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

Guidance on Accounting for Cloud Sub-Processors

An Approach to Managed Services & Outcome-based Procurements

February 2021

Document History

Date	Author	Description
Nov 2020	S. Levac	Original drafting in support of collaboration at GC Cloud Procurement Working Group
Jan 2021	S. Levac	Endorsement by GC Cloud Procurement Working Group
Feb 2021	S. Levac	Endorsement at Cloud & Computing Network of Expertise. Feedback to include scenario where provider switches to cloud part way through the contract.

Contents

Purpose

Increasingly scenarios are emerging where suppliers to the Government of Canada use cloud services to deliver their products and services to the GC.

In these scenarios, the GC may have procured business services such as health care insurance or real property management however those services involve technical solutions such as self-service portals or resource management systems that rely on cloud services. Another example is an outcome-based procurement where a desired scope of outcomes is described, and supplier(s) may propose a set of services and products to meet those outcomes some of which may include cloud services. These are a limited number of examples to help illustrate scenarios where the GC does not directly contract with a cloud service provider, however supplier uses cloud service to process sensitive GC data. In each of these scenarios, we refer to the cloud service provider(s) as sub-processors of GC data. One provider using the services of another provider to process or store its data is also known as a fourth-party vendor risk.

Often, whether the suppliers, or prime, uses a cloud service it is not known until bids are received or at contract award. In a worst-case scenario, it is not known until after contract award. Failing to account for cloud services prior to a requirement being tendered, may introduce the risk of procurement processing being delayed or failure. Managed Services procurements may result in one of three scenarios:

1. The managed service provider uses no cloud sub-processors
2. The managed service provider uses one or more cloud sub-processors and all cloud providers have been previously security assessed by the GC
3. The managed service provider uses one or more cloud sub-processors and one or more of the cloud providers have not been previously security assessed by the GC

What is required is an approach for procuring managed services that account for all three scenarios, however the document will focus on scenarios 2 and 3.

This document is meant to describe an approach for taking cloud services into account before, during, and the procurement process. The Canadian Centre for Cyber Security (CCCS) has published Cyber Security Considerations for Contracting With Managed Service Providers which is focused on IT security considerations to a much greater degree covered in this document. This document complements the CCCS document by having a greater focus on the procurement process itself.

Background

In 2016 the Government of Canada published its first GC Cloud Adoption Strategy providing departments clarity that cloud services are part of the GC's IT landscape and can be used to host sensitive information with proper risk mitigation. In 2018, the GC, under the Policy on Digital and Service, published a cloud first requirement making cloud services the preferred model for deploying technology services. While not specifically excluding other scenarios, to date, the GC's efforts have focused on the GC having a direct contracting relationship with the cloud service provider.

Just as the GC has gone cloud first, so has the private sector. Increasingly, the GC's bidders and suppliers are relying on cloud services to help deliver their products and services to the GC.

A cloud service provider is a sub-processor of sensitive GC data for the supplier. This is significant as the security or the sub-processor's people, facilities, and IT systems must all be assessed as complying with our policies and procedures.

Over the past year the GC has witnessed managed service and outcome-based procurements that has experienced significant delays and interruptions because the possibility of cloud sub-processing was not accounted for in the original requirement tendering. These delays cause friction with suppliers and technical authorities.

Definitions

For the purposes of this document, the following definitions are used:

Cloud Service Provider: Highly commoditized, on demand IT services, that can deliver resources such as compute and storage for building business applications all they way to complete business applications. Cloud service providers are the commercial entities that offer those services. Those providers host the IT systems that collect, store, and process the GC's sensitive data.

Managed Service Provider: A supplier to the Government of Canada who offers business or technology services for GC program and service. MSPs are often viewed as outsourcing a line of business under accountability of the GC. MSPs often take on the responsibility of delivering a line of business or a portion of technology delivery. The contractual relationship between the GC and an MSP is typically governed by a Service Level Agreement (SLA). An MSP may use one or more Cloud Service Providers to deliver the technology components of their services such as self-service portals, case management, and analytics. The GC does not hold a direct contractual relationship with the CSP, but instead the GC holds the MSP contractually accountable for the CSP's services. The GC is a consumer of the MSP's services and in-turn the MSP is a consumer of the CSP's services.

