DGX WORKGROUP ON CLOUD

September 2021

Contents

Introduction 3

Selling the Benefits of Going to Cloud 3

Introduction 3

Singapore's journey 4

Introducing the Cloud Benefits Framework 4

Measuring the Benefits 5

Refining the Cloud Strategy 8

Paying Attention to Change Management 9

Conclusion and Key Takeaways 11

Cloud Baseline Policies 13

Policy 14

Information 14

Outcomes 15

Technology 20

Information 20

Outcomes 20

Capacity 23

Information 23

Outcomes 23

Roles and responsibilities 25

Information 25

Outcomes 25

Procurement 26

There are various approaches of negotiating with CSPs on behalf of agencies and leveraging economies of scale to achieve cost savings and more favorable terms. 26

Information 26

Outcomes 26

Appendix A – Summary of Risks 28

References 12

Introduction

The Digital Government Exchange (DGX) Working Group on Cloud Governance was established in 2020 in response to members' expressed interest in learning about cloud migration. The working group consists of members from Canada, Finland, New Zealand, United Kingdom, World Bank and Singapore (lead).

The working group agreed to share their key learning points from their experience in two practices important to cloud migration: i) Selling the Benefits of Going to Cloud which details the ways to frame the value that cloud migration brings to the government and ii) Data Classification and Baseline Policies which refers to the practices implemented to enable cloud computing and manage risks with cloud adoption. The reports are drafted by GovTech Singapore and the Government of Canada (with input from GovTech Singapore) respectively.

Selling the Benefits of Going to Cloud

Drafted by: Kevin Ng, Ethan Tan, Liyana Fauzi, GovTech Singapore

Introduction

1. Government agencies, like most businesses, are embracing technological innovations to gain the benefits of agility, cost savings and enhanced security. Government agencies need to be adaptive to changing events of the world (e.g., climate change, COVID 19) to tackle immediate day-to-day crisis and critical longer-term horizon effects that need immediate attention.
2. At the same time, we **need to upkeep governance to be cost effective and protect data in the interest of the country.** Traditionally, governments have stringent security requirements, sensitive information that could have national security implications and data breaches that could result in a loss of trust in the institution. As a result, government agencies tended to rely on on-premise data centres or private clouds to protect and have greater control over the data they maintain.
3. Additionally, governments have **specific challenges** that may not be present in private sector use cases. For example:
    a. **Not driven by top-line revenue and profits**
    b. **Need to balance between national security and operational security**
    c. **Even stricter compliance with procurement rules**
4. It creates a dilemma in which the **benefits brought about by cloud technology** are so **impactful** that the governments can no longer take the safest route, as the **benefits of cloud outweigh the risks.**
5. Therefore, we need to be **courageous** in our cloud adoption and yet be mindful to ensure that the **benefits gained from Cloud are commensurate with the required security posture.** To derive the full benefits, government agencies must give **change management** due consideration so that all

agencies within the government can enjoy the benefits of the Cloud while mitigating the trade-offs that come along with migrating to the Cloud.

Singapore's journey

6. In late 2018, the Singapore Government announced a five-year plan to migrate most of its information technology (IT) systems from on-premise infrastructure to the commercial Cloud to speed up the delivery and improve services for citizens and businesses here. In 2019, the Government on Commercial Cloud was established to homogenise the onboarding experience and administrative tasks of agencies on the Cloud, including workload admin, account and billing management, secure access, and compliance to governance policies. In 2020, we set a public target in the Digital Government Blueprint for 70% of eligible government systems to move to Cloud by 2023. To date, the government has almost 600 systems on the Cloud.

Introducing the Cloud Benefits Framework

7. Recently, the Singapore Government conducted a simple study to assess the benefits of the Cloud for systems that have recently migrated over. The study was based on seven Cloud benefits covering qualitative and quantitative measures.

