data classification across all levels of government departments will be difficult to implement due to the different data privacy and security standards mandated by Canada's provincial and federal laws.
  - Defaulting to the highest possible security requirements or designing a blanket policy in an attempt to normalize these standards will only increase the solution costs and limit the providers' pool.
  - Updating the legislation to support common data privacy and security standards across Canada will take a long time.
- If the various government stakeholders are to determine their own security, privacy, and audit needs based on a data classification model with a provincial or departmental scope, there is still a concern related to the accuracy of these decisions. One risk mitigation approach would be an in-house or outsourced business broker taking on this responsibility. An in-house broker would be most beneficial as it would allow the GC to build internally key business brokerage competencies such as:
  - defining data management requirements instead of going straight to selecting a tool or solution;
  - continuously refining data classification, data privacy, data retention models as the business evolves; and
  - monitoring data governance compliance.

Analysis – Security – Security and Information Management

Recommendation

- Define clear and concise data classification principles and labels as well as data risk categories that are required and are applied consistently across all departments (see Appendix C – Information Confidentiality).
- Allow the various government levels to determine their own security, privacy, and audit needs based on a data classification model using their own scope by leveraging a business broker.
- Consider performing periodic audits of local implementations to ensure consistent application of data classification and protection.
- Establish an internal competency center for cloud brokerage.
- Provide risk-based guidance through a common cloud workload decision framework across all departments (see Appendix B - Assessment of a Workload for Cloud Suitability).

Analysis – Security – Cloud security certification

Description
Respondents noted that several Cloud security certifications are available and could be leveraged as part of the cloud initiative rather than build one from the ground up.

Viewpoint(s)		
Leverage established security certification Screen Cloud providers by using existing, industry-established, security certification.	**Augment established security certification** Add GC-specific requirements on top of existing security certification(s).	**Custom-build a new security certification** Create and assess Cloud providers using a custom-built security certification.

Analysis

- Many Cloud service providers have architected their service to meet industry standard framework and invested to demonstrate and maintain compliance.
- The investment required to demonstrate compliance to Cloud security certifications is not trivial and can become a barrier to entry for new or smaller Cloud service providers.
- Control frameworks such as CSA STAR, FedRAMP/NIST and ISO 27001 have emerged as standards in terms of security certification in the industry.
- Audit frameworks such as SSAE16, ISAE 3402 and AT-101, which have been used for compliance in the IT service industry are gaining popularity in assessing Cloud service providers.

Analysis – Security – Cloud security certification

Recommendation

- IT must collaborate with legal and procurement to institutionalize Cloud security governance mechanisms and develop a Cloud security strategy.
- Model and assess risks of cloud security. Determine and lower the trust requirement for Cloud service providers (by using compensating controls) as much as possible.
- Align cloud security certification to established industry standards, to recognize existing Cloud service provider accreditations, and bridge gaps by adding the controls necessary to meet Government of Canada security standards. This will require mapping the main industry security certifications (CSA STAR, FedRAMP/NIST and ISO 27001) to Government standards, inventory gaps and publish additional controls needed to meet the needs of the Government.
- On an ongoing basis, perform assessments in a variety of ways, including reviewing responses to a questionnaire, reviewing third-party audit statements, conducting an on-site audit and/or monitoring the CSP.

Analysis – Security – Security of Public Clouds

Description
Many respondents advanced the notion that Public Cloud providers in many cases can be as secure or more secure than private environments due to intense focus and dedicated resources.

Viewpoint(s)	
Cloud providers are less secure than traditional on-premise environments.	**Cloud providers have a higher level of security than traditional environments.**

Analysis

- In multiple Gartner surveys, security is cited as the number one inhibitor to cloud adoption.
- Many IT professionals have an opinion that cloud computing will be less secure than what they can deliver themselves on premise.
- Many Cloud Service Providers recognize the concern of potential customers and realize a significant breach could have far reaching effects on reputation and business results so invest heavily in appropriate security controls to mitigate risk.
- Large cloud providers have the scale and resources to develop security as a core competency.
- Smaller SaaS providers may not have the same scale as larger players to focus on security in the same way.
- Cloud Service Providers have the ability to at least be as secure as on-premise solutions but the reality will vary by provider based on the security controls in place.

