



Operating Standard

Standard for ITSM Integration

Shared Services Canada

Service Management Transformation / Service Development &
Management Branch

Standard Version:	0.24
Approval status:	Draft
Lifecycle status:	Proposed
Publish Date:	DATE
Security Classification:	Unclassified



STANDARD HISTORY

Author and Collaborators

Name	Role	Organization
Don MacLean	Author	Service Management Transformation
<SSC Process Owners>	Contributor	SSC Service Management Operations
<BDTT members>	Contributor	<various>

Document History

Version	Date	Consulted	Author	Change information
v.0.1	2017-12-04	Don MacLean	Bruce Desarmia	Document Skeleton
v.0.24	2018-03-12	SSC Process Owners GC ITSM Working Group	Don MacLean, Bruce Desarmia,	Updated format to match SSC's process standard template Added SACM process Updates based on feedback from GC ITSM WG and consultations with SSC Process Owners. Update to Data Model to align to IT4IT reference architecture and provide more detail on data requirements Editing document for clarity and readability.

Table of Contents

Standard History	2
Author and Collaborators.....	2
Document History.....	2
Standard approval.....	5
1 Introduction	6
1.1 Purpose.....	6
1.2 Effective date	6
2 Scope	7
3 Normative References	8
4 Terms and Definitions	9
5 Standard statement.....	10
5.1 Change Management.....	10
5.1.1 Customer Initiated Change	10
5.1.2 Service Provider Changes	10
5.1.3 Impact Assessment	12
5.1.4 Change Closure.....	12
5.2 Incident Management.....	13
5.2.1 Incidents Reported by the Customer.....	13
5.2.2 Incidents Reported by the Service Provider	14
5.2.3 Incident Notifications.....	15
5.2.4 Incident Priority and Escalation.....	15
5.2.5 Analysis and Restoration of Service.....	15
5.3 Request Fulfillment	17
5.3.1 Customer Raising Service Request	17
5.3.2 Notifications.....	18
5.3.3 Fulfillment	19
5.4 Service Asset and Configuration Management.....	20
6 Exceptions	21
7 Implementation and monitoring.....	22
7.1 Implementation Process.....	22
7.2 Compliance Monitoring.....	22
7.3 Review	22

8	References	23
9	Inquiries	24
10	Annexes	25
10.1	Data Model	25
10.2	Rules for Calculating Incident Impact, Urgency and Priority	30

List of Tables and Figures

Figure 1	Change Management Process Interactions.....	10
Figure 2	Incident Management Process Interactions.....	13
Figure 3	Request Fulfillment Process Interaction	17

DRAFT

STANDARD APPROVAL

The authorities below concur with the conditions and responsibilities specified within this standard. In the case of recommending/approving committees, the date of the meeting and Record of Decision for the committee will serve.

Approved by Service, Project and Procurement Review Board (SPPRB)	Date
Recommended by Enterprise Strategy and Architecture Review Board (ESARB)	2018-03-19 Date
Presented to Architecture Council (AC)	2018-02-12 Date
	Sponsoring Enterprise Architect, Enterprise Architecture
	Sponsoring Service/Solution Architect, Branch/Directorate/Group
	Chair, Standard Peer Review Committee or Author of the standard

1 INTRODUCTION

The Government of Canada is committed to a whole-of-government or enterprise approach to IT infrastructure and service delivery. Sharing infrastructure and using common IT solutions to meet common needs is one part of leveraging technology in an enterprise approach.

Through the Government of Canada's IT Strategic Plan, Shared Services Canada (SSC) was tasked to put in place enterprise IT service management (ITSM) processes and tools, and to make them available to all departments and agencies.

IT Service Management refers to the entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization to plan, design, deliver, operate and control IT services offered to customers. These activities are enabled through IT tools.

Departments and agencies have implemented their own ITSM processes to manage their own IT functions. As the delivery of IT services requires components owned and managed across multiple departments, there is a need to ensure the integration of these processes.

This standard establishes the high-level requirements for the integration of ITSM processes between government departments.

1.1 PURPOSE

The purpose of this GC Standard on ITSM Integration is to establish requirements for the enterprise ITSM processes supporting the delivery of IT infrastructure services to GC departments and agencies.

Standardization of ITSM processes will lead to improved responsiveness and efficiency in service delivery management, including simplified workflow for employees, streamlined and reduced duplication of processes, and enhanced quality of services delivered to customers.

Rationalizing and standardizing ITSM processes will also help achieve efficiencies in terms of cost, provisioning time and improved service delivery to customers.

1.2 EFFECTIVE DATE

The GC Standard on ITSM Integration becomes effective upon approval by SPPRB.

2 SCOPE

This standard includes:

- Identification of roles in both service provider and customer organizations that interact in the performance of ITSM processes
- Definition of the data that must be exchanged in these interactions.

This standard does not include

- Identification of the roles responsible for any activity in the ITSM processes that does not involve any interaction with the other organization.

DRAFT

3 NORMATIVE REFERENCES

There are no normative references in this document.