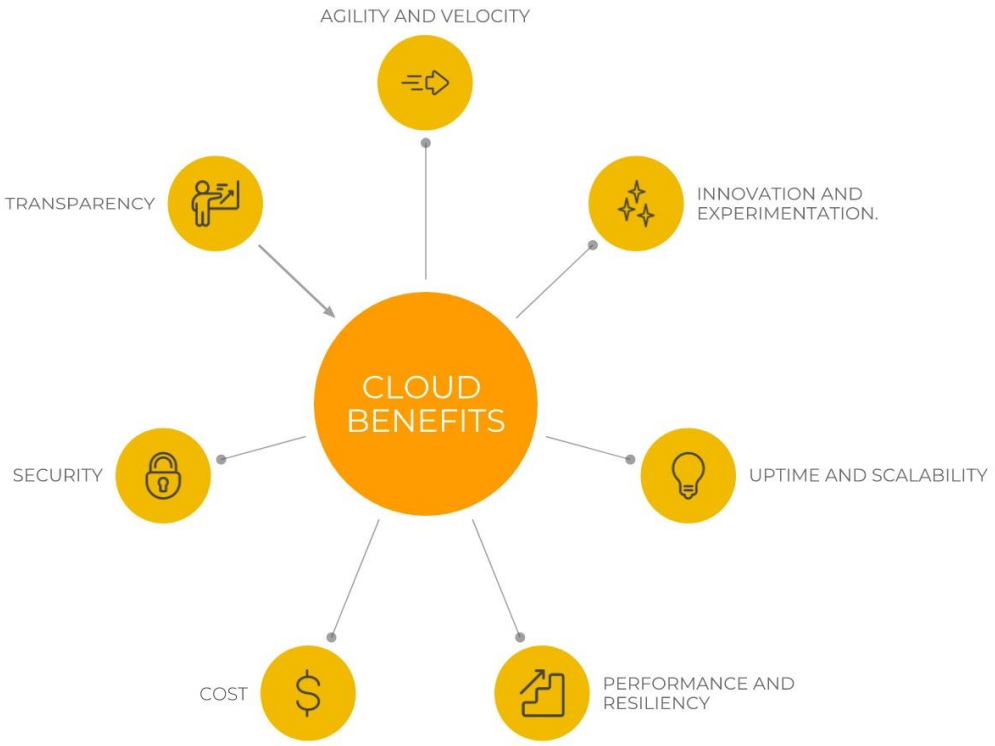

Figure 1: Cloud Benefits Framework

a. **Agility and Velocity**: How fast can an agency respond to business and policy changes by leveraging Cloud-native capabilities? Has the system been able to leverage Agility to leverage digital services for business needs? Is there any use of Cloud for code, microservices deployment, automation in CICD to reduce code and deployment error?
b. **Innovation and Experimentation:** Does the Cloud provide value-added benefits allowing an agency to cultivate development environments and culture to encourage innovation and experimentation? Can solutions be designed innovatively to be Cloud-First where data is stored in the Cloud and accessible across all devices?
c. **Uptime and Scalability:** Are systems able to guarantee more uptime hours on the Cloud? Can systems scale on-demand to meet changing business needs?
d. **Performance and Resiliency:** Are systems more reliable with lesser unplanned downtime?
e. **Cost Savings**: Has migration to the Cloud enabled the agency to save on costs such as operating expenses or manpower costs? In the long-run, does the cost-benefit analysis for Cloud far outweigh on-premise investments?
f. **Transparency**: How has the democratisation of additional information such as utilisation rates enabled decision-makers to save costs?
g. **Security**: How has the change in the security paradigm through Cloud resulted in additional benefits compared to current on-prem solutions? Are there opportunities for zero trust architecture, or using end point protection at the edge?

Measuring the Benefits

8. However, **not all migrations to the Cloud yield the same level of benefits**, as it depends on how such systems take advantage of Cloud-native technology. We simplified to four general migration approaches: **rehost, replatform, replace and redevelop**, akin to what a Cloud service provider has proposed[2].

9. Each of these four approaches supports a specific migration objective, but there is a **corresponding trade-off with the level of benefits realised**. For example, if the aim is to quickly migrate workloads to the Cloud to minimise the reliance on a traditional on-premise data centre infrastructure, the number of resources to fully redevelop the application to take advantage of cloud-native technologies would be prohibitive. For such cases, rehosting the application to cloud-based virtual machines would be the most cost-effective approach. However, as the adoption of cloud technologies is minimal, so would the level of benefits be realised.

Migration Approach	Description	Fit for types of systems	Level of Realised Benefits
Rehost	A lift-and-drop approach, migrating workloads from on-prem to cloud with minimal changes to the application	• Legacy systems that would be redeveloped in the short run • Simple, agency-specific systems that do not require frequent changes	Low
Replatform	Migrate workloads to run on Cloud with some changes to modernise critical components like middleware and/or database	• Legacy systems that are required to operate in the medium term before full redevelopment • Simple, agency-specific systems that do not require frequent changes • Systems in the middle of their life-cycle	Medium
Redevelop	Redevelop apps to take advantage of cloud-based technologies, such as containers and serverless run-time	• Systems that need to fully exploit the capabilities on the Cloud and have more unique needs	High
Replace	Replace with Software-as-a-Service (SaaS), which are licensed on a subscription basis and hosted on Cloud	• Enterprise systems with a high degree of functional commonality and low degree of customisation	Medium-High

10. The different levels of realised benefits for each migration approach were evident in the benefits identified from the following 4 case studies.

<table>
<tr><th rowspan="2">Migration Approach/ Case Study</th><th>Policy Making</th><th>Developer</th><th colspan="2">End-user/Public</th><th colspan="2">Costs</th></tr>
<tr><th>Agility and Velocity</th><th>Innovation & Experimentation</th><th>Uptime and Scalability</th><th>Performance & Resiliency</th><th>Cost Savings</th><th>Transparency</th></tr>
<tr><td>Rehost

(Medium-sized HR system)</td><td rowspan="2">No added benefits to policy-making</td><td rowspan="2">Inability to use cloud-native solutions</td><td>Limited scalability as components are still tightly-coupled</td><td>Better service reliability with no unplanned downtime</td><td rowspan="2">Savings in operating and hosting costs</td><td rowspan="2">No further benefit to cost transparency</td></tr>
<tr><td>Replatform

(Large Manpower Management System)</td><td>Some scalability to meet surges in user demand</td><td>Better service reliability with no unplanned downtime</td></tr>
<tr><td>Redevelop

