

**Annex A**

**Statement of Requirements (SOR)**

**for Public Cloud Services**

**Table of Contents**

- 1. Government Requirement.....2
- 2. Goals, Objectives & Purpose .....2
- 3. Acts, Policy Instruments and Guidelines .....2

DRAFT

## 1. Government Requirement

Canada has a requirement for commercially available cloud services to meet its business needs across a broad spectrum of government organizations.

Access to these services will be enabled and managed by Shared Services Canada and supported by the Chief Information Officer CIO community in the Government of Canada (GC), to ensure cloud services are consumed across the GC with appropriate levels of governance, security, and technical integration with existing Information Technology (IT) services, and business integration with existing financial and contractual processes.

This approach will greatly reduce the burden on the part of individual government departments and organizations, since a significant percentage of the requirements associated with the use of commercial cloud services will be addressed by the Cloud Service Providers (CSP) and result in GC approved-for-use cloud services offered with facilitated access.

## 2. Goals, Objectives & Purpose

Shared Services Canada (SSC) will enable, consolidate and streamline access to CSP service catalogues for consumption by other government organizations. In order to assist the organizations in delivering and meeting their business needs and services, both internally and Canadian Citizen facing, Canada is seeking the access and delivery of CSP services through online service catalogues.

The goal is to provide access to multiple cloud services for the Government of Canada. These services in accordance with the SOR need to be:

- a. On demand;
- b. Provide rapid elasticity;
- c. Reliant and available 24/7 and 365 days a year;
- d. Secure and compliant;

## 3. Acts, Policy Instruments and Guidelines

The Government of Canada must comply with the following Acts, Policies, Guidelines and instruments:

1. Access to Information Act	<a href="http://laws-lois.justice.gc.ca/eng/acts/A-1/index.html">http://laws-lois.justice.gc.ca/eng/acts/A-1/index.html</a>
2. Official Languages Act	<a href="http://laws.justice.gc.ca/eng/acts/O-3.01/index.html">http://laws.justice.gc.ca/eng/acts/O-3.01/index.html</a>
3. Privacy Act	<a href="http://laws.justice.gc.ca/eng/acts/P-21/index.html">http://laws.justice.gc.ca/eng/acts/P-21/index.html</a>
4. Communications Policy for the Government of Canada	<a href="http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12316">http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12316</a>
5. Policy on Access to Information	<a href="http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453">http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12453</a>
6. Policy on Information Management	<a href="http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742">http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742</a>
7. Standard on Web Accessibility	<a href="http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601">http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601</a>
8. Retention Guidelines for Common Administrative Records of the Government of Canada	<a href="http://www.collectionscanada.gc.ca/government/products-services/007002-3100.2-e.html#a">http://www.collectionscanada.gc.ca/government/products-services/007002-3100.2-e.html#a</a>

9. Standard on Web Usability	<a href="http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&amp;id=24227">http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&amp;id=24227</a>
10. Web Experience Toolkit Guideline	<a href="http://www.tbs-sct.gc.ca/ws-nw/wa-aw/wet-boew/index-eng.asp">http://www.tbs-sct.gc.ca/ws-nw/wa-aw/wet-boew/index-eng.asp</a>
11. Standard on Privacy and Web Analytics	<a href="https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26761&amp;section=text">https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26761&amp;section=text</a>
12. Policy on Acceptable Network and Device Use	<a href="http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122">http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27122</a>
13. Policy on Government of Canada Security	<a href="http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578">http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578</a>
14. CSE ITSG-33 IT Security Risk Management: A Lifecycle Approach	<a href="https://www.cse-cst.gc.ca/en/publication/itsg-33">https://www.cse-cst.gc.ca/en/publication/itsg-33</a>
15. CSE ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada	<a href="https://www.cse-cst.gc.ca/en/node/268/html/15236">https://www.cse-cst.gc.ca/en/node/268/html/15236</a>
16. CSE ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zone	<a href="https://www.cse-cst.gc.ca/en/node/266/html/25034">https://www.cse-cst.gc.ca/en/node/266/html/25034</a>
17. CSE ITSG-31 User Authentication Guidance for IT Systems	<a href="https://www.cse-cst.gc.ca/en/node/267/html/22784">https://www.cse-cst.gc.ca/en/node/267/html/22784</a>

## **Security and Technical Contract Deliverables**

Number	Contract Deliverables
1.	The Contractor must deliver, support, manage and operate a commercially available public cloud services which includes access and the ability to provision from online service catalogues
2.	The Contractor must have commercially available published service level agreements.
3.	The Contractor must provide the GC a master account and the ability to create sub-accounts for GC customer departments to enable provisioning and use of public cloud services and access to public online service catalogues
4.	The Contractor must alert and notify the GC Technical Authority via phone and email (7 days x 24 hours x 365 days), based on priority as specified by GC, of detected suspicious events or unusual activities with security implications
5.	The Contractor must report, within the Contractor published SLA timeframe, any suspected or actual Security incidents, including but not limited to: a) denial of service attacks; b) malware; c) social engineering; d) unauthorized intrusion or access; e) information breach; and f) all other security breaches or cyber threats targeting Canada or has an impact on GC cloud service (e.g. Contractor insider threats).
6.	The Contractor must provide all evidence, including logs and audit records, associated with a Security Incident, within 1 hour of an incident , or as specified by the GC.
7.	The Contractor provider must work with Canada's IT Security Incident Recovery Team (ITSIRT) on Security Incident containment, eradication and recovery.
8.	The Contractor must implement an audit and investigation process that: a) allows only specific, pre-authorized representatives of Canada (e.g. SSC IT-Security Incident Response Team (IT-SIRT)) to request and receive discrete access and information associated with GC Data (user data, event logs, content) for the purposes of conducting investigations; b) does not disclose such access to end users; and c) is approved by GC
9.	The Contractor must scan all GC cloud service data, for the presence of malware. There should be an active host-protection mechanisms on servers that are actively scanning malware on a weekly basis.

10.	<p>The Contractor must provide an automated technical solution (for example, a web-application firewall) in front of public-facing web applications that continually checks all traffic to that continually detects and prevents web-based attacks (e.g. injection flaws, buffer overflows, cross-site scripting, etc.).</p>
11.	<p>The Contractor must ensure that the integrity of GC Data is protected using cryptographic solutions unless otherwise protected by alternative mechanisms approved by the GC. Integrity of GC data must be maintained to prevent and detect improper alteration, duplications, or destruction (e.g. double keying, message authentication, digital signature, check sums etc.).</p> <p>This includes:</p> <ul style="list-style-type: none"> <li>a) protecting data transmitted between solution components and between authorized systems to ensure that information is intact and that it has not been changed in transit, either due to malicious intent or by accident; and</li> <li>b) providing the capability to perform source to destination file integrity checks for exchange of data and alert appropriate parties when an error condition occurs (either with a specific message or with systems components).</li> </ul>
12.	<p>The Contractor must ensure that any cryptography used to implement confidentiality or integrity safeguards or as part of authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for the cloud service is configured for use with GC approved cryptographic algorithms and cryptographic key sizes and crypto periods.</p> <p>This includes, but is not limited to:</p> <ul style="list-style-type: none"> <li>a) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSE and validated by the Cryptographic Algorithm Validation Program (<a href="http://csrc.nist.gov/groups/STM/cavp/">http://csrc.nist.gov/groups/STM/cavp/</a>), and are specified in ITSB-111 (<a href="https://www.cse-cst.gc.ca/en/node/1428/html/25015">https://www.cse-cst.gc.ca/en/node/1428/html/25015</a>) or in a subsequent version;</li> <li>b) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (<a href="http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-eng.html">http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-eng.html</a>) to at least FIPS 140-2 validation at Level 1, and</li> <li>c) operate in FIPS Approved Mode of Operation.</li> </ul> <p>The Federal Information Processing Standard (FIPS) 140-2 specifies the security requirements that must be satisfied by a cryptographic module utilized within a security system, sub-system, or component protecting protected information. Prior to using any cryptographic module, the CSP shall provide a copy of the relevant FIPS 140-2 validation certificate as evidence of FIPS 140-2 validation, or, as a minimum, the validation certificate number.</p>
13.	<p>The Contractor cloud solution must support Security Assertion Markup Language 2.0 (SAML 2.0).</p>
14.	<p>The Contractor must provide the capability to implement public key certificates that have been issued under a GC-approved certificate policy or from a GC-approved certificate authority. These certificates must be validated prior to each use.</p>

15.	The Contractor must provide the ability to secure and encrypt communication channels that are used when migrating physical servers, applications, or data to virtualized servers.
16.	<p>The Contractor must provide a list of the data centre city and province/state locations that will be used to provide the services included in this contract. For data centres outside of North America, a list of all the countries in which the data centres are located will suffice.</p> <p>a) For each data centre location, list the tier classification using the tier classification system of the U.S. based Uptime Institute, LLC or its affiliate as referenced at <a href="https://uptimeinstitute.com/">https://uptimeinstitute.com/</a> or any other industry standard to which the data centres conform that the Contractor uses to classify each data centre's availability or site infrastructure performance. Contractor is required to provide evidence of such tier or other independent certification.</p>
17.	The Contractor must provide and maintain the information system documentation and include any changes to the information system/environment of operation or problems identified during plan implementation or security control assessments on an annual basis
18.	The Contractor must provide a list of their personnel, identified by name and role, with system administration, monitoring, and/or security responsibilities that are to receive security alerts, advisories, and directives. This list shall include GC Technical Authority and other GC-approved and specified personnel.