DRAFT

4 TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions given in the [ITIL glossary and abbreviations English](#) and the following apply.

Term	Definition
User	A person who uses an IT Service
Customer	The customer is the GC department or agency who defines and agrees the service level targets for the IT service provided by the Service Provider
Service Provider	SSC as the organization supplying IT services to one or more external customers.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp/ui>

DRAFT

5 STANDARD STATEMENT

5.1 CHANGE MANAGEMENT

This section describes the interactions between Customers and Service Providers in the handling of Requests for Change (RFC) to the IT infrastructure within either organization. The high level process flow diagram describing the Change Management Interaction is provided in Figure 1. This process governs the recording, assessment, approval of RFCs and the review and closure of RFC after the change has been implemented. The actual implementation of change is managed in the Release and Deployment Process, which also includes an activity to update the configuration information in the Configuration Management Database (CMDB).

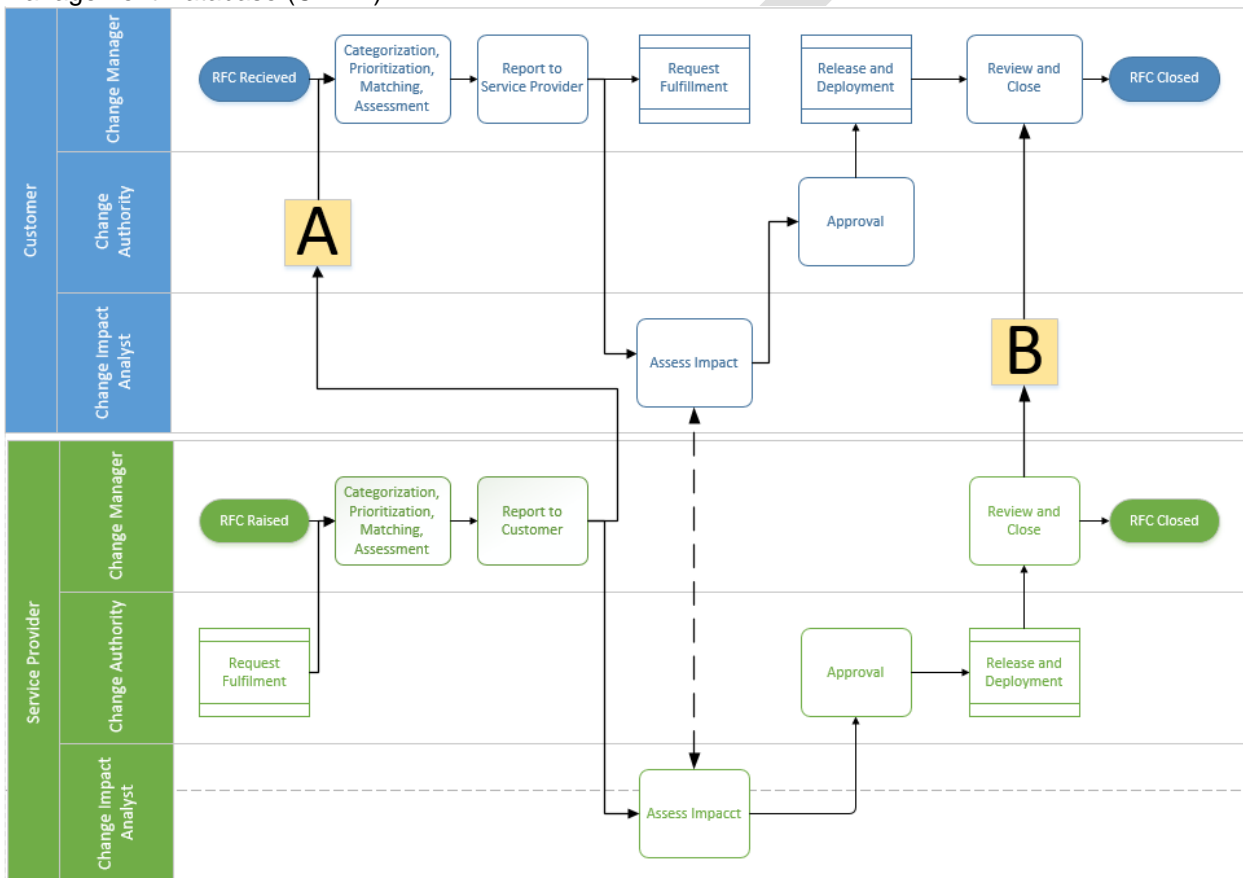


Figure 1 Change Management Process Interactions

5.1.1 CUSTOMER INITIATED CHANGE

When the Customer's analysis of an RFC indicates that changes are required to the Service Provider's IT infrastructure, the **Customer's Change Manager** will initiate the Request Fulfillment process (see section 5.3) to raise a Service Request.

5.1.2 SERVICE PROVIDER CHANGES

The **Service Provider's Change Manager** will ensure all planned changes are recorded as Requests for Change (RFC) in the Service Provider's ITSM Solution when the planning each change begins. The Service Provider's Change Manager will ensure that all emergency changes performed in response to

incidents, are recorded in the Service Provider's ITSM Solution as soon as is feasible. The Service Provider's Change Manager will ensure that the RFC is kept up to date with all new and changed information related to the change as it progresses through to implementation.