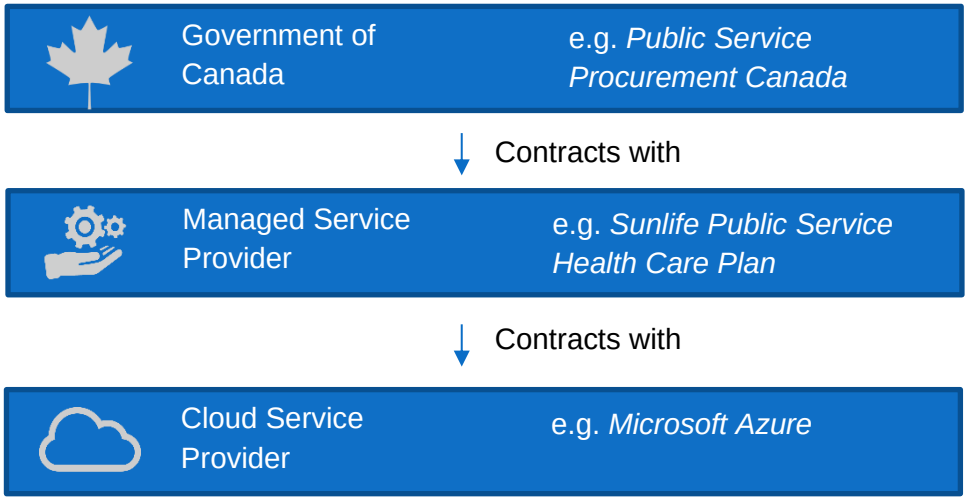


Figure 1: Hierarchy of contracting relationships between providers

Professional Services: A supplier to the Government of Canada who provides services to deploy, implement, and perhaps operate technology and services in a cloud environment. The GC owns a contractual relationship with both the CSP and the professional services provider. The professional

services provider is responsible for augmenting the GC's capacity and capabilities in managing a component of the CSP's service. Accountability for performance issues with the CSP remains with the GC as the professional services provider has no contractual relationship with the CSP.

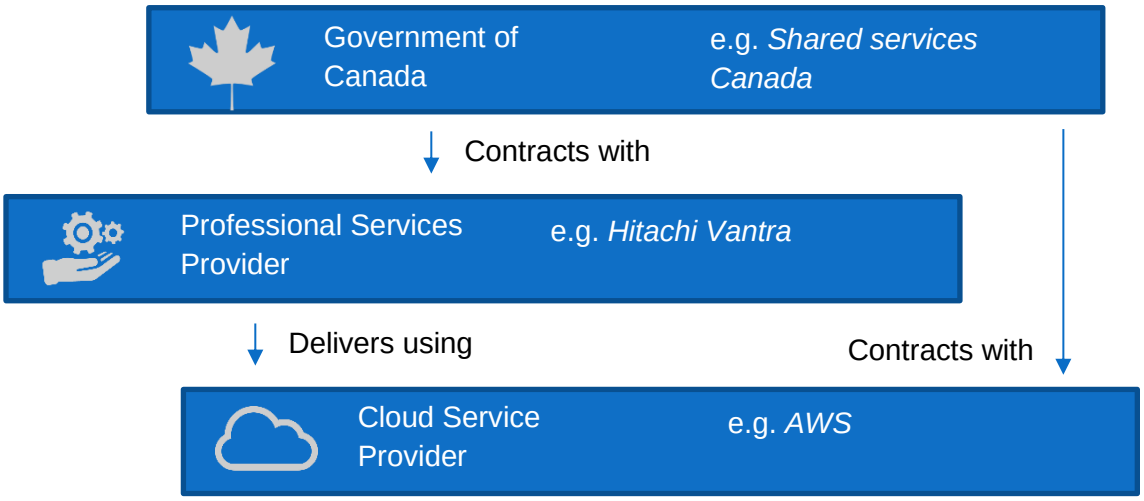


Figure 2: Hierarchy of contracting relationships for a professional services provider

Professional services providers are not covered in this document as the GC maintains a contractual relationship directly with the cloud service provider and are not a sub-processor for the professional services provider.

Outcome-based Procurements

In an outcome-based procurement, the exact solution(s) to be provided may not be known at contract award. Instead, the bidders are responding to a set of desired outcomes to be achieved. This type of procurement may result in products, professional services, managed services, or other delivery models. Outcome-based solutions provide flexibility that the solution set may evolve over time as the user needs and technology environment changes. The suppliers may be cloud service providers, MSPs, and SIs.

Sub-contractor

PSPC states that "a subcontractor with whom a supplier has a direct contractual relationship to perform a portion of the work pursuant to a contract or real property agreement between the supplier and Canada, unless the subcontractor merely supplies commercial-off-the-shelf goods to the supplier"[1]

For the scope of work being performed by the sub-contract, relevant clauses and requirements apply to the sub-contractor. This includes security assessments.