Recommendation

- Assess cloud vendors on an individual basis to determine their security posture and risk and don't assume that cloud solutions are less secure by default.

Analysis – Security – Information confidentiality

Description

Multiple approaches were proposed by respondents to meet information confidentiality requirements while using public Cloud services.

Viewpoint(s)

Filtering	Transformation	Separation
Detecting and preventing sensitive information from leaving the trusted network and reaching Cloud services.	Encrypting, hashing or masking sensitive information through algorithmic changes to obfuscate it.	Omitting or storing sensitive information in an isolated, secure environment such as an on-premises database or content management system.

Analysis

- Different approaches offer varying degree of protection.
  - Separation offers the highest level of confidentiality as it allows sensitive information to remain within.
  - Transformation offers medium-surety protection, provided that the quality of implementation is high.
  - Filtering relies on fingerprints or information fragments, which requires frequent updating and can easily be thwarted. It only offers low-surety protection.
- Approaches can be used in different layers of the infrastructure (e.g. point of use, application, storage, network) and can be combined for greater efficiency.
- Long-term confidentiality through cryptography is very difficult to achieve; over time, secret keys may be compromised, some component schemes may collapse or some assumptions broken.

Analysis – Security – Information confidentiality

Recommendation

- Strong information governance is paramount to ensure appropriate information classification and to minimize risks.
- Clear and concise information confidentiality policies are required and must be applied consistently.
- Determine the maximum classification (e.g. Protected A) or risk rating for information that can be processed and stored on public Cloud services. Use private Cloud systems to process and store sensitive and confidential information above this classification.
- Establish data confidentiality standards for information processed or stored on public and private/community Cloud services. For instance, plan on employing data encryption for all information on public Cloud, both in transit and at rest, as a way to mitigate confidentiality risks. Pay close attention to the physical location of the encryption and decryption process as well as key management. See Appendix C for more details.

Analysis – Security – Data residency

Description
Many jurisdictions have developed regulations to provide legal protection for many different form of sensitive information (e.g. Personally Identifiable Information, Private Health Information, Tax Information, export restricted information). Enforcement of these regulations can result in financial penalties as well as criminal prosecution of individuals or organizations responsible for theft or negligence related to data breaches. In addition, governments have implemented laws granting access to law enforcement authorities and intelligence agencies that can apply to data stored within, or even transmitted through, their jurisdiction. Respondents have indicated that while data residency (both at rest and in transit) was desirable, it may be difficult to enforce when dealing with public Clouds.

Viewpoint(s)		
No assumption or attempt to ensure residency for public Cloud Use public Cloud services assuming that the data can be stored or can transit in other jurisdictions.	**Ensured data residency** Contractually mandate and enforce residency of data, both at rest and in transit, when using public Cloud services.	**Encryption as an alternative to residency** Leverage encryption to prevent the disclosure of data stored on public Clouds in other jurisdictions.

Analysis – Security – Data residency

Analysis

- Most true public Cloud service providers will not be able to guarantee data residency. Some will be able to fence the workload to data centers within a given jurisdiction but very few, if any, can guarantee that the information will not transit outside of the jurisdiction. Furthermore, some multinational Cloud service providers may be subject to laws forcing them to provide secret access to data under their control, regardless of the physical location of the data.
- Encryption does not provide assurance of confidentiality over a long period of time, nor does it provide effective protection against access by foreign governments or entities with significant resources at their disposal.

Recommendation

- Understand what information is required to remain within the jurisdiction and perform a risk / benefits assessment to determine if it can be stored on a public Cloud service.
- Assume that the data used in a public Cloud may ultimately be accessed by foreign governments or entities, even in cases where the workload is hosted within the agreed upon jurisdiction.
- Do not use encryption as a way to circumvent data residency requirements. While encryption may prevent direct access by foreign entities, it does not eliminate liability.

Summary of recommendations

Gartner

Summary of Recommendations

This section summarizes Gartner's key recommendations and organizes them in three phases:

- **Before Cloud**,
- **Cloud Inception** and
- **Cloud Adoption**.