The following information on each RFC will be made available to the Customer (**Flow "A" in the Change process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID Actual Service Name
Incident	Service Provider's Incident ID Title
IT Initiative	IT Initiative ID
Request	Customer Request ID Service Provider Request ID Title
RFC	Approval Status Back-Out Plan Business Justification Change Status Change Type Description Impact Impact Statement Impacted Customer Implementation Plan In Maintenance Window Initiating Customer Planned End Date Planned Start Date Priority Requested End Date Requested Start Date Risk Risk Mitigation Strategy Service Provider's RFC ID Title Urgency Work Log Entry
Service Catalogue	Offer Name Service
User Profile	Assigned To Email Assigned To Full Name Assigned To Telephone

The attributes are described in detail in the Data Model, section 10.1.

The Customer's Change Manager will review the information from the Service Provider's RFC and decide on the appropriate action. This may include:

- Matching to an existing RFC in the Customer's ITSM Solution,
- Creation of a RFC in the Customer's ITSM Solution if the Service Provider's change requires changes in the IT infrastructure of the Customer,
- Monitoring the progress of the Service Provider's RFC, or
- Take no action.

5.1.3 IMPACT ASSESSMENT

The **Service Provider's Change Impact Analysts** may contact their counterparts with the Customer's Change Impact Analysts to ensure the impact statement recorded in the RFC accurately reflects the expected impact of the change to the Customer services that are enabled by the changing IT infrastructure. The impact statement will also indicate if there will be any effect (i.e. outages) to Customer business services during the actual implementation or backing-out of the change.

5.1.4 CHANGE CLOSURE

Once change has been implemented, the **Service Provider's Change Manager** provides final quality control to the RFC, closes the RFC and provides the following information to the Consumer (**Flow "B" in the Incident process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID
	Actual Service Name
Incident	Service Provider's Incident ID
	Title
IT Initiative	IT Initiative ID
Request	Customer Request ID
	Service Provider Request ID
	Title
RFC	Actual End Date
	Actual Impact
	Actual Start Date
	Change Status
	Change Type
	Closure Code
	Description
	Impacted Customer
	In Maintenance Window
	Initiating Customer
	Service Provider's RFC ID
Title	
Work Log Entry	
Service Catalogue	Offer Name
	Service

The attributes are described in detail in the Data Model, section 10.1.

5.2 INCIDENT MANAGEMENT

This section describes interactions between customers and service provider when incidents have been reported against the IT services provided by the service provider. The process is described in Figure 2.