Cloud services are highly commoditized, and the service does not change from one contract to another. Instead, how the prime uses the service may differ. For this reason, CSPs are considered a sub-processor, not a sub-contractor. This does not mean the GC does not assess the security of the cloud security providers, it means these assessments are portable from one contract to another.

Sub-processor

In a managed service or outcome-based procurements where the cloud service provider is not the prime contractor, they are considered a sub-processor. The cloud service must be a commoditized, commercially available, service. It cannot be a service that is tailored or created specifically for the GC. In this sense, a CSP is a utility provider much like a telephony company such as Bell Canada.

A sub-processor may be assessed once by the GC and that assessment can be used across multiple contracts.

Fourth Party Vendor Risk

The risk that exists when a provider outsources or uses the services of another provider to process or store the customer's data. For the purposes of this document, the cloud sub-processor is the fourth party.

[1] https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/4/21/3

Differentiating between SaaS and Managed Services

Because a MSP is often deploying software onto a cloud Infrastructure environment and offering it to a consumer, an MSP and a SaaS can be easily confused. The primary difference between a SaaS and an MSP is in a SaaS, the service is highly commoditized. In a SaaS, many consumers are tenants within the same service. Picture a building where each consumer has an apartment. Each consumer rents a piece of the building. This is analogous to SaaS. No investment was required by the renters for the building to be constructed. They simply begin renting the apartment and when their lease ends, they stop paying rent. In a managed service, although a SaaS sub-processor may be involved, the MSP tailors the offering or combines it with others to create a new offering. Typically, that offering is for one consumer only; the GC.

One must also be aware that some providers will label their managed service as SaaS, managed SaaS, or private SaaS. The nomenclature and marketing alone are not enough to determine if the service offering is a SaaS or managed service. Instead, the table below differentiates some of the attributes of each model.

The difference between a managed service and a SaaS causes different approaches to security, procurement, and they have different risk profiles.

Managed Services	**Software-as-a-Service**
Tailored	Commoditized
Built or highly customized for a consumer	Pre-existing, commercially available, service
Service level agreements can be tailored for the consumer	Service level agreement are pre-established, often publicly available for all consumers
Pricing is tailored to the consumer	Pricing is commercially available, volume discounts available
New features typically result in contract change requests	Innovation and new features require no investment from consumers
Features are determined by contract holder	Feature and product roadmap determined by consumer and market input
Consumers can request that changes, updates, and features be put on-hold	Consumer must move at the pace of innovation
Requires a tailored security assessment approach	Typically hold internationally recognized security certifications such as ISO and SOC
Onboarding may take weeks or months while the provider tailors or builds the service	Onboarding should take minutes. The service is pre-existing.

Assessing the Security Qualifications of the Managed Service

When a managed service includes a cloud provider as a sub-processor, both a security assessment of the MSP and CSP are required, however the approach is different for the two. Also, scenarios can arise where a sub-processor relies on another sub-processor (see Figure 3).

This section is not meant to be a comprehensive overview of assessing the security of an MSP. CCCS has published Cyber Security Considerations for Contracting With Managed Service Providers, providing more comprehensive security guidance. Instead this section is meant to help the reader understand the different approaches than for the MSP versus those of cloud sub-processors.

In the case of an MSP, the IT systems used by the provider must be security assessed in accordance with IT Security Risk Management: A Lifecycle Approach (ITSG-33). If the MSP is using one or more CSPs as sub-processors, then the MSP will use the security assessments of all the CSP(s) as evidence to support the portion of the IT system operated by the CSP(s). When gathering the assessment evidence for the CSP(s) one of two scenarios may arise:

1. The GC has a current and up-to-date assessment of the CSP. Under this scenario, the GC has assessed the security of the CSP and no further assessment is required. A full list of those providers that have been assessed by the GC can be found here https://cloud-broker.canada.ca/s/?language=en_CA

2. The GC has not previously assessed the CSP. Under this scenario, an assessment will need to be conducted aligned to the GC Cloud Tiering Assurance Model.

Assessing the provider's security qualifications can occur during one or more of the following procurement phases:

- *Bid evaluation*. Evaluating security qualifications of the MSP will create a longer evaluation process, but the GC will have certainty of the contractor's qualifications before contract award. A portion or all security assessment activities may take place during bid evaluation.