## 1. Concept of Operations

### 1.1. Purpose

This Concept of Operations (CONOPS) is intended to ensure that the public cloud is deployed and operated consistent with established cloud standards, thus contributing to effective risk management and the achievement of a balanced security, enrollment and support posture. This document also provides the vision of “how” the new service should work and under what operational conditions.

The public cloud project was initiated to offer a central procurement authority and provide government departments with a sanctioned procurement method of consuming cloud services. In addition, cloud services provide SSC a method of providing computing capacity required to meet demand, acquired through “pay for use” financial models – similar to models for consumption of traditional utilities like water, electricity, gas and telephony. This allows governments to move from a Capital Expense (CAPEX) to an Operational Expense (OPEX) model as they do not need to invest in significant infrastructure, professional services and support.

This document will evolve over the life of the project. Version 1.0 is intended to coincide with the completion of the requirements period gathering.

### 1.2. Objectives

The objective of the *SSC Cloud Enablement Program* is to execute on the GC Cloud Adoption Strategy by establishing the GC Cloud Service Broker (CSB) Service and cloud procurement vehicles for self-serve provisioning of cloud resources by customers\*.

The immediate objectives of the Cloud Enablement Program are as follows:

1. Establish the new GC Cloud Broker Business Line in SSC
2. Architect and Implement the capabilities of the GC CSB
3. Establish procurement vehicles for Cloud consumption
4. Provide a cost effective, easier, secure and more productive means for the GC to navigate, integrate, consume and extend cloud services

### 1.3. Assess Sensitivity of Data

**Who:** Departmental business /program owners, Departmental project authorities, CIO staffs, or any departmental body with the mandate to provide IT capabilities to departmental business owners.

**What:** The objective of this activity is to determine the security categories of the selected business activities that are to be outsourced to a cloud service provider. It is assumed at this point, that the sponsoring department or agency has identified which business functions are in scope and intended to be executed in a cloud environment. Once these business activities and related information are identified, a security category will express the highest levels of expected injuries from threat compromise with respect to the security objectives of confidentiality, integrity, and availability.

**When:** The identification of the security categorization of the business activity is required in order to confirm which Cloud deployment model is applicable to the outsourcing of the business activity in question, and which security controls will apply in the form of a security control profile. This activity should happen early during the SDLC process followed by departments and agencies, and is critical to the appropriate procurement and deployment of the right cloud capabilities and deployment models within the GC Cloud Adoption strategy.

**How:** Through the sub-activities identified below, and by using the security categorization tool (link provided). The tool is meant to capture the information produced during the sub-activities above, allows for a standardized methodology to capture the information on processes and information types, define injury levels and extrapolate a high water mark rating of injury in the confidentiality, integrity, and availability security dimensions as it applies to a business process or service that is planned for implementation in a cloud environment.

#### 1.4. Identify Business Processes and Related Information Assets

There are several sources from which to identify and describe business processes and related information assets, which can include:

- Business cases;
- Concepts of operations (CONOPS);
- Business functional specifications;
- Enterprise architecture documentation which typically describes an organization's business processes and related information assets in some detail;
- Discussions or interviews with business analysts and other individuals within related business communities; and
- TBS's Government of Canada Strategic Reference Model (GSRM) Service Reference Patterns may also be useful in identifying and describing business processes.

#### 1.5. Assess Injuries from Threat Compromise

Ideally, departments assess injury for their business processes and related information assets through a departmental process using multidisciplinary teams that include representatives from business, legal, access to information, and privacy areas.

#### 1.6. Determine Security Category of Business Activity

A business activity may involve one type of information with an assessed injury level of low for confidentiality and another type of information with an assessed injury level of medium for the same security objective (both for non-national interest). These individual values are important and should be documented. However, the security category of the business activity should reflect the highest level of injury.

The output of this step is the security category of the business activity, which can be expressed using the same marking format as for individual business processes and information.

**Concept of High Water Mark.** Determining the security category of business functions to be supported by cloud information system requires the business owner to consider the security categories of all information types which will be processed or stored in the cloud. For an information system, the potential injury level values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the cloud information system.

### 1.7. Determine Security Category Statement

A security categorization statement should include:

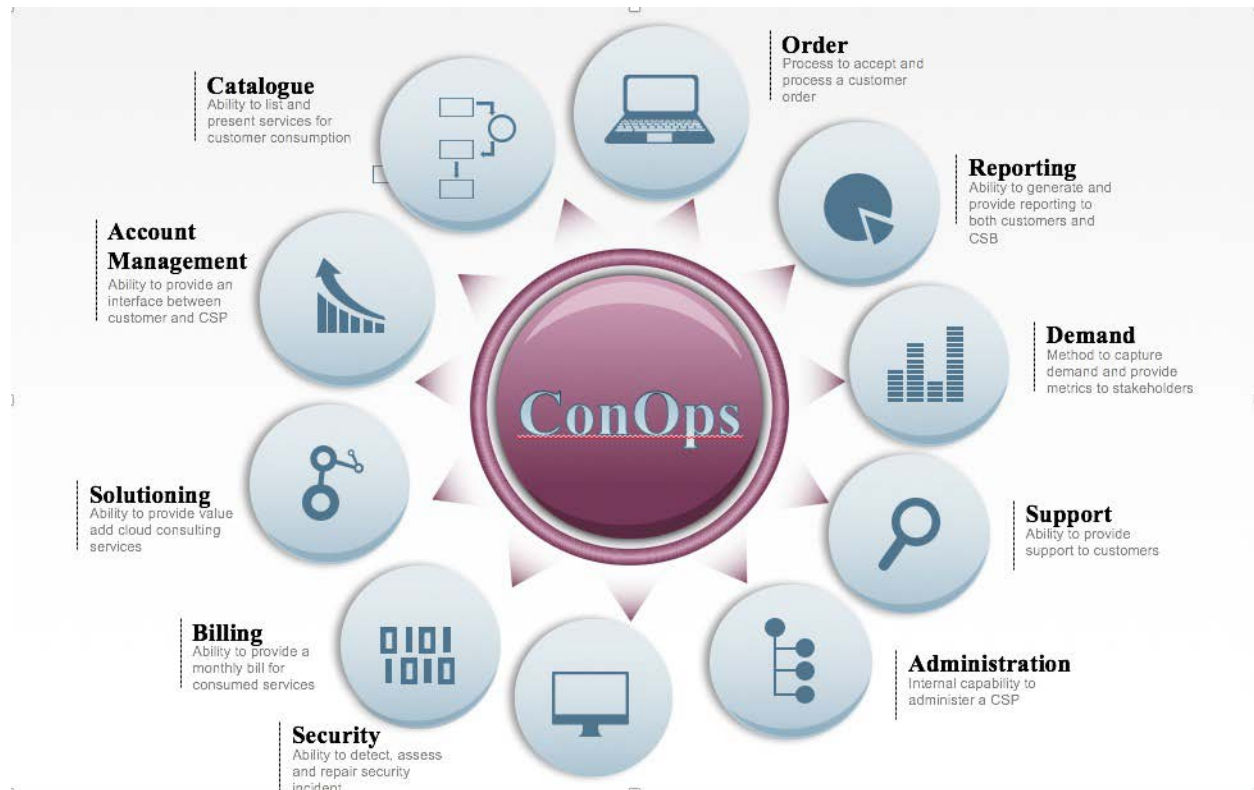
- A short description of the business requirement being hosted in the cloud offering, the process(es) being effected through this medium, and the information being exchanged;
- A description of the expected injuries from threat compromise;
- The levels of expected injury as they relate to confidentiality, integrity, and availability; and
- The rationale for attributing the levels of injury
- An explicit statement of acceptance from stakeholders of the assessed security categorization for the business process (es) to be outsourced to CSPs.

The security categorization statement is produced once security categorization activities have been completed to the satisfaction of the project team and supporting security practitioners.

### 1.8. Workflows









The following information is intended to describe the various workflows of the cloud enablement program. Roles and responsibilities will be detailed followed by fundamental processes core to the operation of the program.

The following processes will be described:



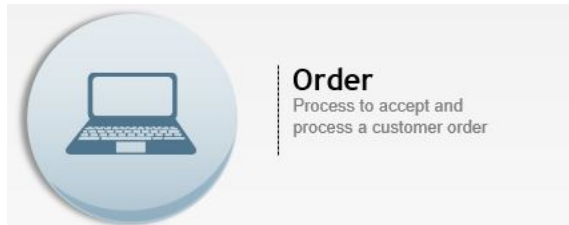
#### 1.8.1. Roles and Responsibilities

The following table defines the roles and responsibilities of each party as it pertains to the attached work flows.