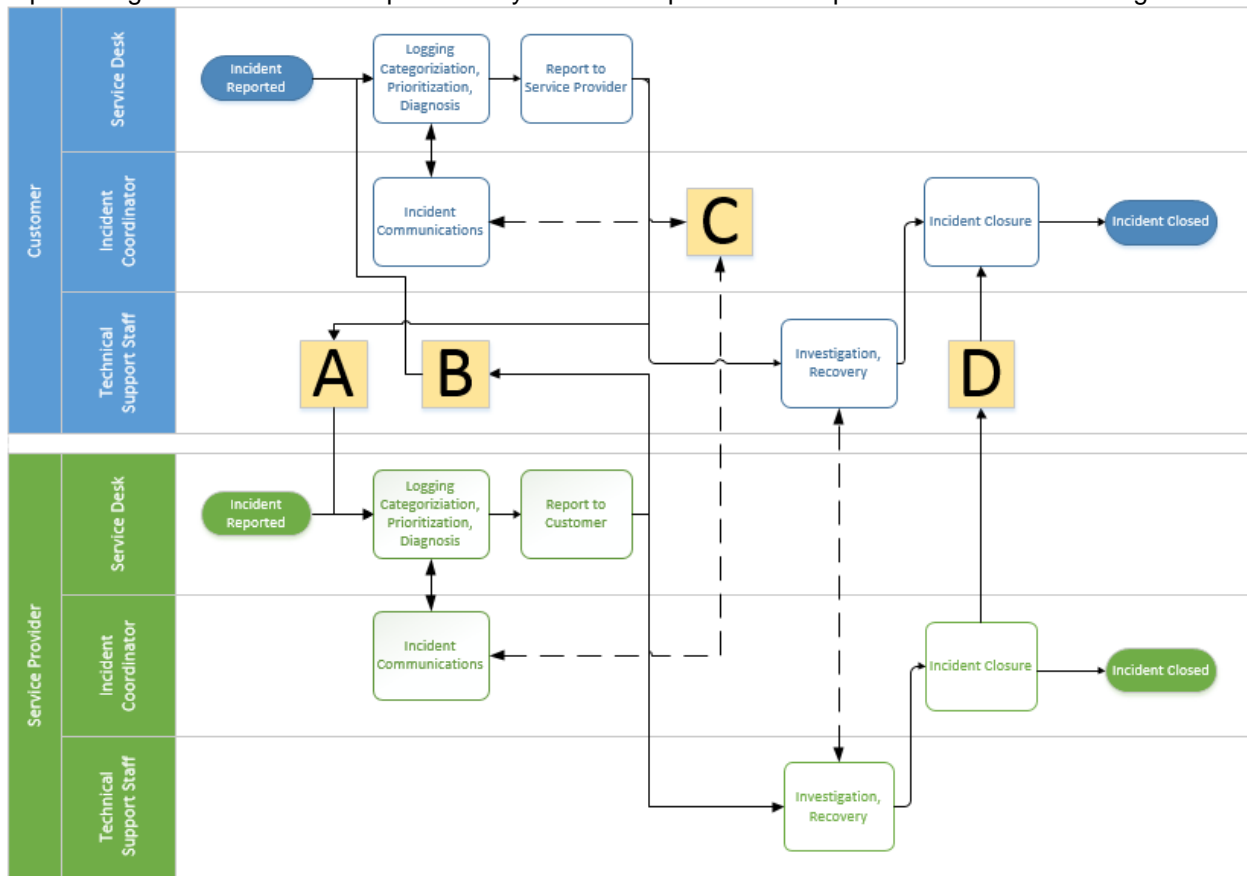


Figure 2 Incident Management Process Interactions

5.2.1 INCIDENTS REPORTED BY THE CUSTOMER

When the customer investigates an incident and identifies a failure in service provider's IT services, this incident is reported to the service provider. The **Customer's Service Desk** will contact the Service Provider's Service Desk to report the incident. The following information is required when reporting an incident to the Service Provider (**Flow "A" in the Incident process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID Actual Service Name
Incident	Customer Incident ID Description Incident Location Title
Service Catalogue	Offer Name Service

User Profile	Customer Department User Email User Full Name User Telephone
---------------------	---

The attributes are described in detail in the Data Model, section 10.1.

The **Service Provider's Service Desk** acknowledges the receipt of the incident, by providing the following information to the Customer's Service Desk (**Flow "B" in the Incident process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID Actual Service Name
Incident	Customer Incident ID Description Estimated TTR Impact Incident Location Priority Service Provider Incident ID Status Title Urgency
Service Catalogue	Offer Name Service
User Profile	Customer Department Assigned To Email Assigned To Full Name Assigned To Telephone

The attributes are described in detail in the Data Model, section 10.1.

5.2.2 INCIDENTS REPORTED BY THE SERVICE PROVIDER

When there is a failure with IT infrastructure services, the **Service Provider's Service Desk** will contact the Service Desk of the customers consuming these services to report the incident. The following information will be provided (**Flow "B" in the Incident process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID Actual Service Name
Incident	Description Estimated TTR Impact Incident Location Priority Service Provider Incident ID Status Title Urgency
Service Catalogue	Offer Name Service

User Profile	Customer Department Assigned To Email Assigned To Full Name Assigned To Telephone
---------------------	--

The attributes are described in detail in the Data Model, section 10.1.

5.2.3 INCIDENT NOTIFICATIONS

While the incident is open, notifications will be sent by the Service Provider to all Customers affected by the incident. Affected Consumers are those whose business and IT services are dependent on those of the failed IT infrastructure components. The **Service Provider's Incident Coordinator** provides incident status and notifications to all stakeholders until the incident is resolved. The frequency of the updates will be determined by the priority assigned to the incident. The following information will be provided (**Flow "C" in the Incident process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID Actual Service Name
Incident	Customer Incident ID Description Estimated TTR Impact Incident Location Priority Service Provider Incident ID Status Title Urgency Work Log Entry
Service Catalogue	Offer Name Service
User Profile	Customer Department Assigned To Email Assigned To Full Name Assigned To Telephone

The attributes are described in detail in the Data Model, section 10.1.

5.2.4 INCIDENT PRIORITY AND ESCALATION

The rules used by the Service Provider to determine the impact, urgency and priority of incidents reported to or by the Service Provider are described the Appendix, section 10.2. The priority is based on the combination of the impact and urgency of the incident. The **Service Provider's Incident Coordinator** will calculate the priority of the Incident and use this value to govern notification frequency, and target times for restoration of service.

If 1) it is believed that there has been an error in the calculation of the priority of the incident, or 2) additional information has become available on the impact or urgency of the incident or 3) the extent or nature of the service failure has changed, the **Customer's Incident Coordinator** can contact the Service Provider's Incident Coordinator to request that the priority be recalculated.

5.2.5 ANALYSIS AND RESTORATION OF SERVICE

The **Service Provider's Technical Support Staff** will update the work log of the incident record with the actions taken to diagnose the service failure and to identify required remediation. The Service Provider's Technical Support Staff may contact their counterparts with the Customer's Technical Support Staff.

Once service has been restored, the **Service Provider’s Incident Coordinator** provides final quality control to the incident record, issues the final Incident notification to customer stakeholders and closes the Incident record. The following information is provided to the Service Consumer (**Flow “D” in the Incident process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID
	Actual Service Name
Incident	Closure Code
	Customer Incident ID
	Description
	Estimated TTR
	Service Provider Incident ID
	Status
	Title
Service Catalogue	Work Log Entry
	Offer Name
User Profile	Service
	Customer Department

The attributes are described in detail in the Data Model, section 10.1.