- *Execution, pre-launch*. After the contract is awarded, but before the service launches, assessment activities can take place. This is particularly useful for outcome-based procurements when the exact nature of the solution is not known during bid evaluation. Additionally, bidders may not want to invest in detailed assessment activities until after the contract is awarded.

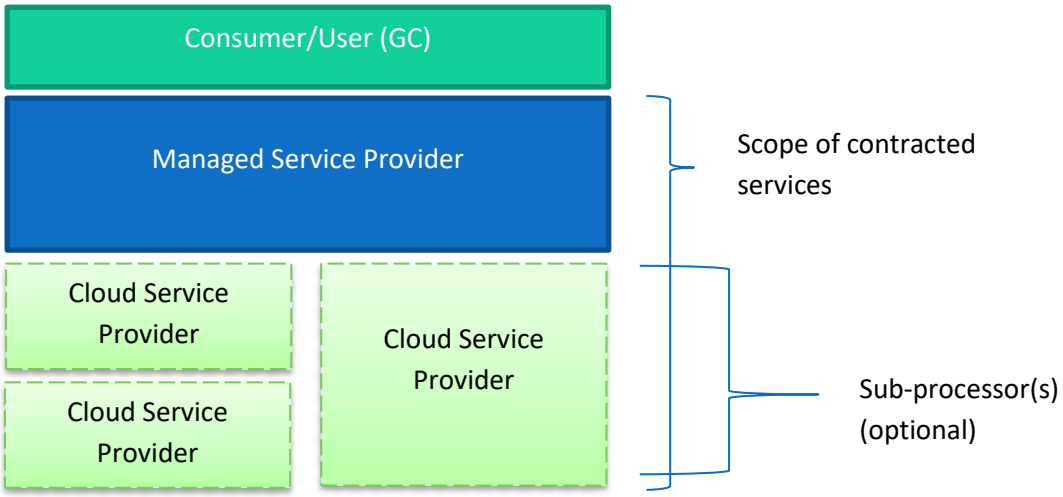


Figure 3: Hierarchy of inherited security and contracting relationships

Assessing the Security Qualifications of Cloud Service Providers

This section is not a comprehensive view of assessing the security of cloud service providers. More comprehensive procedures are available in the Government of Canada Cloud Security Risk Management Approach and Procedures. Instead this section is meant to provide the reader and overview of what cloud providers require to be assessed. Cloud Service Providers, whether when directly contracted, or as sub-processors for managed services or outcome-based suppliers, must undergo security assessments that are related to the categorization of the data they process. A key goal of the GC's assessment of Cloud Service Provider's security qualifications is to assess the provider once based upon the GC Cloud Tiering Assurance Model and not with every contract for which they are a supplier or sub-processor. This is because a Cloud Service Provider's service offering is highly commoditized and does not change with each procurement process. This is a key difference with traditional IT models where the offering often changes with the requirements of each procurement process. A cloud provider only needs to be assessed once (and remain compliant), but apply that assessment across multiple contracts.

Another key element of assessing cloud providers is the use of internationally recognized security certifications such as ISO270017 and SOC 2 as demonstration of meeting the GC's IT security controls.

Assessing a cloud service provider requires that the organization, the personnel, facilities, IT security controls, policies, and procedures must all be assessed.

Departments, through a procurement process, must require that Cloud Service Providers undergo the following security assessments:

	Who Assesses	How are the Requirements Determined?	When is Assessment Performed?
Organizational Screening	PSPC contract security program	Completing SRCL with Classification Guide (sample provided in Appendix B)	Before contract award
Facilities Screening The facilities that store protected data must be screened.	PSPC contract security program	Completing SRCL with Classification Guide (sample provided in Appendix B)	Before contract award
Personnel The personnel who access protected data must be screened.	PSPC contract security program	Completing SRCL with Classification Guide (sample provided in Appendix B)	Before contract award
Cloud Assessment Program	Refer to the GC Cloud Tiering Assurance Model	See Appendix A for template clauses.	Once successful bidder(s) is determined

Approach for accounting for Cloud in procurements

The Approach for accounting or cloud sub-processors is embedded through-out the procurement life-cycle.