Role	Description	Responsibility
 Customer	The Client refers to any government department or entity who procures cloud services through SSC's contracting vehicle.	The Client is responsible for preparing the cloud service request, seeking Chief Information Officer (CIO) and Chief Financial Officer (CFO) approval and provisioning any sub accounts they require.
 Customer CIO/CFO	SSC will require CIO and CFO approval prior to provisioning cloud services.	The CIO and CFO will approve their departments cloud request.
 Cloud Service Provider	The Cloud Service Provider refers to the CSP that the customer has selected.	The CSP will provide services in accordance with the customer selected service from the CSP catalogue.
 SSC CSB	The SSC Cloud Enablement Program refers to the internal business unit responsible for running the Cloud Enablement Program at SSC. The Technical Authority of the cloud program provides an interface into SSC.	The SSC Cloud Enablement Program and Technical Authority will manage customers, work with procurement, interface with CSPs and other stakeholders where required.
 CSB Admin	The CSP Administrator is a role in the SSC cloud enablement program.	The CSP Administrator will manage customer accounts, provide technical and admin support and provision customers when required.
 SSC PVR	SSC Procurement is SSC's internal procurement organization.	SSC Procurement is responsible for handling all procurement related activities.
 SSC SOC	The SSC SOC is the Security Operations Center.	The SOC will be responsible for handling security incidents and instigating internal processes and procedures until resolution. They will interface with any relevant stakeholders including the CSP.
 SSC NOC	The SSC NOC is the Network Operations Center.	The NOC will be responsible for network related requests and incidents. The NOC will ensure basic connectivity is in place between customers and the CSP. They may also be involved in security incidents.

### 1.8.2. Order

SSC has developed an Order workflow that addresses the onboarding of customers into the cloud enablement program. This model will be executed when a customer identifies a requirement for a particular CSP:



**Owner:** Marc Contois

**Tools:** Tracking Form (Needs to be Developed to capture Order Information), Business Case (Hosted), Email, Demand Management Document, Order Form (PVR)

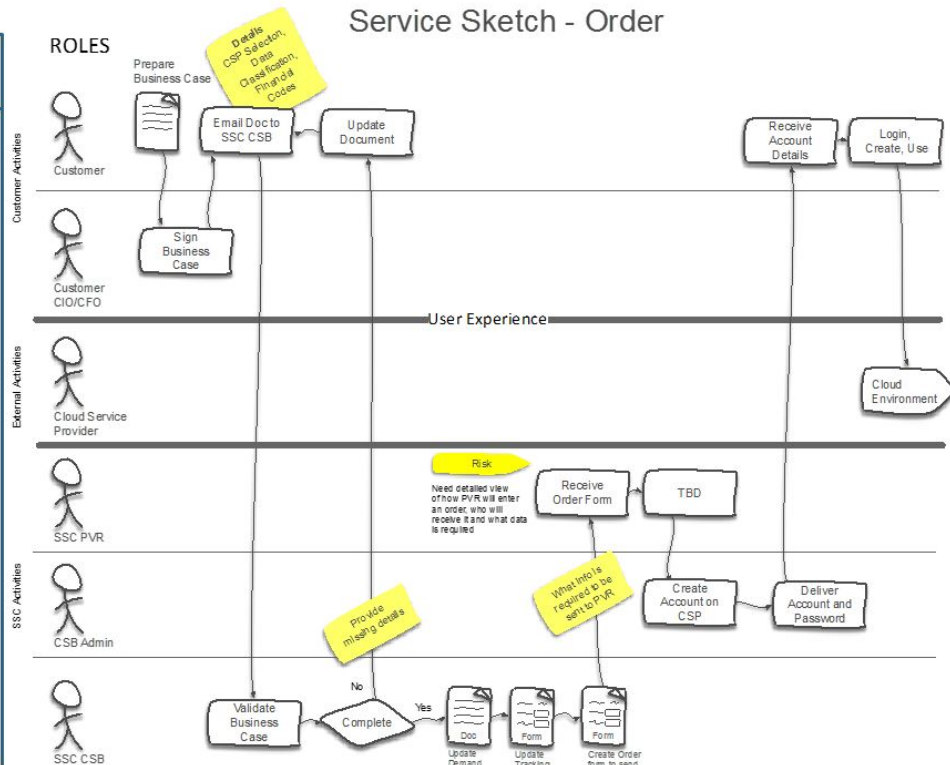
**Service Level Agreement:** Upon order receipt, the order will be acted upon within 2 business days and sent to PVR for fulfillment.

**Frequency of Process:** On demand when Order is submitted

**Process Description:**

1. Receive Business case from customer via email to CSB;
2. The CSB will review the submission, verify CIO/CFO signoff, verify financials and data classification;
3. If the business case is missing information it will be sent back to the customer for completion;
4. The CSB will enter all relevant information into the demand management excel spreadsheet;
5. The CSB will enter the order information into an Order Form and send to PVR;
6. An order will be sent to PVR with customer details, services ordered, financial codes and cost centers;
7. PVR will process the order then notify the CSB that account creation can commence;
8. A CSB administrator will create a new account in the CSP environment, set the password and communicate login credentials to the customer;
9. The customer can login and create their environment.

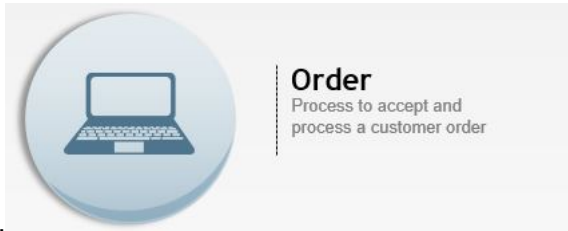
- Assumptions**
- 1) Customer has completed business case;
  - 2) Customer has sufficient network capacity;
  - 3) Customer is low touch;
  - 4) Customer has selected Cloud Service Provider;
  - 5) Customer has selected services from CSP catalog.



The SSC Technical Authority will evaluate the request and verify the information in the request. Once all information has been verified, the SSC Technical Authority will send the request to SSC Procurement. SSC Procurement manages the cloud contract and will evaluate the request. If the request is for access to a new CSP for that customer, procurement will validate sufficient room is left on the vehicle and will issue a call up against the contract for the value requested by the customer. Once this is complete, SSC procurement will notify the CSP of the new business. The SSC CSP administrator will be notified and proceed to create a customer account on the selected CSP. These credentials will then be delivered to the customer who can then proceed to use the cloud service.

If procurement receives a request for a customer to purchase additional cloud services with a CSP where they already have an existing account, the 'Buy' process in the next section will be utilized.