DRAFT

5.3 REQUEST FULFILLMENT

This section describes the interactions between Customers and Service Providers in the handling of service Requests made by Customers for the Service Provider. The high level process flow diagram detailing the interactions is provided in Figure 3.

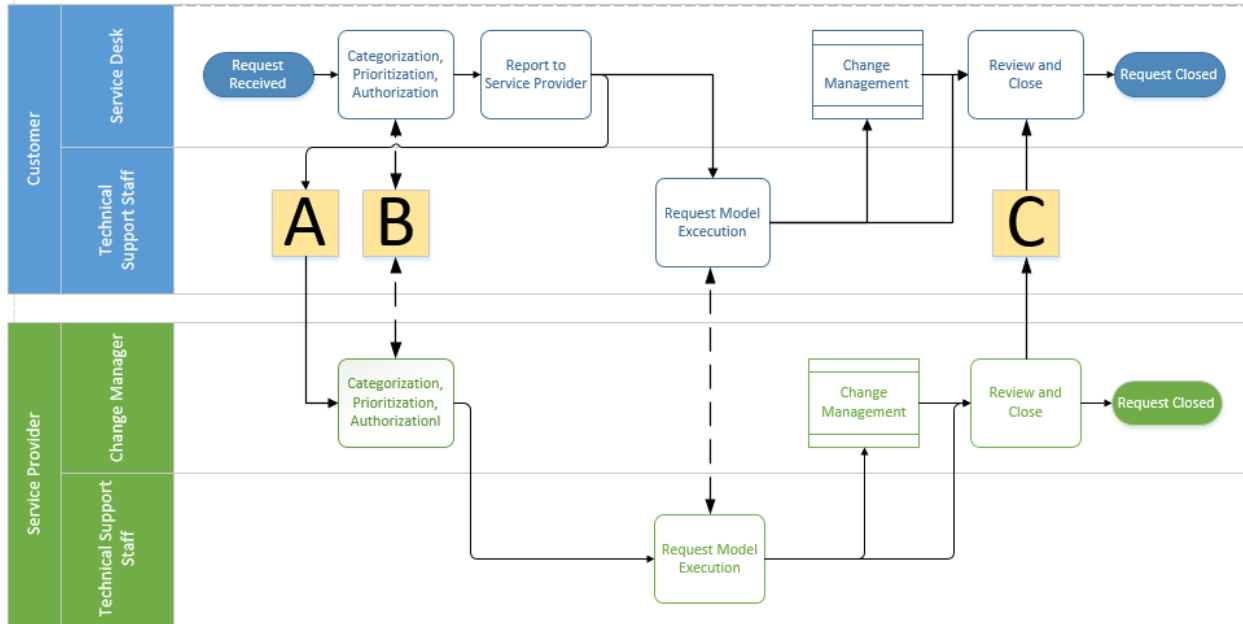


Figure 3 Request Fulfillment Process Interaction

The request will be one of two types:

- Request for a service offer described in the Service Catalogue, and
- Request for a quote for a new offer or a change to an existing offer.

When the process is complete, the customer will have either the offer instantiated as an Actual Service consumed by the Customer or a quote describing the new or changed offer.

5.3.1 CUSTOMER RAISING SERVICE REQUEST

The Customer's Service Desk is responsible for ensuring that all requests being made of the Service Provider have been properly categorized and prioritized and that the request has received that proper technical and financial approvals before the request is raised to the Service Provider. To make the request, the Customer's Service Desk will provide the following information to the Service Provider's Service Desk (**Flow "A" in the Request Fulfillment process flow diagram**):

Record	Attribute
Request	Customer Request ID Impact Maximum Fulfill Date Priority Required Values Title Urgency
Service Catalogue	Offer Name Service

User Profile	Customer Department User Email User Full Name User Telephone
---------------------	---

The attributes are described in detail in the Data Model, section 10.1.

The **Service Provider's Service Desk** acknowledges the receipt of the request, by providing the following information to the Customer's Service Desk (**Flow "B" in the Request Fulfillment process flow diagram**):

Record	Attribute
Request	Customer Request ID Estimated Fulfill Date Impact Maximum Fulfill Date Priority Request Date Required Values Service Provider Request ID Status Title Urgency Work Log Entry
RFC	Service Provider RFC ID Title
Service Catalogue	Offer Name Service
User Profile	Customer Department Assigned To Email Assigned To Full Name Assigned To Telephone

The attributes are described in detail in the Data Model, section 10.1.