Planning

Early planning can help manage expectation for compliance and assessment activities while reducing friction with all stakeholders. Planning for the last day of the contract can also help set requirements to avoid lock-in and transfer of assets, such as data, to facilitate the day after the contract is no longer present. Specific activities should include:

- **Categorize your data.** Knowing the Categorization of your data will drive many downstream decisions for requirements and the scope of stakeholders involved in the procurement process. Outcome-base procurement may serve a broad scope of solutions. If the exact data categorization is not known at the onset, other approaches can be taken. For example, you may want to set a 'high water mark' representing the highest possible data categorization the resulting contract(s) will serve. This however, may exclude bidders and solutions for what may be a small scope of highly sensitive data. Creating tiers where bidders can meet an increasing level of requirements associated with increased sensitivity is another approach. This provides a great level of flexibility, but will likely add complexity to the evaluation process.
- **Reference the GC Cloud Security Tiering** model (link required). The categorization of data combined with the scope of users for the solution will determine the security stakeholders that may need to participate in the procurement process. For enterprise (GC-wide) solutions, CCCS will likely be a stakeholder and their participation will need to be scheduled.
- **Determine Roles and Responsibilities:** Understanding the roles and responsibilities of the provider(s) versus those of the GC is critical to driving security and performance requirements. In a managed service, the provider will be held accountable for the performance and security of the activities within their scope. For outcome-based procurements, the exact roles and

responsibilities of the provider may not be known. In this case, those roles and responsibilities should be articulate when there is a call-up or task authorization for services against the contract.

- **Build a schedule and assemble a team.** With the participation of key stakeholders, build a schedule. The focus on the team's participation should be at the requirements drafting and evaluation phases of the procurement. During drafting, security assessors will need to have a strategy for assessing the security qualifications of the bidders. This will include the participation of the PSPC CISD, CCCS, your department's IT security assessors. Their assessment activities will drive the requirements of the RFP. During the evaluation phases, those same team members will perform their assessment activities. Technical authorities from the business owner will need to state outcomes, service level agreement expectations, and the responsibilities of the provider(s).
- **Plan for the last day of the contract.** In managed services and outcome-based agreements, the provider is often hosting sensitive data on behalf of the GC. At the onset, the GC should understand those assets and articulate how they will be transferred back to the GC or transition them to a new provider at the end of the contract period. Additionally, it should be made clear if the supplier can retain that data or whether they must destroy it.

Requirements Drafting

- **Include clauses accounting for cloud.** At the onset, you may have no idea if the successful bidder(s) will include cloud sub-processors as part of the services or solutions. For this reason, a set of model clauses have been created to account for that possibility. Those clauses can be found in Appendix X.
- **Requirements for articulating roles and responsibilities**. Typically, managed services requirements articulate the role of the provider versus that of the GC, however this is not always the case. Often, the GC seeks flexibility from bidders to suggest the scope of services they can deliver. In this case, as part of the bidder's response, they should be required to describe the responsibilities of the provider, their sub processors, versus those of the GC in the form of a Responsibility, Accountability, Consulted, Informed (RACI) matrix. For outcome-based procurements, this may not be known at contract award, in which case their should be a requirement for the provider to describe the RACI at the time of the task authorization.

Solicitation

In this phase potential bidders respond to the GC's requirements and ask clarifying questions.

Evaluation

The bid evaluation phase provides the evaluation team with a first look at the models, services, and security qualifications of the services being proposed by the provider. The level of detail provided in the bids will depend upon the requirements in the original requirement. There are valid reasons to be more specific in your requirements during the solicitation phase and valid reasons to await to the execution

phase to obtain those details. Asking for more detail in the solicitation phase will drive up each bidders' cost and create a more complex evaluation phase. In outcome-based procurements, the exact nature of the solution(s) being proposed are likely not yet known until the execution phase.

If possible, the evaluation phase should determine:

- Roles and responsibilities of the provider, both MSP and any sub-processors. Knowing the roles and responsibilities of each versus those of the GC will help understand the scope of security assessment required for each.
- Provided the template clauses were used, the bidders should indicate, in their bids, if they use cloud service providers are sub-processors. This will lead to one of the three following possibilities:
    1. No cloud sub-processors. Under this scenario the MSP operates all IT systems and the security assessment procedures outlined in the IT Security Risk Management: A Lifecycle Approach (ITSG-33) can be used.
    2. All cloud providers have been assessed by the GC. Under this scenario, no further assessment activities focused on the sub-processors is necessary. All security assessment activities can be focused on the MSP.
    3. One or more cloud sub-processors have not been assessed by the GC. In this case, both the CSPs without previous assessments and the MSP must be assessed. For the CSP, the GC Cloud Tiering Assurance Model will decide who performs the activities and what activities depending upon the data categorization and scope of users.

Award

For the purposes of this document, no activities have been included

Execution

Once the contract is awarded, the onboarding of the provider can begin. This phase is further divided into two sub-phases. Activities are divided into pre-launch and post-launch activities.