(Large Grants Portal)</td><td>Faster onboarding of new business processes with faster and more frequent app releases</td><td>Accelerate business processes with reusable microservices</td><td>Ability to self-heal and automatically scale to meet spikes in user demand</td><td>Better service reliability with no downtime to services required for maintaining, patching, and securing VMs with serverless compute</td><td rowspan="2">Savings in operating and hosting costs, as well as business costs</td><td>Savings from optimisation of utilised infra resources</td></tr>
<tr><td>Replace

(Large SaaS Solution)</td><td>Accelerate the streamlining of common corporate processes, and faster</td><td>Utilise new features provided by SaaS provider</td><td>High scalability managed by SLA with SaaS provider</td><td>Better service reliability with no unplanned downtime</td><td>Simplified billing with subscription-based pricing model</td></tr>
</table>

	onboarding time					

Refining the Cloud Strategy

11. The initial cloud strategy was focused more on mass cloud adoption and learning about the cloud as an organisation. During the Covid-19 pandemic, cloud capabilities were put to the test, enabling governments to spin up services to help citizens cope with the pandemic. For Singapore, these included applications such as Trace Together which were check-in solutions for contact tracing in the event of an infection. Without the Cloud, such spin-ups would not have been possible.

12. Based on the initial benefit study and Covid-19 use cases, it is clear that to maximise benefits from cloud migration, it would be ideal for all migrating systems to either (a) be redeveloped to take advantage of cloud-native technologies, modernised architecture, and modernised practices, or (b) adopt SaaS solutions to benefit from common and abstracted functionalities (especially for corporate or enterprise systems).

13. However, due to resource and time constraints, redeveloping or adopting SaaS may not be possible and pragmatic choices should be made:

    - People - Does your organisation have access to a sufficiently large pool of technical specialists that are well-versed in Cloud technologies (whether in-sourced or out-sourced)? Many organisations today lack such expertise as most of their specialists could have been focusing on on-premise deployments.

    - Process - How much time and funding can your organisation allocate towards cloud migration? Legacy systems tend to be complex, requiring a long time and costs to be redeveloped for the Cloud.

    - Platform – Does the organisation have sufficient in-house development capability to warrant a centralised platform for delivering cloud services? If the organisation already has a large in-house development team, it will be more streamlined to create a platform structure to provide internal services so that the development teams can be focused on their applications.

14. A possible shift to the cloud adoption strategy could be to focus on **"Out or Up"**, where an organisation has to choose between moving "out to the cloud" or "up the stack".

15. The first strategy, **"out", prioritises moving systems out to the Cloud**, usually through **rehosting or replatforming**, extracting benefits where possible while achieving economies of scale. This strategy minimises the intensive effort required to redevelop systems and applications while also allowing an organisation to get oriented towards operating a cloud-based model.

16. The second strategy strives to move systems **"up" the tech stack, redeveloping them to utilise cloud-native technologies.** This strategy also increases the agility to innovate faster and respond to rapidly changing business needs. A challenge with this strategy is that it would require more costs and additional technical competency. Another option is to replace systems with SaaS solutions, but this

is contingent on generalising the business needs of the system to find a suitable solution with minimal customisation.

17. One strategy is not better than the other, and **a hybrid model blending both strategies** is the most likely outcome. Differing requirements of systems and their corresponding workloads would determine the optimal approach to realising the full benefits from Cloud migration.

Paying Attention to Change Management

18. Change management is a must for shifting towards Cloud as the journey takes time for the mindset shift of people, not just technology shift of systems[3]; not all stakeholders are privy to the benefits and trade-offs of the Cloud. The average policymaker may not understand the direct linkage of the Cloud in government service delivery. Moving towards the Cloud should be viewed as a key component of digital transformation. Adopting Cloud as new technology will thus require a transformation in people, processes, and technical expertise. Some key components required for Change Management are:

    a) Clarity in Cloud adoption strategy

    It is important for **stakeholders from top to bottom** to understand the value of Cloud adoption, and how they can apply within your government context. There needs to be also the implications from cost and security perspectives. Once the strategy is decided, the **highest level of government leadership needs to buy-in and help set the tone of Cloud adoption.** Specifically, governments can set a policy that requires new systems to adopt Cloud by default, i.e., **Cloud-first policy**. Additionally, there may also be a need to address residual security concerns with the adoption of Cloud, and spell out clearly what is in scope for Cloud adoption, through careful calibration based on risk profiles. For example, governments may consider enabling more systems to be "cloud-eligible", and leaving “non-cloud-eligible” for national security and secret systems.

    The **rank-and-file needs to understand the impetus for change** and be given the **opportunity to create and share the collective future**. It is important to drive the narrative that the benefits of Cloud go beyond cost reduction as a fiscal exercise. There should be a common understanding on purpose that the use of Cloud will contribute to better governance and improvement in government services, benefitting government employees, citizens (and residents) and businesses operating within the governed domain.

    There is a need to review the strategy over time, and make adjustments as the wider organisation learns more based on actual practice.

    b) Collaboration through a centralised cloud adoption team

    To address the initial knowledge gap, governments can consider setting up a **centralised cloud adoption team to advise the independent territories and/or agencies on how to approach cloud migration.** This team can serve as functional experts to facilitate discussions on intended architecture and processes. They should engage the independent territory and/or agencies early,

as IT budgeting and planning can take a long time as they are typically multi-year processes. The centralised cloud adoption team can indirectly help create opportunities for **demand aggregation with key Cloud Service Providers** and this approach provides leverage for **better contractual outcomes**. In addition, standing up a team dedicated to the task gives visibility to the overall cloud adoption efforts across the board, and is much needed to handle such a complex and multi-year undertaking.