5.3.2 NOTIFICATIONS

Until the Request is completed, notifications will be sent by the Service Provider's Service Desk to the Customer's Service Desk. The frequency of the updates will be determined by the priority assigned to the Request. The following information will be provided (**Flow "B" in the Request Fulfillment process flow diagram**):

Record	Attribute
Request	Customer Request ID Estimated Fulfill Date Impact Maximum Fulfill Date Priority Required Values Service Provider Request ID Status Title Urgency Work Log Entry
RFC	Service Provider RFC ID Title

Service Catalogue	Offer Name Service
User Profile	Customer Department Assigned To Email Assigned To Full Name Assigned To Telephone

The attributes are described in detail in the Data Model, section 10.1.

5.3.3 FULFILLMENT

Requests will be fulfilled following the Request Model Executions the Customer and Service Provider will have created to complete the Offers. The **Service Provider's Technical Support Staff** may contact their counterparts with the **Customer's Technical Support Staff** to complete the request execution model.

If the fulfillment of the request requires change to the configuration of a Configuration Items (CIs) of either the Service Provider or Customer, the respective Technical Support Staff will initiate the Change Request Process (section 5.1) for impact assessment and approved, and to subsequently initiate the Release and Deployment process to implement the changed configuration.

Once request has been fulfilled, the **Service Provider's Service Desk** provides final quality control to the Request record and closes the Request record. The following information is provided to the Service Consumer (**Flow "C" in the Request Fulfillment process flow diagram**):

Record	Attribute
Actual Service	Actual Service ID Actual Service Name Actual Service Owner Actual Service Type
Request	Actual Fulfill Date Customer Request ID Request Closure Code Required Values Service Provider Request ID Status Title Work Log Entry
RFC	Service Provider RFC ID Title
Service Catalogue	Offer Name Service
User Profile	Customer Department

The attributes are described in detail in the Data Model, section 10.1.

5.4 SERVICE ASSET AND CONFIGURATION MANAGEMENT

There are no interactions between Customers and Service Providers with respect to the Service Asset and Configuration Management process.

DRAFT

6 EXCEPTIONS

The GC Standard for ITSM Integration identifies no exceptions that apply.

DRAFT

7 IMPLEMENTATION AND MONITORING

7.1 IMPLEMENTATION PROCESS

This standard identifies no implementation processes that apply.

7.2 COMPLIANCE MONITORING

This standard identified no compliance monitoring processes that apply.

7.3 REVIEW

This standard shall be reviewed, at a minimum, once each year after it has been approved.



DRAFT

8 REFERENCES

ISO/IEC 20000-1:2011, <https://www.iso.org/standard/51986.html>
IT4IT Reference Architecture v2.1, <http://pubs.opengroup.org/it4it/refarch21/IT4ITv2.1.html>
ITIL Continual Service Improvement 2011 edition, <https://www.axelos.com/store/book/itil-continual-service-improvement>
ITIL Service Design 2011 edition, <https://www.axelos.com/store/book/itil-service-design>
ITIL Service Operation 2011 edition, <https://www.axelos.com/store/book/itil-service-operation>
ITIL Service Strategy 2011 edition, <https://www.axelos.com/store/book/itil-service-strategy>
ITIL Service Transition 2011 edition, <https://www.axelos.com/store/book/itil-service-transition>
SSC Incident templates and tools,
<https://gcdocs.gc.ca/ssc-spc/lisapi.dll?func=ll&objId=17506376>

DRAFT

9 INQUIRIES

For any inquiries, please contact: Monika Kumari, Service Management Transformation, Service Delivery and Management Branch, SSC.

DRAFT

10 ANNEXES

10.1 DATA MODEL

This section provides the specifications of the data that is shared between Service Provider and Customer that are listed in section 5 of this document.

Record	Attribute	Definition	Variable Type	Authoritative Source	Format / Values	ChM	IM	RFL
Actual Service	Actual Service ID	Unique Identifier that represents the realized deployment of the service. Includes Configuration Items that represent the implemented service components.	System Generated	CMDB Data Model		AB	ABCD	C
Actual Service	Actual Service Name	Name of the Actual Service	Keyed Text	CMDB Data Model		AB	ABCD	C
Actual Service	Actual Service Owner	Group or person that is assigned to own the Actual Service	Keyed Text	CMDB Data Model				C
Actual Service	Actual Service Type	Type of the Actual Service	Selection List	CMDB Data Model				C
Incident	Closure Code	Description of the final disposition of the Incident	Selection List	This document	<from ECD>		D	
Incident	Customer Incident ID	Customer's unique identifier for the Incident	System Generated	n/a	Format and values from Customer's ITSM Solution		ABCD	
Incident	Description	Description of the Incident. Including: - Environment (Production or Development) - Critical Business Application Service - Type of service failure (full outage, partial outage, degraded performance, other) - Affected client type (Public, External Client, Internal) - Affected client number - Location (Designated Site, Non-Designated Site, Mobile, n/a)	Keyed Text	n/a	<from ECD>		ABCD	
Incident	Estimated TTR	Estimated time to restore service - estimated Date/Time when the service will be restored	Keyed Text	n/a	<from ECD>		BCD	
Incident	Impact	Describes the business impact resulting from the Incident	Selection List	This document	see section 10.2		BC	
Incident	Incident Location	Description of the geographic extent of the Incident	Keyed Text	n/a	<from ECD>		ABC	
Incident	Priority	Priority for fixing the Incident	System Generated	This document	see section 10.2		BC	
Incident	Service Provider Incident ID	Service Provider's unique identifier for the Incident	System Generated	n/a	<from ECD>	AB	BCD	