Pre-launch

Before the service launches, the following activities are required:

- Whatever security assessments were not completed during contract evaluation must be completed before the service is launched.

- Establish security incident response process. With multiple stakeholders potentially involved in responding to incidents, having a response plan is key.

Post-launch

After the launch of the service, the following activities should take place:

- Change of sub-processors. If the supplier changes sub-processors, those sub-processors will need to be assessed before implementation of changes take place. Additionally, if the GC
- Continuous compliance. Ensure the suppliers existing sub-processors remain in good standing over time.
- Perform security incident response exercises. Using the previously established incident response plan and using incident scenarios, perform table-top simulations or drills to ensure everyone understands their roles and responsibilities.

Close-out

As the contract closes, ensure the transfer of information assets back to the GC or the new supplier. If required, ensure the supplier disposes of the GC's data.

Changing Service Models Post-Launch

Until this point the document has focused on a linear progression of activities, but what if the managed service provider changes delivery models post-award? If the approach outlined in this document is followed, the requirements should allow for both traditional IT models and cloud models to be used. If the provider wants to change the delivery model or change providers, then the provider will need to comply with the security, privacy, and assessment requirements related to cloud services in the original solicitation.

Guidance Summary

This section is intended to be a high-level overview of the guidance provided in this document.

1. All Managed Service and Outcome-based procurements should account for cloud providers as sub-processors
2. Categorize the data that will be processed by the provider as it will drive critical decisions. Even when the exact scope of data is not known at the onset, it is advisable to chose an upper limit to the data that will be processed by the provider(s).
3. Under the roles and responsibilities of the managed service provider, cloud sub-processors, and the GC in the deliver and management of the service. This will help determine the scope of security assessment for each role.
4. The GC Cloud Tiering Assurance Model will help determine the stakeholders who need to be included in security assessments and will drive the schedule of the critical path.
5. Use the template clauses and requirements in Appendix A to account for cloud service providers as sub-processors
6. While the document does not focus on professional services scenarios, when this scenario occurs, it is preferable to use existing enterprise-wide contracts to provide the cloud services the professional services provider will use.

Appendix A – Template Clauses

Note: clauses taken from PSHCP RFP found here: https://buyandsell.gc.ca/cds/public/2020/08/31/2392d112167c01e82a59483e1e0cb68b/ABES.PROD.PW__XF.B002.E38428.EBSU000.PDF

Pre-launch

Purpose: Requires that, when an MSP uses a cloud sub-processor, the MSP provides the certification assessment reports of the CSP to the GC prior to the service launching.

When should the requirement be met?: pre-launch of service (Service Ready Date)

Protected B, Medium Integrity and Medium Availability for cloud sub-processors (If Applicable)

i. If the Contractor's solution includes one or more cloud-based solution, The Contractor must obtain Project Authority Approval, prior to the Service Ready Date, that the Contractor is in compliance with the security requirements selected in the Government of Canada Cloud Security Risk Management Approach and Procedures.

https://www.canada.ca/en/government/system/digital-government/digitalgovernment-innovations/cloud-services/cloud-security-risk-managementapproach-procedures.html

ii. The Contractor must provide certification or assessment reports. The Contractor must meet the Government of Canada public cloud security requirements for information and services up to Protected B

Threat Monitoring

Purpose: Requires that log information be provided to the GC for threat monitoring purposes. The depth of logs to be provided depends upon the cloud service model being used.

When should the requirement be met?: pre-launch of service (Service Ready Date)

a) For cloud-based environments:

i. The Contractor must allow for application data and associated network traffic to be copied and forwarded to a Government of Canada approved location.

ii. The Contractor must deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for the services at the Contractor's managed host and network layer, for all components managed by the Contractor.

iii. All events and logs for systems supporting the service must be forwarded to a Government of Canada approved system. Alternatively, the Contractor must provide APIs that provide the ability to:

a) Inspect and interrogate data at rest in SaaS applications; and

b) Assess events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access, stored in SaaS application logs.

Continuity Management

Purpose: Ensures that if the MSP must meet priority of service requirements that their cloud sub-processors must also comply with those requirements.

When should the requirement be met?: pre-launch of service (Service Ready Date)

In the event that the Contractor subcontracts or leverages a cloud solution, they must ensure that all dependencies on subcontractor and/or cloud solutions must provide a similar priority of service.

Third-Party Assurance and Certifications

Purpose: Ensures that if the MSP uses cloud service providers as sub-processors, those CSP must maintain valid security certifications through-out the life of the contract.