There is a need over time to **build up cloud expertise within each independent entity**, so that the centralised cloud adoption team serves to impart knowledge across the larger group, whilst not becoming the "crutch" of the independent entities. The initial collaboration between the centralised cloud adoption team and the independent entity provides the balance between bringing the specialised Cloud knowledge and tapping the local domain specialists, respectively. In the book Team Topologies[4], this centralised cloud adoption team is referred to as the Enabling Team.

c) Collection of experiences and data

As we undertake the effort to migrate to the cloud, it is important to reflect on progress so as to understand what has been achieved, and what can be improved. Both success and failure stories are important to make Cloud adoption a longer-term success. Successful **case studies** need to be understood and could be positioned to help pitch the benefits of the Cloud across all levels of the stakeholders. Anti-patterns from the adoption, particularly collected at the engineering level through service journey mapping, will help guide possible enhancements to both the systems and processes of using the Cloud. Sharing these understandings of case studies and anti-patterns can ensure that independent entities can get well equipped to sustain the Cloud transformation independently over a longer time period.

"What gets measured, gets done". Measuring and tracking Cloud adoption, user experience, system resiliency and benefits quantitatively and consistently will be an evidential scorecard for validating the effort spent on Cloud migration and could serve as evidence that cloud adoption is on track to deliver overall benefits within the government. In addition, setting goals and targets for adoption, user experience and system resiliency will allow for proper tracking of whether progress has been made.

d) Cloud Competency Management

Competency management is important to ensure there is a **sufficient pool of technical specialists** to move towards the Cloud. Besides Government employees, the Government should **consider the larger ecosystem including Cloud Service Provider specialists and vendors,** but due to the talent crunch globally, it may be difficult to source for expertise externally.

Furthermore, with the advent of Cloud, there will be a group of people (such as engineers who have been managing vendors and administering data centres) **who may have their skills atrophied and lost.** Governments should not only consider **reskilling** existing Government

employees but also consider **rotation** for existing employees to create opportunities for them to practice what they learn formally.

It is useful to communicate to the existing employees the skills required to be successful in the Cloud context and support them with robust learning and development plans, complemented with desired competency targets as part of performance management. While there is temptation to hire from outside to augment existing teams, it may be very time-consuming and costly if done at scale, and such external hiring should be more selective to fill niche areas.

e) Cultivation of a Learning Culture

The Cloud technology arena is still at a phase of rapid change in the year of 2021. Hence, both as organisations and individuals, we need to adopt a growth mindset[5]. This mindset requires us to **test fast, learn fast and scale fast**.

Testing faster requires us to set up smaller pilot and shorter time period, also known as **time-boxing**. **Learning faster** requires us to pay attention to both **successes and failures**, and understand why they are successful or not successful, so as to iterate again to refine the learnings. Scaling faster requires us to **take what we have narrowed down as feasible and working and scaling that across the organisation**. These aspects may well be the hardest to achieve within a government context where there is a higher level of regulatory compliance that encourages significant forward planning and larger than usual undertaking, so as to minimize the governance overhead that needs to be applied consistently across all projects. Hence, there is a need to ensure audit, funding, procurement, and security processes are transformed alongside cloud adoption.

Conclusion and Key Takeaways

19. In this paper, we shared three concepts to frame and articulate the value of the Cloud to governmental organisations. First, we introduced a framework consisting of **7 (seven) types of benefits** gained from moving to Cloud. Second, we gave an example of how the **benefit framework** could be applied during cloud adoption based on the **4 (four) migration approaches**. Third, we showed how the initial outcomes can be used to guide the cloud adoption strategy by considering questions in **the 3 (three) strategic areas of people, process, and platform.** Fourth, we addressed the importance and key considerations of **change management** that can make or break cloud adoption programmes.

20. In this framework, several questions will help you identify and reap the most value and benefits from Cloud for your organisation.

- Which benefits are important to you?
- What is your current and optimal mix of migration approaches?
- What are the resources and constraints you have and what are the capabilities you want to grow?

- What change management levers are you able to own and control?

7 Cloud Benefits	4 Migration Approaches	3 Strategic considerations	5 Change Management Levers
• Agility and Velocity • Innovation and experimentation • Uptime and scalability • Resiliency and performance • Cost • Transparency • Security	• Rehost • Replatform • Redevelop • Replace	• People • Process • Platform	• Clarity in Strategy • Collaboration through a Centralised Cloud Adoption team • Collection of Experiences and Data • Competency Management • Cultivation of Learning Culture

References

1. Wikipedia entry on VUCA - https://en.wikipedia.org/wiki/Volatility,_uncertainty,_complexity_and_ambiguity (Retrieved Aug 29, 2021)
2. AWS Documentation Whitepaper - https://docs.aws.amazon.com/whitepapers/latest/aws-migration-whitepaper/the-6-rs-6-application-migration-strategies.html (Retrieve Aug 29, 2021)
3. The Technology Fallacy: How People Are the Real Key to Digital Transformation, Gerald C. Kane, Anh Nguyen Phillips, Jonathan R. Copulsky, Garth R. Andrus (Published in 2019)
4. Team Topologies: Organizing Business And Technology Teams For Fast Flow, Matthew Skelton and Manuel Pais (Published in 2019)
5. Mindset: The New Psychology of Success, Carol Dweck (Published in 2007)