Record	Attribute	Definition	Variable Type	Authoritative Source	Format / Values	ChM	IM	RFL
Incident	Status	Controls the status of the Incident	Selection List	This document	<from ECD>			BCD
Incident	Title	Title given to the Incident	Keyed Text	n/a	<from ECD>	AB		ABCD
Incident	Urgency	An indication of the time before the business is severely impacted	Selection List	This document	see section 10.2			BC
Incident	Work Log Entry	Running log of actions taken to resolve the Incident	Keyed Text	n/a	<from ECD>			CD
IT Initiative	IT Initiative ID	Describes the IT Initiative generating this Change	System Generated	n/a	<from ECD>	AB		
Request	Actual Fulfill Date	Date/time on which the Request is fulfilled.	System Generated	n/a	<from ECD>			C
Request	Customer Request ID	Customer's unique identifier for the Request.	System Generated	n/a	Format and values from Customer's ITSM Solution	AB		ABC
Request	Estimated Fulfill Date	Estimated date/time when the Request is expected to be fulfilled	Keyed Text	n/a	<from ECD>			B
Request	Impact	Describes the business impact resulting from the request	Selection List	This document	see section 10.2			AB
Request	Maximum Fulfill Date	Maximum date/time on which the Request needs to be fulfilled.	Keyed Text	n/a	<from ECD>			AB
Request	Priority	Priority for fulfilling the Service Request	System Generated	This document	see section 10.2			AB
Request	Request Closure Code	Description of the final disposition of the Service Request	Selection List	This document	<From ECD: AUT, RWWFLS, RWW, RWOI, RPFLS, RP, NRNR, NRCO, NR>			C
Request	Request Date	Date/time the Request was received.	System Generated	n/a	<from ECD>			B
Request	Required Values	Mandatory options or variables linked to the service which need to be provided by the consumer to prevent issues during the fulfillment.		SSC Service Catalogue	Specific required values (as well as formatting) will vary depend on the Offer. The required values are described in the SSC Service Catalogue. Some of the options or variables might not be selectable for customers, but are pre-filled by the Offer itself upon creation of the Offer.			ABC
Request	Service Provider Request ID	Service Provider's unique identifier for the Request.	System Generated	n/a	<from ECD>	AB		BC

Record	Attribute	Definition	Variable Type	Authoritative Source	Format / Values	ChM	IM	RFL
Request	Status	Controls the status of the fulfillment	Selection List	This document	<from ECD>			BC
Request	Title	Brief description of the request	Keyed Text	n/a	<from ECD>	AB		ABC
Request	Urgency	An indication of the time before the business is severely impacted	Selection List	This document	see section 10.2			AB
Request	Work Log Entry	Running log of actions taken to fulfill the Request	Keyed Text	n/a	<from ECD>			BC
RFC	Actual End Date	Date/time when the implementation of the RFC actually ended	Keyed Text	n/a	<from ECD>	B		
RFC	Actual Impact	Actual impact to the users from the implementation of the RFC	Keyed Text	n/a	<from ECD>	B		
RFC	Actual Start Date	Date/time when the implementation of the RFC actually began	Keyed Text	n/a	<from ECD>	B		
RFC	Approval Status	The current status of the Approval of the RFC	Selection List	This document	<from ECD>	A		
RFC	Back-Out Plan	The conditions under which the RFC will be backed-out and the procedures to follow to do so	Keyed Text	n/a	<from ECD>	A		
RFC	Business Justification	Business reasons supporting implementation of the RFC	Keyed Text	n/a	<from ECD>	A		
RFC	Change Status	The current step in the RFC workflow	Selection List	This document	<from ECD>	AB		
RFC	Change Type	Indicates if the RFC is an emergency change	Selection List	This document	Values: - Emergency - Non-Emergency	AB		
RFC	Closure Code	Description of the final disposition of the Incident	Selection List	This document	<from ECD>	B		
RFC	Description	Description of the Change. Includes: - Criteria to use to determine if the change was successful	Keyed Text	n/a	<from ECD>	AB		
RFC	Impact	Describes the business impact resulting from the request	Selection List	This document	see section 10.2	A		
RFC	Impact Statement	Description of the impact of the Change for users of services supported by the Actual Services affected by the change - including the impacts (e.g. outages) required to implement the change	Keyed Text	n/a	<from ECD>	A		
RFC	Impacted Customer	Indicates the Customer(s) impacted by the change in that their services are supported by the Actual Service(s) involved in this change	Selection List	PSPC - List of legal department names and their respective numbers	http://donnees-data.tpsgc-pwgsc.gc.ca/ba1/min-dept/min-dept.csv	AB		