### 1.8.3. Service Cancellation



**Owner:** Marc Contois

**Tool:** Cancellation Tracking form

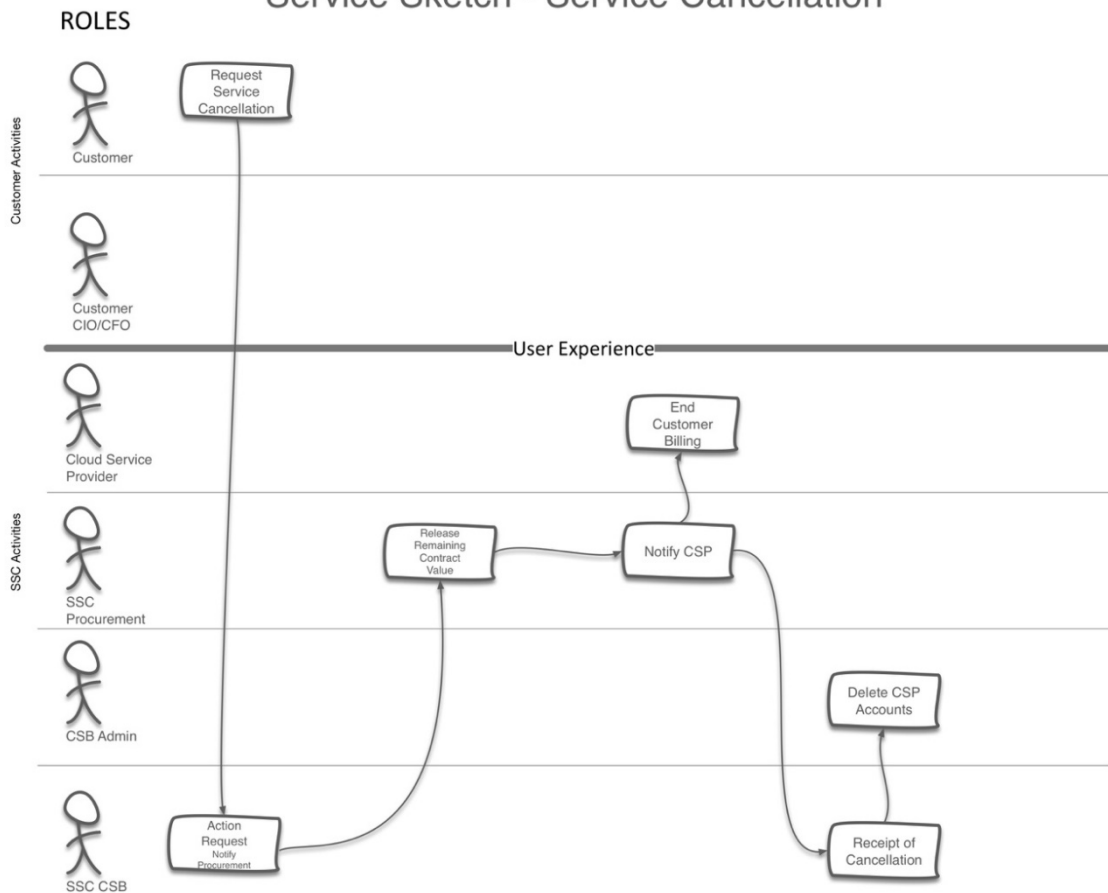
**Service Level Agreement:** TBD

**Frequency of Process:** On Demand.

**Process Description:**

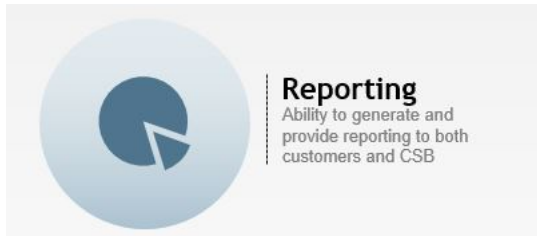
1. Customer will notify the Cloud CSB that they wish to terminate their service with a particular CSP.
2. The Cloud CSB will notify SSC Procurement.
3. Procurement will release the contract value and inform the CSP that the customer engagement is complete.
4. Procurement will notify the CSB.
5. The CSB will then provide the CSB Admin accounts to delete.

### Service Sketch - Service Cancellation



Customers who choose to cancel their service with a cloud service provider will first notify the SSC Technical Authority in writing of their intention to discontinue service. The SSC Technical Authority will notify SSC Procurement of the final day of service. SSC Technical Authority will terminate the customer account and release any remaining contract value back to the vehicle. Additionally, SSC Procurement will notify the Cloud Service Provider of service cancellation ensuring no further billing takes place. Procurement will provide a written confirmation of successful service termination to the SSC Technical Authority who will then log into the CSP and delete the sub level accounts on behalf of the customer

### 1.8.4. Reporting



**Owner:** Marc Contois

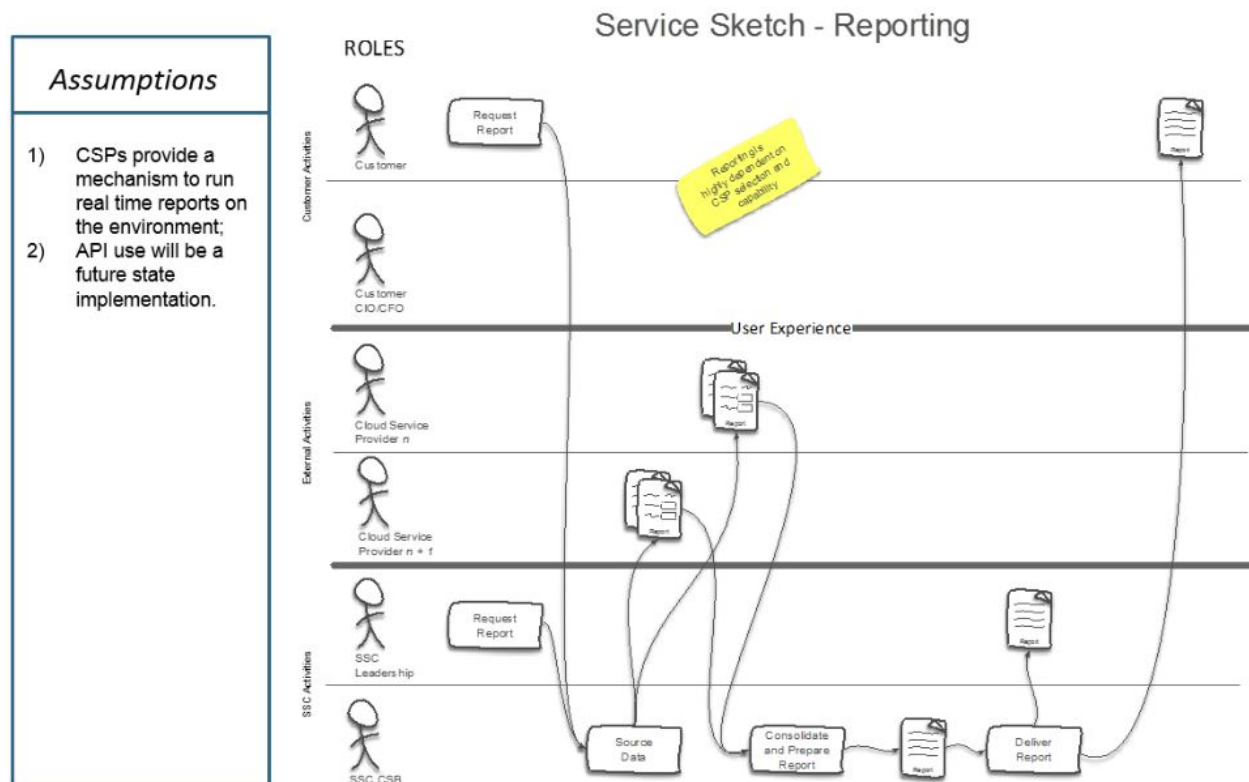
**Tool:** CSP Dashboard, CSP API, Excel

**Service Level Agreement:** The CSB will require the capability to provide reporting on a variety of metrics within 2 days of request.

**Frequency of Process:** On demand

**Process Description:**

1. A request for reporting will be sent to the CSB;
2. The CSB will log onto the CSP dashboard and generate reports;
3. Custom reports with multiple data sources will be prepared in Excel;
4. The CSB will prepare the requested report and deliver to the requester.





1.8.5. Demand



**Owner:** Marc Contois

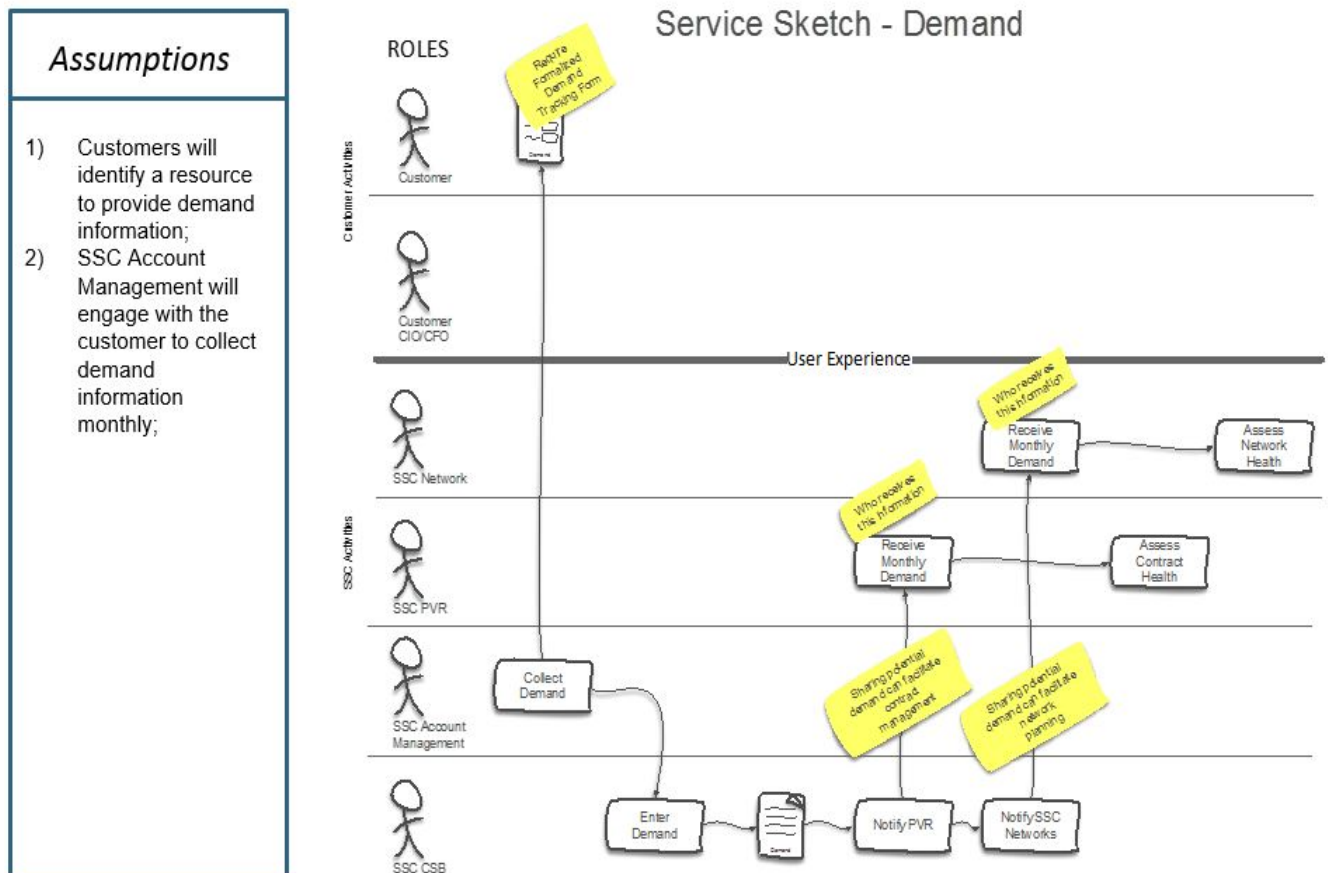
**Tool:** Customer Demand Template, Rollup Demand Template