Cloud Baseline Policies

Drafted by: Government of Canada

Cloud computing has introduced a fundamental shift in the way information system services are delivered. Many organizations in both the private sector and public sector are looking to leverage this alternative service delivery model which provides many benefits including service performance, innovation, agility, and elasticity. However, cloud computing also has similar risks to those currently faced in IT, including span of control. In order to manage the risks associated with cloud adoption, it is important to understand the risk scenarios which may exist, both in general and inherent to the cloud, and ensure these risks and cloud specific vulnerabilities were accounted for as the practices continued to evolve.

The ENISA 2009 Cloud Risk Assessment paper groups risk scenarios into the following categories:

1. Policy & Organizational
2. Technical
3. Legal
4. Risks not specific to the cloud (common to on-premise and should be considered carefully when assessing risk of cloud-based systems)

These categories break down further into specific risks, some of which are considered when developing an activity or practice, and is summarized in Appendix A – Summary of Risks.

The Cloud Security Alliance (CSA) examines the risks inherent with cloud security and maintains a list of top threats to cloud computing known as The Egregious Eleven which includes:

1. Data Breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential, access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. Metastructure and applistructure failures
10. Limited cloud usage visibility

11. Abuse and nefarious use of cloud services

To enable the adoption of cloud computing, care must be taken to mitigate risks associated with using cloud services. The following sections below describe the practices implemented by the Government of Canada (GC) to enable cloud computing and manage risks with cloud adoption. These practices include:

1. Policy – Data classification and Cloud baseline policy
2. Technology – Tools and templates to enable secure cloud implementation
3. Capacity – Establishing a Cross-functional Cloud Adoption Team of Experts
4. Roles and Responsibilities – Centralisation and distribution of roles and responsibilities
5. Procurement – Cloud Framework Agreements

Policy and Technology are fundamental requirements for the successful implementation of a secure cloud ecosystem. Capacity management, roles and responsibilities and procurement are all optimizations that will help with the efficient and successful growth and management of the ecosystem.

Policy

The process of applying baseline policies that correspond to the different classifications of data (e.g. classified, restricted, etc.). This includes the details of cloud security configuration, such as "guardrails".

Information

Background including past experiences and operating landscape:
The GC has adopted a "cloud-first" strategy in which cloud is the preferred option for delivering Information Technology (IT) services and public cloud is the preferred option for cloud deployment. As part of this strategy, the GC has implemented an approach to managing security risks in cloud adoption that safeguards Canadians' data and privacy and a series of principles that will guide chief information officers (CIOs) as they adopt cloud services. The GC has also adopted a guardrails approach instead of a traditional governance process which is focused on formal gating. Gating unlike guardrails interrupts the flow of work and impedes progress. Additionally, gating approval and delivery are centralized in a traditional delivery model. These qualities are in opposition to digital delivery of services. A guardrail approach is ideal for cloud as it can be maximized to its full potential. Guardrails allow work to progress smoothly along as it is done within the borders. Guardrail compliance is monitored through automation. Guardrails are aligned to self-service delivery models.
Approach
• Establish cloud direction in the Treasury Board policy framework. • Use governance to determine the correct guardrails

• Determine the best method to monitor guardrail compliance • Assign roles and responsibilities • Continuously increase automation
Challenges and key learning points
• Setting the direction to use cloud as the preferred choice for deploying IT and having oversight of those decisions was a signal to the IT community that IT delivery is shifting, and they must consider new technologies. • Cloud made the movement of data outside of Canada relatively easy. This raised questions around residency and if we should allow data to be stored outside of Canada. Canadians may view the decision to store data outside of Canada negatively and therefor impact the reputation of the government and public service. • Canada did not want to create new compliance verticals that cloud providers must adhere to, but instead leverage existing compliance verticals such as SOC2 and ISO. The Cloud security control profile is tailored from the Government of Canada's security control catalogue found in IT Security Risk Management: A lifecycle Approach ITSG-33 and maps to the controls in ISO and SOC2. • The culture of government is to fall back into gating instead of guardrails. Processes that include gates need to be continuously challenged. The flow of work should be frictionless while maintaining governance requirements. Decisions should stay at the practitioner level.

Outcomes

Ref	Title	Description	References	Risks Addressed
1.	**Cloud First Policy and Architecture Governance**	In 2018 the GC issued a 'cloud first' policy requirement. This policy requires department and agency CIOs to evaluate cloud as their primary deployment model. Furthermore, when CIOs don't use cloud, they must explain that decision at the GC Enterprise Architecture Review Board. Setting the direction to use cloud as the preferred choice for deploying IT and having oversight of those decisions was fundamental to make it clear that there was a need to shift	Directive on Service and Digital – Section 4.4.3.12 Guideline on Service and Digital - Section 4.3	• Loss of governance