When should the requirement be met?: Through-out execution until close-out

The Contractor must maintain the following valid and up-to-date industry certifications for the period of the Contract:

a) ISO/IEC 27001:2013 Information technology -- Security techniques – Information security management systems – Requirements; (see https://www.iso.org/standard/54534.html)

b) ISO/IEC 27017:2015 Information technology (see https://www.iso.org/standard/43757.html) -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 (see https://www.iso27001security.com/html/27002.html) for cloud services; and

c) AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, privacy and confidentiality - issued by an independent Certified Public Accountant.

ii. Each certification or audit report provided must:

(i) identify the legal business name of the Contractor or applicable Sub-processor;
(ii) identify the Contractor's or Sub-processor's certification date and the status of that certification;
(iii) identify the services included within the scope of the certification report. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor. iv. Each SOC 2 Type II audit report must have been performed within the 12 months prior to the Operations Ready Date. A bridge letter may be provided to demonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end). v. The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, and SOC 2 Type II for the period of the Contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

Cloud Service Provider (CSP) IT Security Assessment Program

Purpose: If the MSP changes IT deployment model to cloud, the MSP must provide perform the appropriate secure assessment activities and provide the appropriate evidence.

When should the requirement be met?: Through-out execution until close-out

i. If during the period of the Contract and following the approval of the Project Authority, the Contractor migrates the application and/or data from an on premise to a Cloud-based solution, the Contractor must demonstrate that the Cloud Service Provider:

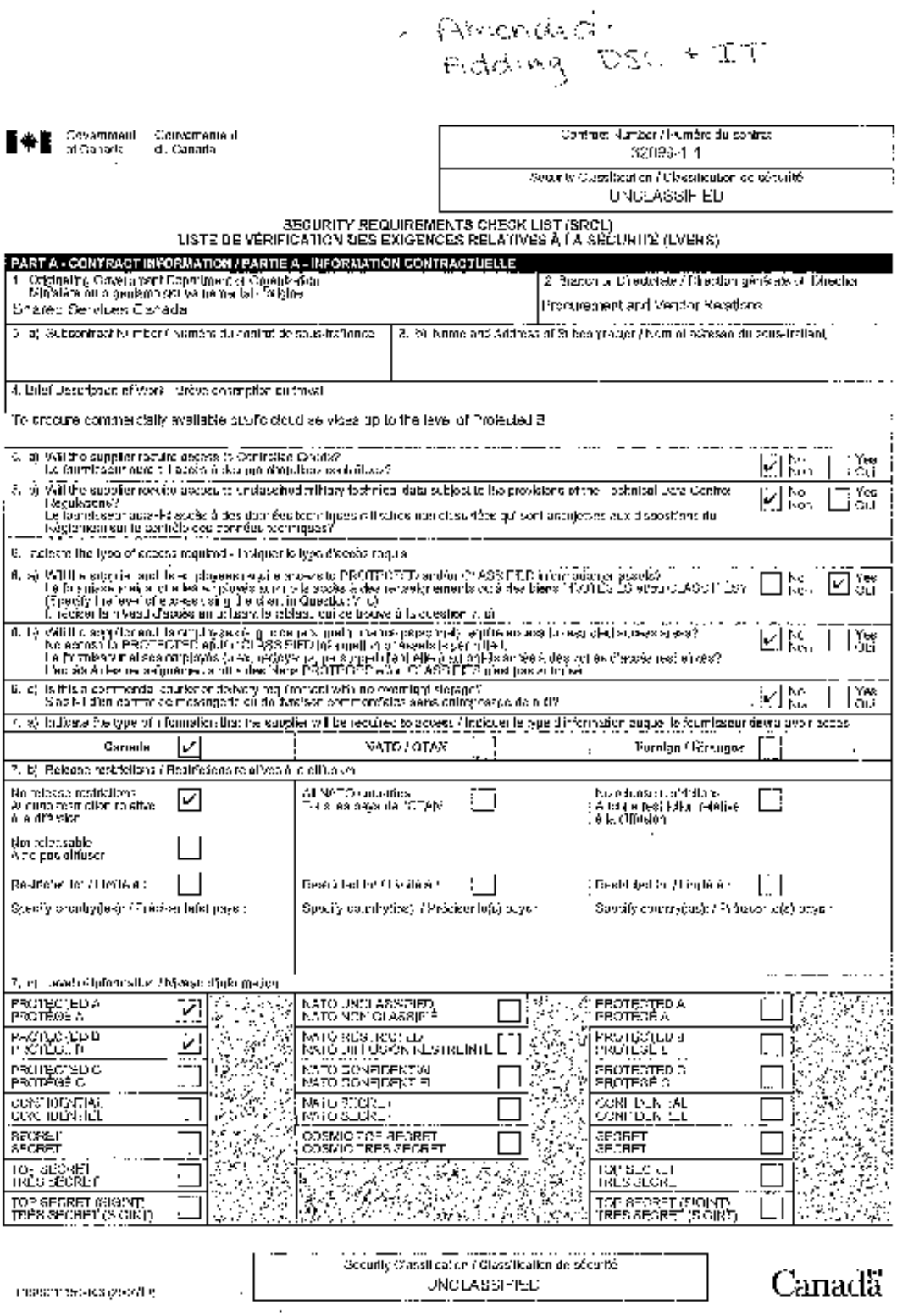
a) Is compliant with the security requirements selected in the Government of Canada Security Control Profile for Cloud-Based Services for GC Services (https://www.canada.ca/en/government/system/digital-government/digitalgovernment-innovations/cloud-services/government-canada-security-controlprofile-cloud-based-it-services.html) for Cloud Services that are leveraged for the solution; and