**Service Level Agreement:** Demand will be sent monthly to PVR and SSC Networking

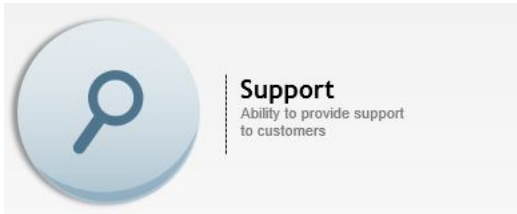
**Frequency of Process:** Per Order, Monthly

**Process Description:**

1. SSC Account Managers will provide a demand survey monthly to customers;
2. A form will be sent to a customer to anticipate spend and cloud service vendor selection;
3. The information will be sent to SSC CSB to collect and collate;
4. Information will be entered into a master demand template;
5. Each month a summary of demand will be sent to PVR and SSC Networks;
6. Analysis will be performed by PVR and Networks to facilitate contract management and network demand.



1.8.6. Support



**Owner:** Marc Contois

**Tool:** Service Desk Ticket System

**Service Level Agreement:** Tickets will be resolved in 24 hours

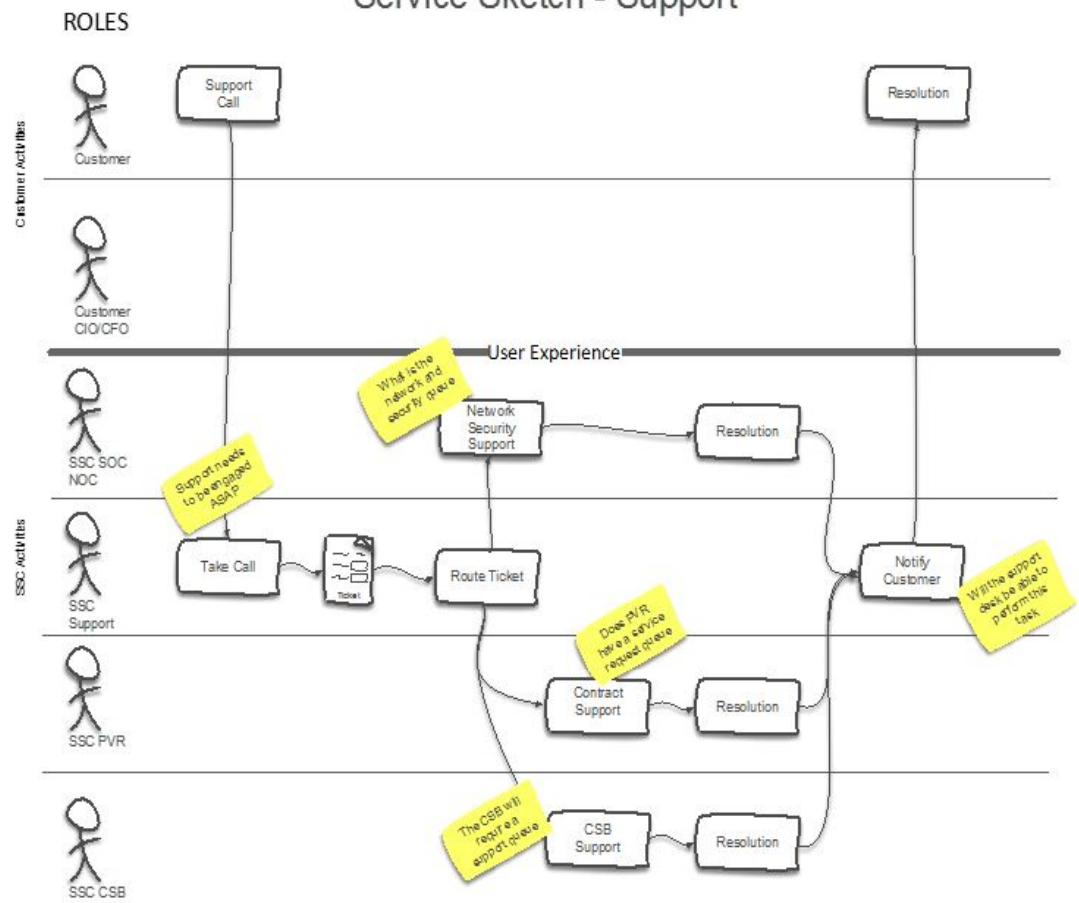
**Frequency of Process:** On Demand

**Process Description:**

1. Customer will place a service request with the SSC Service Desk;
2. The agent will evaluate the call and forward to either the network organization, security organization, PVR or the CSB.
3. The ticket will be evaluated, acted upon and resolved.
4. The agent will forward the ticket back to the service desk to notify the customer of resolution.

<i>Assumptions</i>
1) SSC Support organization will create a queue for the CSB; 2) Front line support will take support calls and route to the appropriate destination; 3) Front line support will notify the customer of resolution.

Service Sketch - Support



1.8.7. Administration



**Owner:** Marc Contois

**Tool:** CSP Admin Dashboard, Work Order Form for Admin, Form for Customer

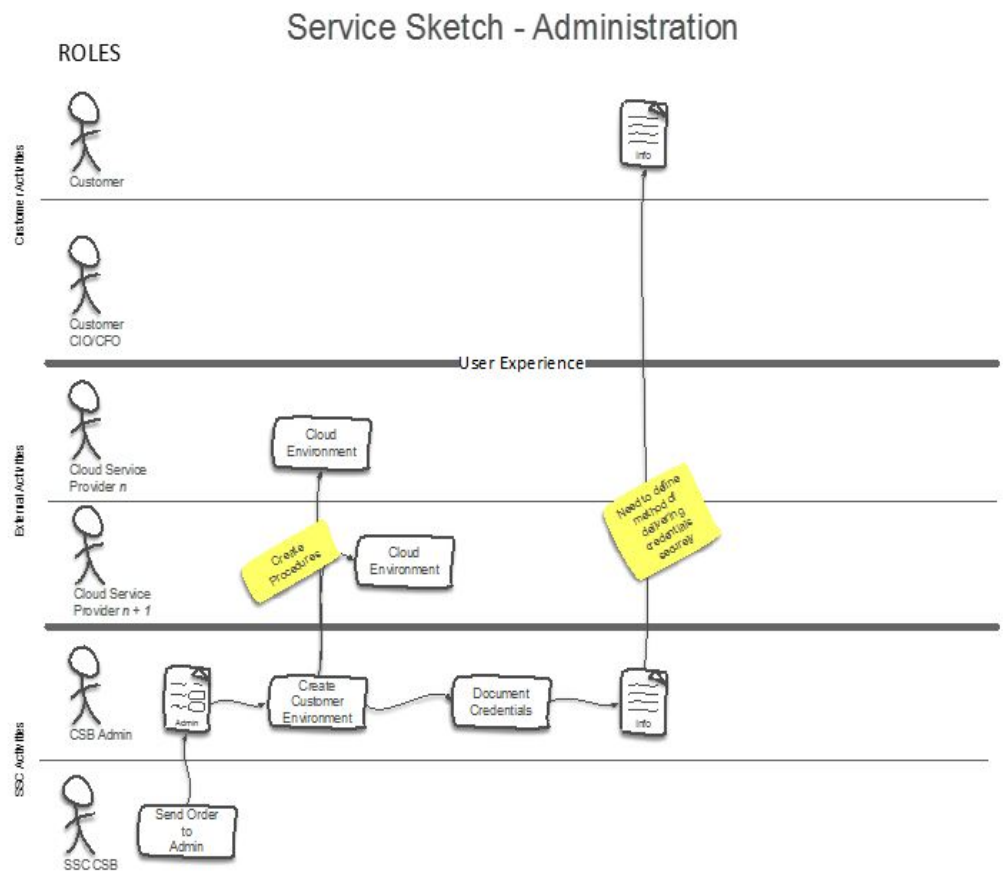
**Service Level Agreement:** Upon order receipt, the order will be acted upon within 2 business days with credentials sent to customer

**Frequency of Process:** On Demand


**Process Description:**

1. The CSB will send a work order to the CSB administrator;
2. The order will articulate the account information that needs to be provisioned in the CSP environment;
3. The CSB administrator will log in to the CSP environment and create the necessary resources;
4. The CSB administrator will document the environment in a form;
5. The form will be sent to the customer in a secure manner.