Ref	Title	Description	References	Risks Addressed
		the approach and considering new technology was important.		
2.	**Data Residency Policy Requirements**	While moving data outside of Canada has always been a concern, cloud makes it very easy to store data outside of Canada with a few clicks of a mouse. For this reason, the Government of Canada built a data residency policy that favours storing Protected B data in Canada but provides CIOs the ability to evaluate storing data outside of Canada.	Directive on Service and Digital – Section 4.4.3.13 Guideline on Service and Digital - Section 4.4	• Reputational risks • Cloud service failure (availability)
3.	**Data Sovereignty**	The purpose of this paper is to provide an overview of the risk to data sovereignty that is associated with using commercial public cloud environments. The risks to data residency and security are also discussed. These risks are examined in the context of the GC's cloud-first strategy.	Government of Canada White Paper: Data Sovereignty and Public Cloud - Canada.ca	• Reputational risks • Legal risks - Risks from changes of jurisdiction
4.	**Cloud Security Policy**	The purpose of this Security Policy Implementation Notice (SPIN) is to support departments in understanding existing TBS security policy requirements in the context of cloud computing and to set out guidance to assist organizations in the secure use of commercial cloud services (cloud services).	Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) - Canada.ca	• Compliance challenges • Cloud service failure (availability) • Lack of knowledge • Lack of asset categorization

Ref	Title	Description	References	Risks Addressed
		This SPIN applies to Government of Canada (GC) information that has a security category of Protected B for confidentiality, medium integrity and medium availability.		
5.	**Cloud Risk Management Approach and Procedures**	Under the cloud computing paradigm, the GC will depend on vendors for many aspects of security and privacy, and in doing so, will confer a level of trust onto the cloud service provider (CSP). To establish this trust, the GC requires an information system security risk management approach and procedures that are adapted to cloud computing. This document describes the authorities, approach, and procedures for managing security risks to GC services when they are hosted on cloud services provided by commercial service providers.	Government of Canada Cloud Security Risk Management Approach and Procedures - Canada.ca	• Compliance challenges • Cloud service failure (availability) • Technical risks – data leakage, compromise between customer hardening and cloud environment (shared responsibility model) • Legal risks – data protection risks
6.	**Cloud Security Assessment**	This document assists with security assessment and authorization of cloud-based services and includes: • review third-party assurance frameworks. • recommend ways to assess cloud service provider (CSP) controls; • recommend ways to assess your organization's controls;	Guidance on Cloud Security Assessment and Authorization (ITSP.50.105) - Canadian Centre for Cyber Security	• Compliance challenges • Technical risks • Legal risks

Ref	Title	Description	References	Risks Addressed
		• recommend ways to authorize, continuously monitor, and maintain the authorization of cloud-based services; and • provide assessment considerations for security controls.		
7.	**Cloud Security Controls – Baseline Controls**	This document describes the security control profile for cloud-based GC services and related information having a security category of Protected B, medium integrity, and medium availability (PBMM). It specifies the security controls that need to be implemented in these information systems and summarizes the context for which they apply.	Government of Canada Security Control Profile for Cloud-based GC Services - Canada.ca Annex B Cyber Centre MEDIUM Cloud Profile Recommendations of the Guidance on the Security Categorization of Cloud-Based Services (ITSP.50.103)	• Compliance challenges • Cloud service failure (availability) • Technical risks – data leakage, compromise between customer hardening and cloud environment (shared responsibility model) • Legal risks – data protection risks
8.	**Cloud Guardrails – Implementation Guidelines**	The GC has established cloud guardrails which represent a minimum baseline configuration all cloud environments must follow. The policy requirements in the Policy on Government Security and Policy on Service and Digital are operationalized with these guardrails which ensure the security of the cloud tenant environment. Shared Services Canada (SSC) validates that these guardrails are in place, and a process for establishing an	https://github.com/canada-ca/cloud-guardrails https://github.com/canada-ca/cloud-guardrails-O365 GC Cloud Guardrails Escalation Process (Aug_2020)	• Loss of governance –set a minimum baseline for all cloud users • Compliance challenges • Technical risks – data leakage, compromise between customer hardening and cloud environment (shared responsibility model)

Ref	Title	Description	References	Risks Addressed
		automated approach for monitoring cloud environments is underway, to ensure there is no drift from the minimum configuration. In addition, service-specific cloud guardrails for the Microsoft 365 environment were also established, as part of the COVID-19 pandemic response, to enable the rapid, deployment of secure collaboration tools and support departments in accelerating their implementations of Microsoft Office 365. The guardrails are meant to ensure all cloud tenants have a minimum baseline configuration. That minimum is monitored for drift. This allows departments to work autonomously while governance has assurances the policies set are being respected and complied with.		

Technology

The technology refers to the stack of services and functions required to support the business applications and data. The shift from an on-premise model of data centres with pre-defined zones and infrastructure to a new deployment approach with shared responsibilities and shared risks; where the migration of workloads and connection points must be secured.