These recommendations will contribute to the advancement of the Government's Cloud adoption maturity along five critical dimensions:

Organizational

The people, teams and structure involved in designing, implementing, supporting and utilizing public cloud services

Governance

The set of principles, policies, standards, processes and guidelines that enables business and IT to successfully leverage public cloud services to meet business goals

Technology & Applications

The tactical and strategic technology components and application workload evolution that enable organizations to consume public cloud services efficiently and securely

Provider Selection & Management

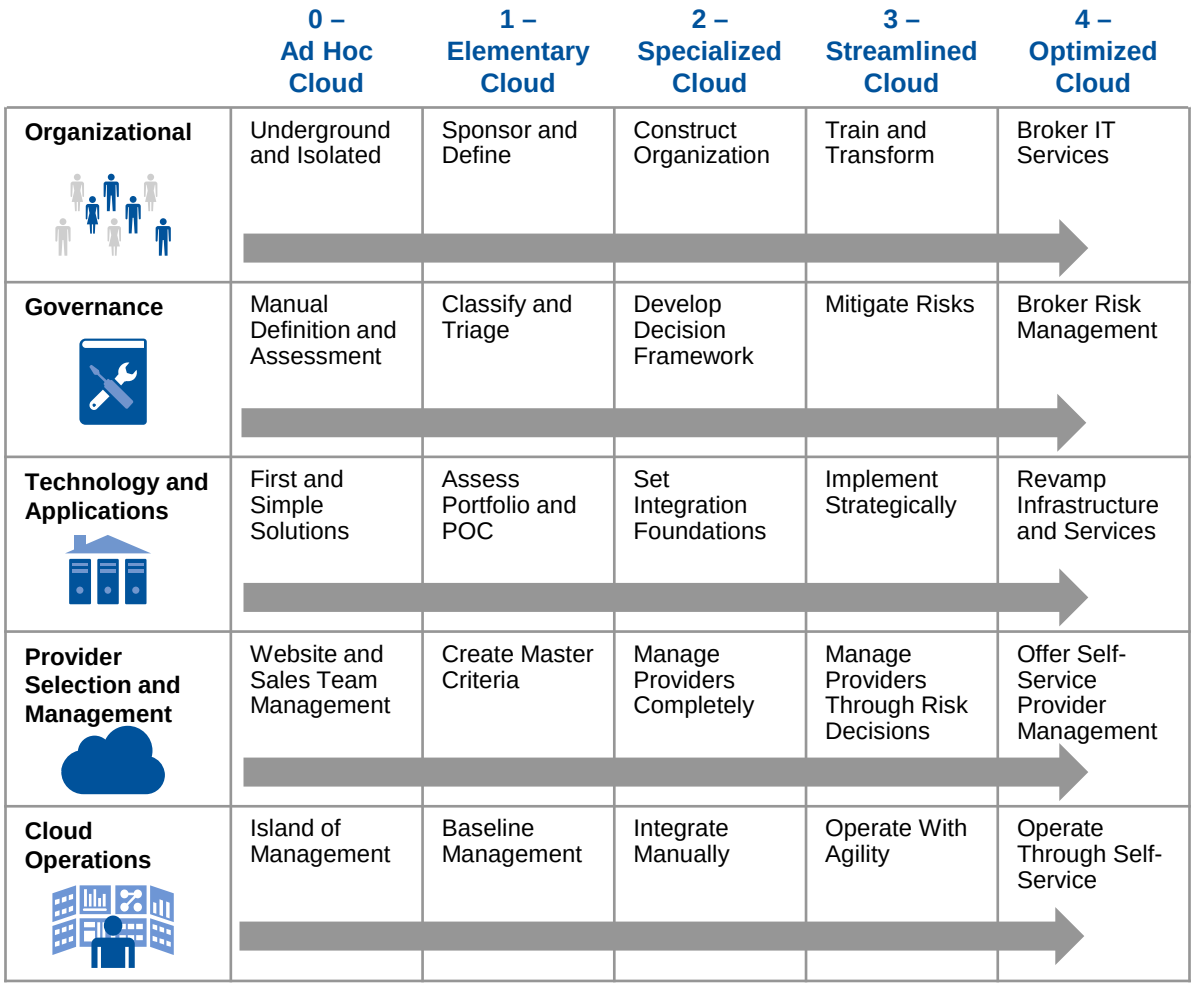
The act of evaluating, selecting, negotiating and managing public cloud service provider (CSP) relationships.