<i>Assumptions</i>
1) A master tenant model will be utilized;



1.8.8. BILLING



**Billing**  
Ability to provide a monthly bill for consumed services

**Owner:** Marc Contois

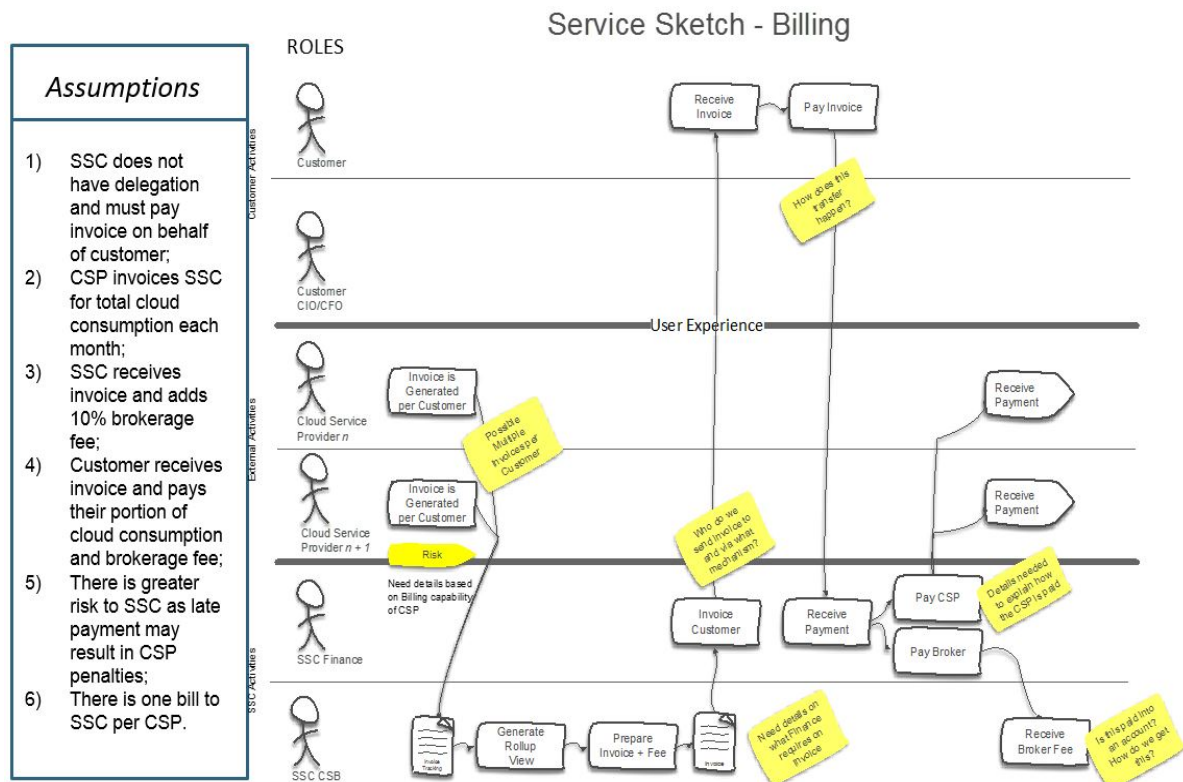
**Tool:** CSP Invoice, Rollup View Template, CSB Invoice Template, Invoice Tracking Template, Broker Fee Account

**Service Level Agreement:** Bills shall be delivered to SSC Finance within 2 days of receipt from the Cloud Service Provider.

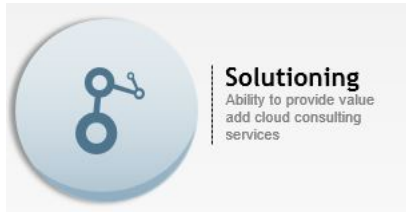
**Frequency of Process:** Monthly

**Process Description:**

1. The CSP will notify SSC via an email that a bill is due for a customer;
2. The CSB log into the CSP console, print the bill, enter the total into an Invoice tracking spreadsheet;
3. The CSB will prepare a single invoice with a subtotal per CSP engaged with;
4. The CSB will prepare an Invoice that includes the 10% broker fee;
5. The invoice will be sent to Finance by the CSB;
6. Finance will send the invoice to the customer who will transfer the funds to Finance;
7. Finance will pay each CSP (mechanism needs to be defined);
8. Finance will pay the broker fee to the SSC CSB account.



1.8.9. Solution



**Owner:** Marc Contois

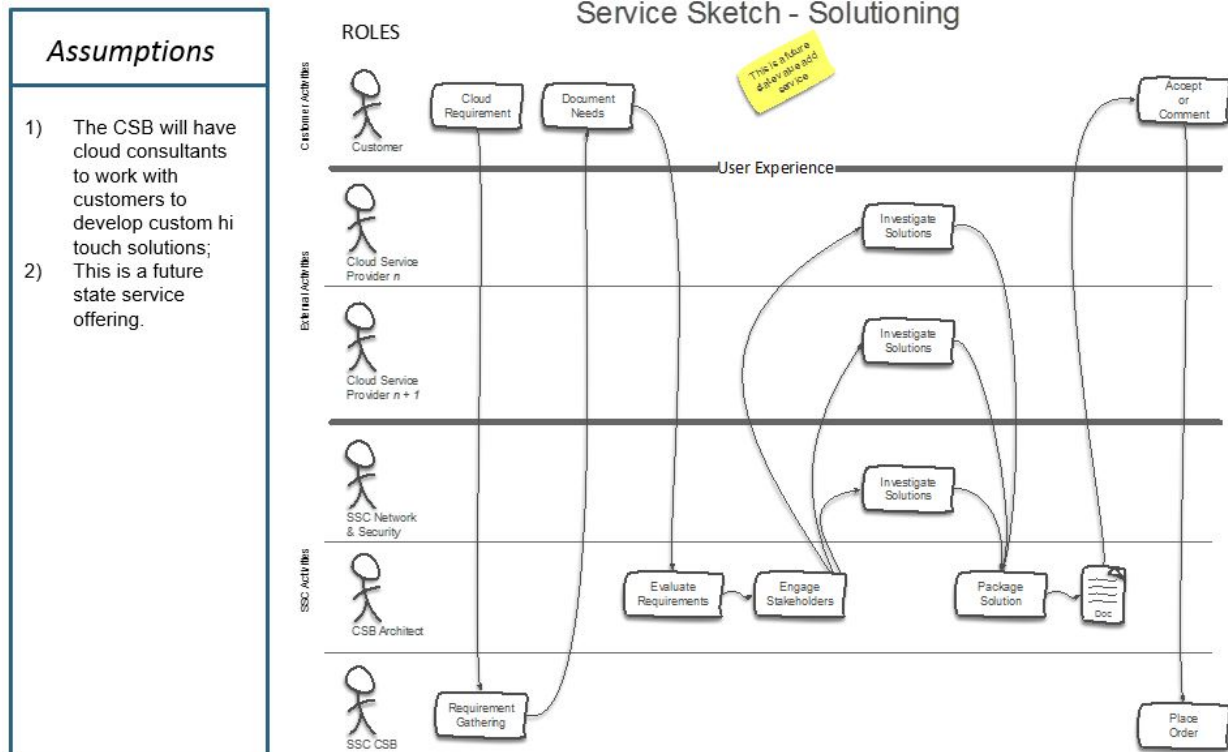
**Tool:** CSP Service Catalogue, Customized Solution Template

**Service Level Agreement:** TBD

**Frequency of Process:** On Demand.

**Process Description:**

1. Customer will approach the CSB with a custom requirement;
2. The CSB will work to refine requirements;
3. The requirements will be delivered to a CSB Cloud Architect;
4. The cloud architect will evaluate the requirements and investigate solutions ranging from CSP solutions to SSC solutions;
5. The cloud architect will package a solution and present to the customer;
6. The customer can then work to refine the solution, accept it, or deny it.
7. If accepted, the order process will execute.