Information

Background including past experience and operating landscape:
• IaaS puts more configuration and operational burden on organizations. • Each department and agency are at a different point in their cloud journey • Opportunities exist to work as community to build and share common tools in the cloud • Most organizations are in a hybrid IT model where applications are deployed in data centres and cloud services
Approach
• An opinionated landing zone for IaaS environments aligned to the Government of Canada's security control profile • Guidance on technology considerations • Connectivity patterns to help organizations connect cloud services
Challenges and key learning points

• Validation activities
• Ongoing monitoring
• Most departments and agencies are currently in a Hybrid IT model (on-prem and cloud) and use a number of cloud services (AWS, Office 365, Salesforce, etc.…). The GC connection patterns help to reduce the risk of:
  ○ Duplicative effort
  ○ Security
  ○ Compliance
  ○ Lack of speed and agility

Outcomes

Ref.	Title	Description	References	Risks Addressed
1.	**Accelerators**	To help departments and agencies quickly get their cloud tenants up and running while reducing duplication, Infrastructure as Code templates to build out preconfigured landing zones have been built for Azure and AWS.	GitHub - canada-ca/accelerators_accelerateurs-azure: [AZURE] GitHub - aws-samples/aws-secure-environment-accelerator: [AWS]	• Compliance challenges • Cloud service failure (availability) • Technical risks – compromise between customer hardening

Ref.	Title	Description	References	Risks Addressed
		With many departments and agencies deploying landing zones as a first step in their journey to adopt IaaS, creating a template for an infrastructure-as-code landing zone with security controls baked in reduces the time to market as well as reducing duplication.	GitHub - canada-ca/accelerators_accelerateurs-gcp: [GCP]	and cloud environment (shared responsibility model)
2.	**Cryptographic Protection**	The purpose of this document is to help GC departments and agencies use cryptography to protect sensitive GC data in their cloud-based deployments.	Government of Canada Considerations for the Use of Cryptography in Commercial Cloud Services - Canada.ca	• Data protection risks
3.	**Connectivity**	Most departments and agencies are not 100% in the cloud or 100% on-prem. Additionally they must connect data centres, SaaS, and IaaS environments. A set of architectural patterns have been documented to help organizations understand use cases for connecting across cloud services and on-prem data centres.	GC Cloud Connection Patterns	• Network management • Modifying network traffic • Intercepting data in transit
4.	**Vendor Lock-in**	Guidance on Evaluating Technical Lock-in & Exit. IT professionals often resist moving up the technology stack and using cloud-native platform services because they fear lock-in. To help IT professionals navigate weighing the risks associated with lock-in, guidance has been created. As departments will often avoid technologies higher up the technology stack (serverless, PaaS, SaaS) due to fear	Application Modernization Guidance Evaluating Technology	• Lock-in

Ref.	Title	Description	References	Risks Addressed
		of technology and vendor lock-in and often ignore the benefits of reduced time to market and lower operational burden. This guidance is meant to address the following risks: - Lack of modernisation - Status quo - Lead time		
5.	**Workload Migration & Application Modernization**	Under SSC 3.0, the Workload Migration (WLM) Program facilitates the migration of government applications from aging legacy data centres to modern, more secure and reliable solutions – whether cloud, state-of-the-art enterprise data centre (EDC) or a hybrid of the two. The ultimate purpose is to migrate department workloads to reliable, modern, and secure hosting options.	Workload Migration (WLM) Program - wiki (gccollab.ca)	• Data protection risks • Compliance challenges
6.	**Security Playbook for Information System Solutions**	The *Security Playbook for Information System Solutions* document is a "playbook" for federal departments and agencies and outlines a set of security tasks for consideration when designing and implementing solutions for GC information systems in cloud environments.	Security Playbook for Information System Solutions - Canada.ca	• Data protection risks • Compliance challenges • Technical risks – compromise between customer hardening and cloud environment (shared responsibility model)

Capacity

Agencies may not have adequate in-house capabilities and may consider building up multi-functional subject-matter expertise through a virtual team to understand agency needs and provide expertise and advise.

Information

Background including past experiences and operating landscape:
• Our ability to scale our use of cloud is directly proportional to our ability to adopt cloud. Unlearning traditional approaches is challenging. Often an 'on-prem' mentality limits the benefits we experience from cloud.
Approach
• Communities of practice for sharing experiences and failures • Annual events that allow departments to demonstrate their accomplishments and discuss limitations • Online forums for sharing tools, artefacts, and approaches
Challenges and key learning points
• Community building is very challenging and an often-forgotten part of cloud but is an extremely effective tool for growing a community of practitioners.

Outcomes

Ref.	Title	Description	References	Risks Addressed
1.	**Communities of Practice**	To encourage a community of collaboration and sharing, monthly community meetings are held. One at the director/senior management level, the other more technical in nature for delivery teams.	GC Cloud Infocentre - wiki (gccollab.ca)	• Lack of skills • Duplication of efforts
2.	**Events**	An annual event called Stratosphere is held as a platform for Government of Canada IT professionals to share their experiences adopting cloud and devops practices. The first year, it was held as a 1-day in person conference. The second year, due to the pandemic, YouTube was used to broadcast content to IT	Stratosphere2019 - wiki (gccollab.ca) Stratosphere2020 - wiki (gccollab.ca) Stratosphère Cloud - YouTube	• Lack of skills • Duplication of efforts

Ref.	Title	Description	References	Risks Addressed
		professionals. The goal is creating a simple gathering for sharing and demonstrations without vendor driven content.		
3.	**Collaboration forums**	To facilitate sharing amongst IT professionals adopting cloud, a wiki page has been created where relevant documents can be shared. https://wiki.gccollab.ca/cloud allows IT professionals to share tools and processes while rationalizing efforts in the community. Cloud Security artifacts are also made available internally for the GC Community.	GC ESA Artifact Repository - GCpedia (available internally to GC only)	• Lack of skills • Duplication of efforts

Roles and responsibilities

This could mean deciding the roles and responsibilities between the federal government and agencies on cloud adoption. For some, centralised cloud service centres might put together the requirements and configuration, but the agencies might be responsible for the roll-out, adoption and training of staff. We recognize a tension that exists between central planning units and agencies and the complexity of having differing maturity levels of agencies that makes this a critical practice to try and get right at the beginning.