Cloud Operations

The ability to extend traditional IT operations management (ITOM) practices to public cloud services and applications

Gartner

Gartner's Cloud adoption maturity plan



Source: Solution Path for Implementing a Public Cloud Adoption Maturity Plan, May 2015 (G00263762)

Summary of Recommendations by phase

Before Cloud (3-6 months)	Cloud Inception (12-18 months)	Cloud Adoption (ongoing)
Establish Governance ▪ GC Cloud Council ▪ GC Cloud Center of Excellence **Define initial policies and guidelines** ▪ R&D tax credits and tax relief ▪ Cloud workloads decision tool ▪ Confidentiality-based information classification ▪ Data residency ▪ Data protection (encryption, risk-based guidance) ▪ GC Cloud definition ▪ Migration planning ▪ Cloud taxonomy **Plan Cloud inception phase** ▪ Initial Cloud workloads and Pathfinder projects	**Execute Cloud pilots** ▪ Potential cloud workloads **Gather insights** ▪ Cloud registry **Refine policies and guidelines** ▪ Cloud sprawl mitigation ▪ Cloud broker definition ▪ Define Cloud broker roles within GC ▪ Democratized procurement ▪ Cloud solutions security assessment **Establish procurement** ▪ SLAs definition and negotiation ▪ Cloud vendor prequalification ▪ Cloud Service Catalogue ▪ Collaborative procurement	**Expand cloud usage** ▪ Cloud Federated Identity ▪ Plan for the redistribution of IT and non-IT skills **Monitor and control for continuous improvement** ▪ Assessment approach

Establish Governance

Before Cloud

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Establish a GC Cloud Council made up of public sector participants and manage on-going collaboration with industry and other third parties through existing Cloud Computing Industry Working Groups.		■						
Establish a multi-disciplinary team led by TBS to serve as a Centre of Excellence and Program Management Office for the Cloud program to develop and communicate the strategy and best practices across procurement, security, integration, cloud service management and change management.		■						

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Define Initial Policies and Guidelines

Before Cloud

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Examine and promote existing incentives (R&D tax credits and tax relief) to encourage Canadian cloud SMEs while respecting existing trade obligations		■						
Publish a Cloud decision tool to provide guidance to departments in consistently identifying Cloud candidate workloads.		■	■		■			
Choose GC Cloud for classified workloads requiring the level of security that can only be provided by SSC (or a pre-qualified private IaaS provider) and maximize the use of public commercial cloud services for non-sensitive workloads.				■				
Broaden the definition of GC Cloud to also include private IaaS that has been pre-qualified by Canada and shown to meet security requirements.		■				■		

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Define Initial Policies and Guidelines (cont.)

Before Cloud

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Facilitate future migration by promoting use of standards, ensuring competition, availability of migration tools and contractual rights to data		■						
Use the NIST taxonomy for the entire sourcing cycle as well as for any formalized internal policies (governance, enterprise architecture, procurement standards, service catalogs, etc.)		■	■	■	■	■	■	■
Define clear and concise data classification principles and labels as well as data risk categories that are required and are applied consistently across all departments		■	■					
Provide risk-based guidance through a common cloud workload decision framework across all departments		■	■		■			
IT must collaborate with legal and procurement to institutionalize Cloud security governance mechanisms and develop a Cloud security strategy		■	■		■	■	■	■

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Define Initial Policies and Guidelines (cont.)

Before Cloud

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Align cloud security certification to established industry standards, to recognize existing Cloud service provider accreditations, and bridge gaps by adding the controls necessary to meet Government of Canada security standards								■
Determine the maximum classification (e.g. Protected A) or risk rating for information that can be processed and stored on public Cloud services. Use private Cloud systems to process and store sensitive and confidential information above this classification			■					■
Establish data confidentiality standards for information processed or stored on public Cloud services			■					■
Do not use encryption as a way to circumvent data residency requirements				■		■	■	■

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Define Initial Policies and Guidelines (cont.)