1.8.10. Account Management



**Owner:** Marc Contois

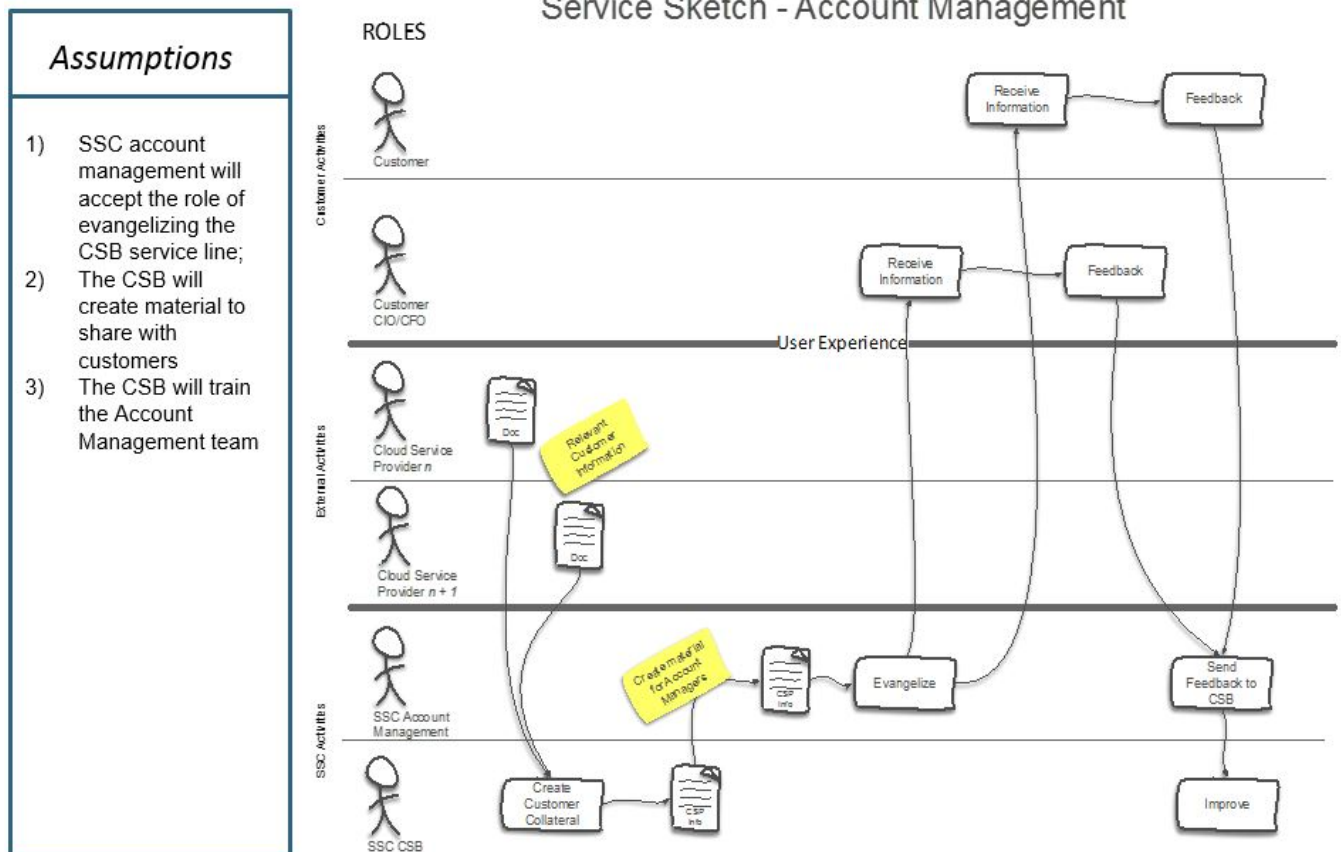
**Tool:** CSB Service Collateral, Training Material for Account Management

**Service Level Agreement:** The CSB will offer quarterly seminars to update account management of new capabilities and features.

**Frequency of Process:** Quarterly

**Process Description:**

1. The CSB will source pertinent information from the selected CSPs;
2. The CSB will create customer collateral and provide current information to the Account Management team;
3. The CSB will provide seminars to outline the breadth and depth of services available via the CSB;
4. The Account Management team will act as evangelists to customers, answering questions and queries with respect to the service.
- 5.



1.8.11. Catalogue



**Owner:** Marc Contois

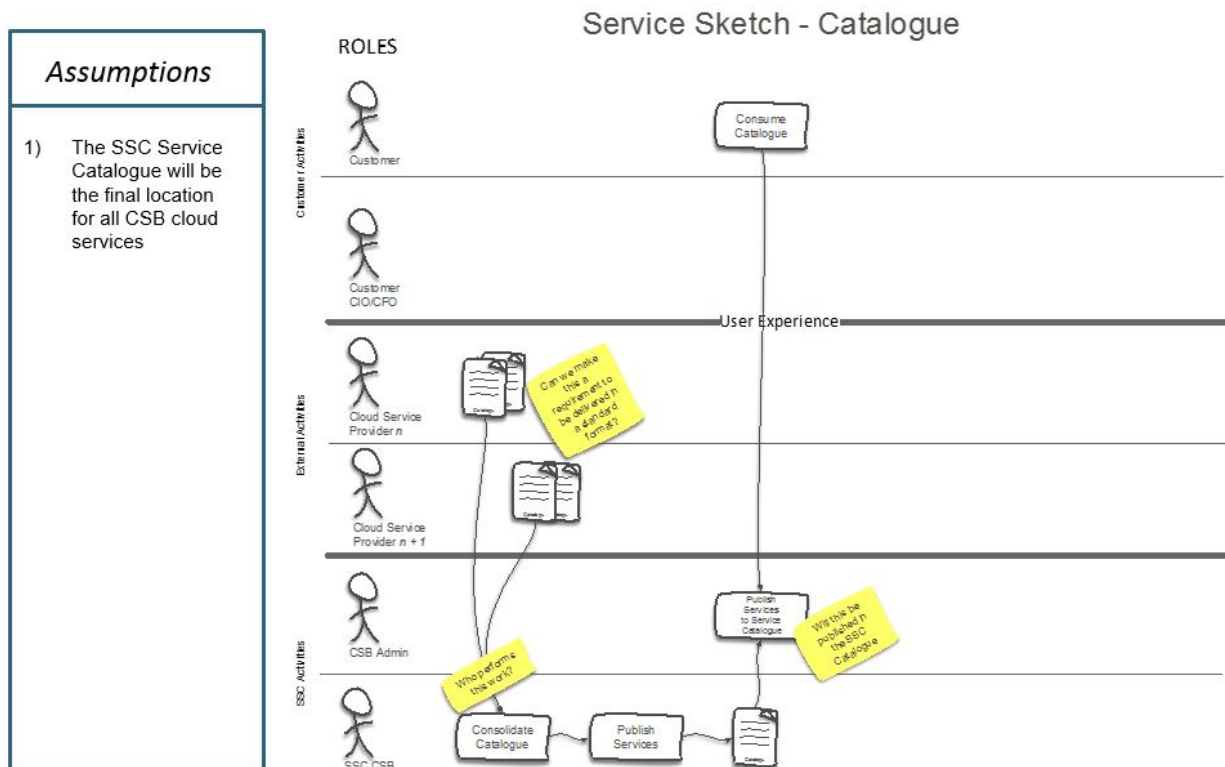
**Tool:** CSP Service Catalogue, CSB Catalogue View

**Service Level Agreement:** The catalogue will be kept up to date on a weekly basis

**Frequency of Process:** Weekly

**Process Description:**

1. The CSB will source each CSP catalogue;
2. The CSB will consolidate the catalogues into a view compatible with the SSC service catalogue;
3. The CSB Admin will publish the consolidated catalogue to the SSC Service Catalogue



### 1.8.12. Support Work Flow



**Owner:** Marc Contois

**Tool:** Service Desk Ticket System

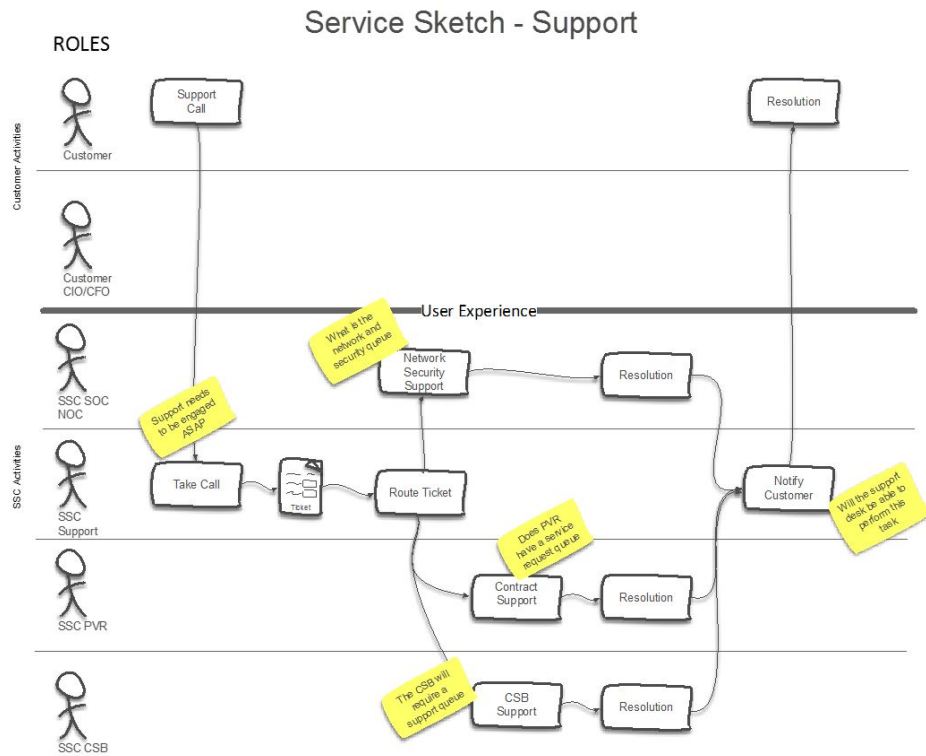
**Service Level Agreement:** Tickets will be resolved in 24 hours

**Frequency of Process:** On Demand

**Process Description:**

1. Customer will place a service request with the SSC Service Desk;
2. The agent will evaluate the call and forward to either the network organization, security organization, PVR or the CSB.
3. The ticket will be evaluated, acted upon and resolved.
4. The agent will forward the ticket back to the service desk to notify the customer of resolution.