Information

Background including past experience and operating landscape:
Within the Government of Canada, some responsibilities are centralized, for example the Security Operations Centre (SOC). The roles and responsibilities for public cloud have been clearly articulated so that departments understand what roles they must fulfill. This is not the roles and responsibilities between the provider and the consumer, but instead how the consumer roles are divided amongst government organizations.
Approach
• Develop a cloud roles and responsibility matrix
Challenges and key learning points
• Authorities

Outcomes

Ref.	Title	Description	References	Risks Addressed
1.	**Cloud Roles and Responsibilities**	In the shared responsibility model, the CSP is responsible for deploying the security controls under the scope of their responsibility depending on the cloud service model selected. The GC is also responsible for deploying security controls on the GC scope of responsibility. To help ensure a cost-effective and risk-managed use of cloud computing to support program and service delivery, the *GC Cloud Roles and*	Cloud Roles & Responsibilities Cloud Roles & Responsibilities Matrix	• Loss of governance

Ref.	Title	Description	References	Risks Addressed
		Responsibilities document describes the roles and responsibilities of the various GC actors who will be involved in the governance, planning, orchestration, implementation, operations, and maintenance of cloud-based information system services.		

Procurement

There are various approaches of negotiating with CSPs on behalf of agencies and leveraging economies of scale to achieve cost savings and more favorable terms.

Information

Background including past experience and operating landscape:
Shared Services Canada (SSC) has created a procurement broker for cloud services for the GC. SSC has qualified 8 hyperscale cloud providers to host services up to and including Protected B. Departments and agencies are able to buy cloud services from these contracts thus reducing procurement time and standardizing the requirements cloud providers must compete against.
Approach
• Iterative approach – Unclassified (Launched in 2017) to Protected B (Launched in 2019 and replaced Unclassified vehicle)
Challenges and key learning points
• CSP security assessments • There is a need for standard contract clauses – department has procurement authorities, in addition to PSPC and SSC • Complexity of SaaS assessments and procurement

Outcomes

Ref.	Title	Description	References	Risks Addressed
1.	**Cloud Broker Service**	The Government of Canada has invested in creating a procurement broker for cloud services. The contracts created by this group are focused on hyperscale providers. Any department	GC Cloud Broker	• Loss of governance • Cloud provider acquisition • Supply chain failure • Compliance challenges • Poor provider selection

Ref.	Title	Description	References	Risks Addressed
		and agency can access these contracts thereby simplifying the procurement process for departments and shortening the lead time required to get started with cloud. Departments and agencies are able to buy cloud services from these contracts thus reducing procurement time and standardizing the requirements cloud providers must compete against.		• Redundancy • Time to market
2.	**SaaS Acquisitions**	Public Services and Procurement Canada (PSPC) has published a Request for Supply Arrangement (RFSA) for cloud-based Software as a Service (SaaS). The goal is to have these procurement vehicles available to all of Government.	RFSA - SaaS Method of Supply (GC Cloud)	• Loss of governance • Cloud provider acquisition • Supply chain failure • Compliance challenges • Poor provider selection • Redundancy • Time to market

Appendix A – Summary of Risks

The following table is extracted from the *ENISA Cloud Computing Risk Assessment* document.

Category	Risks
Policy and organizational risks	R.1 Lock-in R.2 Loss of governance R.3 Compliance challenges R.4 Loss of business reputation due to co-tenant activities R.5 Cloud service termination or failure R.6 Cloud provider acquisition R.7 Supply chain failure
Technical risks	R.8 Resource exhaustion (under or over provisioning) R.9 Isolation failure R.10 Cloud provider malicious insider - abuse of high privilege roles R.11 Management interface compromise (manipulation, availability of infrastructure) R.12 Intercepting data in transit R.13 Data leakage on up/download, intra-cloud R.14 Insecure or ineffective deletion of data R.15 Distributed denial of service (DDoS) R.16 Economic denial of service (EDOS) R.17 Loss of encryption keys R.18 Undertaking malicious probes or scans R.19 Compromise service engine R.20 Conflicts between customer hardening procedures and cloud environment
Legal risks	R.21 Subpoena and e-discovery R.22 Risk from changes of jurisdiction R.23 Data protection risks R.24 Licensing risks
Risks not specific to the cloud	R.25 Network breaks R.26 Network management (i.e., network congestion / mis-connection / non-optimal use) R.27 Modifying network traffic R.28 Privilege escalation R.29 Social engineering attacks (i.e., impersonation) R.30 Loss or compromise of operational logs R.31 Loss or compromise of security logs (manipulation of forensic investigation) R.32 Backups lost, stolen

	R.33 Unauthorized access to premises (including physical access to machines and other facilities) R.34 Theft of computer equipment R.35 Natural disasters