Before Cloud

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Understand what information is required to remain within the jurisdiction and perform a risk / benefits assessment to determine if it can be stored on a public Cloud service		■	■	■				■

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Execute Cloud Pilots

Cloud Inception

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Potential workloads include the following, assuming a compatible security and risk profile: ▪ PaaS/IaaS – Information Dissemination ▪ PaaS - Development and Test environments ▪ SaaS – CRM/Case Management (for processes that are external and public-facing) ▪ SaaS – Collaboration (with citizens, private sector organization or other governments) ▪ SaaS/PaaS – Geo-spatial ▪ IaaS – Project specific (unique requirements), through SSC			■	■				

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:*  Organizational  Governance  Technology & Applications  Provider Selection & Management  Cloud Operations

Gartner

Gather Insights

Cloud Inception

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Create a central Cloud registry to inventory workloads and Cloud providers in order to quickly identify bright spots, identify patterns and monitor adoption.			■			■		

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Refine Policies and Guidelines

Cloud Inception

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
To control cloud sprawl use a combination of governance, automation (e.g. governors) and cost transparency.		■	■			■		
Define what a cloud broker means for GC with a focus on a small set of cloud broker functions in the context of the first phase of cloud adoption		■	■					
Define Cloud broker roles within GC (e.g. SSC as the GC IaaS broker, PWGSC as a SaaS broker)		■	■			■		
Allow departments to be their own brokers by democratizing PaaS and SaaS procurement		■						
Consider outsourcing the cloud security access broker role		■						■
Assess cloud vendors on an individual basis to determine their security posture and risk and don't assume that cloud solutions are less secure by default.				■			■	■

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Establish Procurement

Cloud Inception

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Expect limited vendor willingness to negotiate existing SLAs for public commercial cloud offerings and focus on business-outcome SLAs for custom SaaS cloud offerings		■					■	
Implement a pre-qualification approach for Cloud solutions and make them available to consumers through a Service Catalogue			■				■	
Explore the approaches from the U.K., U.S. and Australia to understand lessons learned as input to the design and delivery of an effective Cloud Service Catalogue			■				■	
Use collaborative procurements when the Cloud service is part of a larger service or major project involving significant professional services or when looking to down-select vendors in an often-procured market segment	 			■			■	

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Gartner

Expand Cloud Usage

Cloud Adoption

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
Federated Identity should be considered in order to secure access to Cloud services by any user, anywhere.		■	■			■		
Expect and plan for the redistribution of IT and non-IT skills that accompany the movement of workloads from an in-house delivery model to a Cloud delivery model.		■		■				

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:*


Organizational


Governance


Technology & Applications


Provider Selection & Management


Cloud Operations

Gartner

Monitor and Control

Cloud Adoption

Recommendation	Dimension[2]	TBS	GC Cloud CoE	Consumers[1]	GC Cloud Council	SSC	PWGSC	CSEC
On an ongoing basis, perform assessments in a variety of ways, including reviewing responses to a questionnaire, reviewing third-party audit statements, conducting an on-site audit and/or monitoring the CSP.						■	■	■

[1] *Consumers: Departments, Provinces and Territories, Municipalities*

[2] *Dimension:* Organizational, Governance, Technology & Applications, Provider Selection & Management, Cloud Operations

Contacts

Client Contact
Serge Caron
Senior Director
Treasury Board Secretariat
+1 613.952.0960
Serge.Caron@tbs-sct.gc.ca

Gartner Contact
Yannick Bergeron
Associate Director
Telephone: +1 613.696.0427
Yannick.Bergeron@gartner.com

Gartner Contact
Georgiana Badea
Associate Director
Telephone: +1 613.696.0435
Georgiana.Badea@gartner.com

Gartner Contact
Chris Rickard
Director
Telephone: +1 613.696.0423
Chris.Rickard@gartner.com

Client Contact
Troy MacFarlane
Senior Technical Specialist
Treasury Board Secretariat
+1 613.716.9662
Troy.MacFarlane@tbs-sct.gc.ca

Gartner Contact
James McCabe
Associate Director
Telephone: +1 613.696.0428
James.McCabe@gartner.com

Gartner Contact
Rehan Qureshi
Senior Director
Telephone: +1 416.228.7685
Rehan.Qureshi@gartner.com

Gartner Contact
Chuck Henry
Senior Managing Partner
Telephone: +1 613.696.0408
Chuck.Henry@gartner.com