b) Has been assessed under the Canadian Centre for Cyber Security (CCCS) CSP Information Technology (IT) Security Assessment Process(ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technologysecurity-assessment-process-itsm50100

ii. Any Cloud Service Provider that has participated in the process must provide documentation to confirm that they have completed the onboarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS.

iii. To initiate the on-boarding process, the Cloud Service Provider should contact the CCCS Client Services to receive a copy of the onboarding submission form and any additional information related to the CSP IT Assessment Program.

Appendix B – Sample SRCL and Classification Guide



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
32099-11

Security Classification / Classification de sécurité
UNCLASSIFIED

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine
Shared Services Canada

2. Branch or Directorate / Direction générale ou Direction
Procurement and Vendor Relations

3. a) Subcontract Number / Numéro du contrat de sous-traitance

3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail
To procure commercially available audio cloud services up to the level of Protected B

5. a) Will the supplier require access to Controlled Goods?
Le fournisseur aura-t-il accès à des marchandises contrôlées? — No / Non ☑ Yes / Oui ☐

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?
Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? — No / Non ☑ Yes / Oui ☐

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?
Le fournisseur et ses employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?
(Specify the level of access using the chart in Question 7. c)
(Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) — No / Non ☐ Yes / Oui ☑

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.
Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. — No / Non ☑ Yes / Oui ☐

6. c) Is this a commercial courier or delivery requirement with no overnight storage?
S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? — No / Non ☑ Yes / Oui ☐

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑ | NATO / OTAN ☐ | Foreign / Étranger ☐

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / Ne pas diffuser ☐		
Restricted to / Limité à : ☐	Restricted to / Limité à : ☐	Restricted to / Limité à : ☐
Specify country(ies) / Préciser le(s) pays :	Specify country(ies) / Préciser le(s) pays :	Specify country(ies) / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SCI) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SCI) ☐

Security Classification / Classification de sécurité
UNCLASSIFIED

Canada

Appendix A – Security Classification Guide

The following table outlines the personnel and facility security clearance requirements based on the expected roles and access to GC data.

Table A-1 Security Classification Guide for Commercial Cloud Services

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required[1]	Responsibility	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	Reliability	Contractor	This is for any Contractor personnel including facilities management resources that have physical access to the Cloud Services hardware equipment at the Contractor data centers.
2.	Any Contractor personnel who have logical access to the Contractor services	• All Business Data • Data as stored on the Contractor's compute, storage, and network components	Both	Reliability	Contractor	This is for any Contractor personnel that has logical access to the GC data hosted in the Contractor data centers and any sensitive system and security incident data.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components • Assets include GC data and credentials	Both	Secret	Contractor	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers and any sensitive system and security incident data.
4.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[1] Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

Document history

V0.02 – Nov 2020	Initial drafting based upon working group discussions
V0.03 – Dec 2020	Feedback from OCIO Cyber – added fourth party vendor risk Added explanation of SaaS and managed services
V0.04 – Dec 2020	Feedback from CCCS including • Clarifications on language and explanation • Highlight the need for GC to have NDA with CSP to get ISO and SOC reports • Changed definition of a system integrator to professional services provider • GC Cloud Tiered Assurance Model clarifications • Use of CCCS published controls in lieu of TBS controls