Assumptions
1) SSC Support organization will create a queue for the CSB;
2) Front line support will take support calls and route to the appropriate destination;
3) Front line support will notify the customer of resolution.





### 1.8.13. Security Incident Work Flow

In the event of a detected security incident, the Cloud Service Provider must communicate this information to the SSC SOC.



**Owner:** Marc Contois

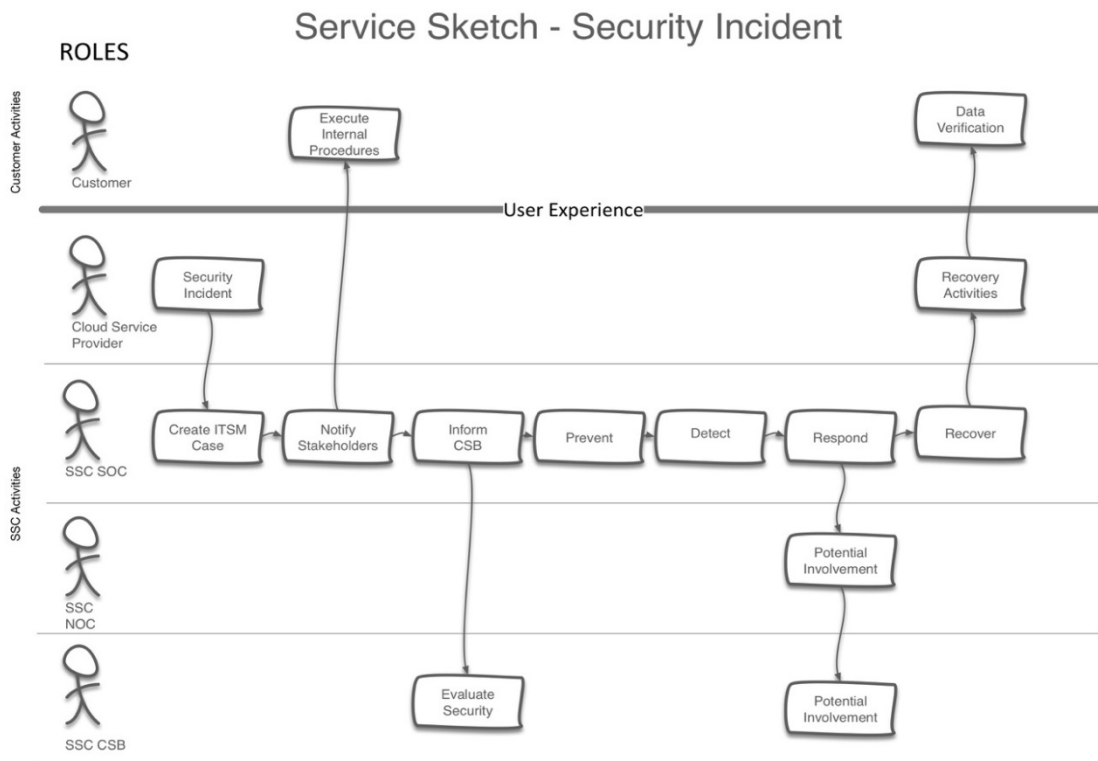
**Tool:** Incident Management,

**Service Level Agreement:** TBD

**Frequency of Process:** On Demand.

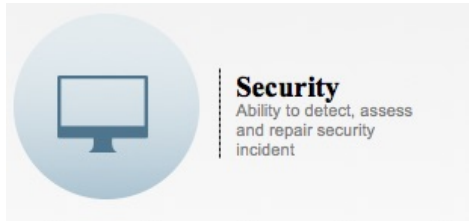
**Process Description:**

1. Email and phone notification is sent within 10 minutes of start of Severity 1 Incident to identified SSC Management.
2. CSP will maintain list of contacts;
3. Escalation procedures will provide mechanism to provide alternate means of resolution.



### 1.8.14. Customer Discovered Security Incident

In the event of a detected security incident by the customer, the customer must communicate this information to the SSC SOC. The SSC SOC will engage necessary stakeholders, including the CSP to work towards resolution.



**Owner:** Marc Contois

**Tool:** Incident Management,

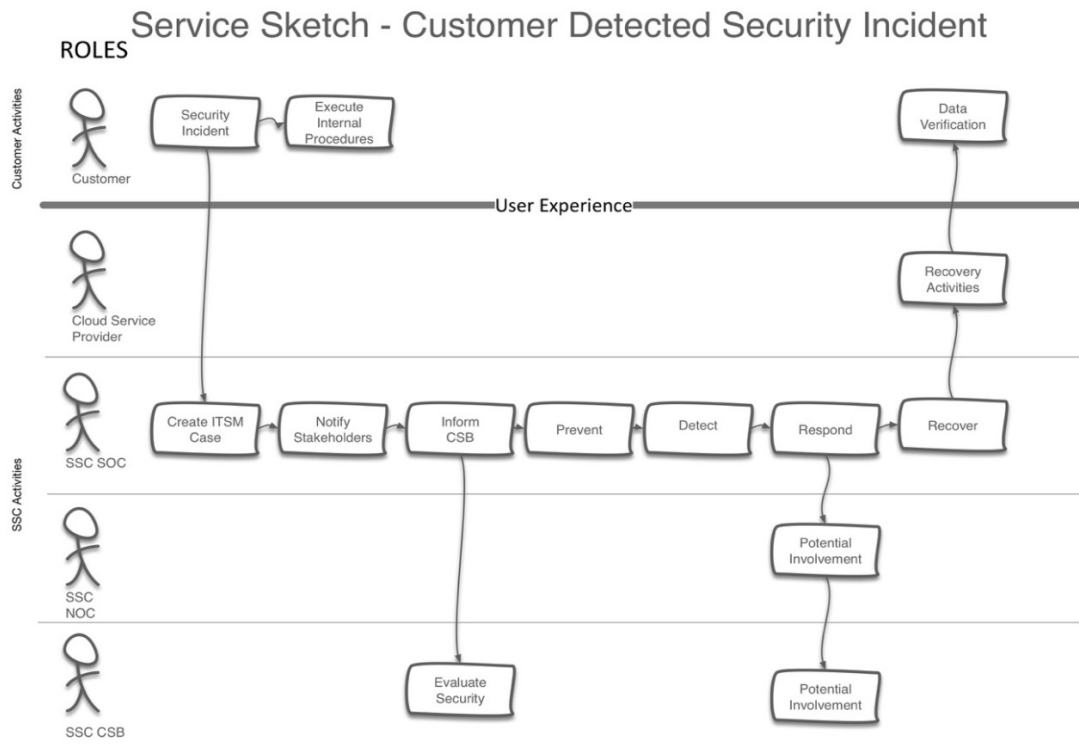
**Service Level Agreement:** TBD

**Frequency of Process:** On Demand.

**Process Description:**

1. Email and phone notification is sent within 10 minutes of start of Severity 1 Incident to identified SSC Management.
2. CSP will maintain list of contacts;
3. Escalation procedures will provide mechanism to provide alternate means of resolution.

### 1.8.15. Incident Notification



An email and phone notification is sent within 10 minutes from the start of the Severity 1 incident to a selective group of SSC management personnel. The CSP will maintain the list of agreed to resources who will receive notifications.

#### **1.8.16. Escalation Procedure**

Shared Services Canada will offer escalation support for customers requiring assistance with incident management. The Shared Services cloud enabling technical authority will intervene on behalf of customers and engage with the Cloud Service Provider in order to facilitate resolution. Customers who have engaged a CSP and have not achieved satisfactory resolution can engage the SSC Cloud Service desk. The following process will need to be followed:

1. Customer has contacted CSP regarding an incident and has not achieved a satisfactory resolution;
2. Customer will contact SSC Service desk;
3. The SSC Cloud Service desk will assess the call and offer guidance where possible, or escalate to the SSC Cloud Technical Authority;
4. The SSC Technical Authority will contact the customer to understand the incident;
5. The SSC Technical Authority may then contact the CSP in order to escalate and manage the incident with the CSP.

In addition to interfacing with CSPs, the SSC Technical Authority may also escalate internally to SSC. This can occur during provisioning network and security services to facilitate connectivity to CSPs.

#### **1.8.17. Escalation Timeframes**

Any incident to be resolved that will (or is expected to) exceed the service level (SL) threshold shall be escalated, and the SSC representative will be notified by an auto-generated email and by a phone call. The SSC SOC will notify necessary parties and perform their internal security process. The SOC will engage with the CSP and other stakeholders during the life of the incident until resolution has been achieved.

#### **1.8.18. Performance Management**

A more in-depth assessment of the performance management structure will be conducted as the project progresses; however, it has been determined that performance management functions will be integrated into the Enabler group. This group will be responsible for monitoring the use of CSP services and will have a suite of tools in order to generate reports. It is anticipated that the Enabler group will monitor aspects such as usage, functionality and service requests.

In addition, CSP's "public" Service Level Agreement will be utilized during the project.