Record	Attribute	Definition	Variable Type	Authoritative Source	Format / Values	ChM	IM	RFL
RFC	Implementation Plan	Schedule of activities required to implement the change. Includes assignment of activities and ordering of activities. Includes strategy for communicating the change to affected users	Keyed Text	n/a	<from ECD>	A		
RFC	In Maintenance Window	Indicates that the change will be implemented in the maintenance window of that Actual Service	Selection List	n/a	Values: - Yes - No	AB		
RFC	Initiating Customer	Indicates the Customer Department that initiated the RFC	System Generated	PSPC - List of legal department names and their respective numbers	http://donnees-data.tpsgc-pwgsc.gc.ca/ba1/min-dept/min-dept.csv	AB		
RFC	Planned End Date	Date/time that RFC implementation is planned to end	Keyed Text	n/a	<from ECD>	A		
RFC	Planned Start Date	Date/time that RFC implementation is planned to start	Keyed Text	n/a	<from ECD>	A		
RFC	Priority	Priority for Implementing the Change	System Generated	This document	see section 10.2	A		
RFC	Requested End Date	Date/time requested by initiator to end the implementation of the RFC	Keyed Text	n/a	<from ECD>	A		
RFC	Requested Start Date	Date/time requested by initiator to start the implementation of the RFC	Keyed Text	n/a	<from ECD>	A		
RFC	Risk	The probability that the change could cause harm or loss, or affect the ability to achieve objectives	Selection List	This document	<from ECD>	A		
RFC	Risk Mitigation Strategy	Strategy to mitigate the risks identified with the implementation of this change	Keyed Text	n/a	<from ECD>	A		
RFC	Service Provider RFC ID	Service Provider's unique identifier for the Change	System Generated	n/a	<from ECD>	AB	x	BC
RFC	Title	Title of the Change	Keyed Text	n/a	<from ECD>	AB		BC
RFC	Urgency	An estimate of how soon the change should be implemented. Urgency represents the current level of necessity to make the change right away	Selection List	This document	see section 10.2	A		
RFC	Work Log Entry	Running log of actions taken to assess impact, approve, and implement the change	Keyed Text	n/a	<from ECD>	AB		
Service Catalogue	Offer Name	Requestable service offering identified in the Service Catalogue	Selection List	SSC Service Catalogue	From SSC Service Catalogue	A		ABC

Record	Attribute	Definition	Variable Type	Authoritative Source	Format / Values	ChM	IM	RFL
Service Catalogue	Service	Name of a customer-facing service	Selection List	SSC Service Inventory	http://service.ssc-spc.gc.ca/en/services	A		ABC
User Profile	Assigned to Email	Email of the group or person assigned to - resolve an Incident - implement an RFC	Keyed Text	n/a	<from ECD>	A	BC	B
User Profile	Assigned to Name	Name of the group or person assigned to - resolve an Incident - implement an RFC	Keyed Text	n/a	<from ECD>	A	BC	B
User Profile	Assigned to Telephone	Telephone of the group or person assigned to - resolve an Incident - implement an RFC	Keyed Text	n/a	<from ECD>	A	BC	B
User Profile	Customer Department	The customer department	Selection List	PSPC - List of legal department names and their respective numbers	http://donnees-data.tpsgc-pwgsc.gc.ca/ba1/min-dept/min-dept.csv		ABCD	ABC
User Profile	User Email	Email of the user who: - imitated the service request - reported the incident	Keyed Text	n/a	<from ECD>		A	A
User Profile	User Full Name	Full name of the user who: - imitated the service request - reported the incident	Keyed Text	n/a	<from ECD>		A	A
User Profile	User Telephone	Primary phone number of the user who: - imitated the service request - reported the incident	Keyed Text	n/a	<from ECD>		A	A

10.2 RULES FOR CALCULATING INCIDENT IMPACT, URGENCY AND PRIORITY

	Data Element	Values
Incident Record	Incident Impact	<p>Extensive - Critical business applications & services of SSC and/or Partners are fully affected or reputation is potentially at stake. The business or businesses may be unable to achieve their objectives such as satisfying the needs of their clients. The risk to public confidence and/or safety may be severe.</p> <p>Significant - Critical business applications & services of SSC and/or Partners are partially affected. There may be considerable disruption to business activities. The risk to public confidence and/or safety may be considerable.</p> <p>Moderate – Limited or no impact on the critical business applications & services of SSC and/or Partners. There may be some disruption to the business' non-core activities and therefore a reduced productivity of users. There may be limited or no actual risk to public confidence and/or safety.</p> <p>Minor - There is no disruption to the critical business applications & services of SSC and/or Partners. There may be minimal to no disruption to non-core business activities. Users are inconvenienced but can still carry-out the business activity or other business activities.</p>
	Incident Priority	
	Incident Urgency	<p>Critical – Severe effect on SSC and/or Partner timely delivery of their services. May be extremely time sensitive, harmful to the business or its reputation.</p> <p>High – Considerable effect on SSC and/or Partner timely delivery of their services. May be highly time sensitive as the harm to the business or its reputation is likely to occur in a short timeframe.</p> <p>Medium – Some effect on SSC and/or Partner timely delivery of their services. Sufficient time to allow a response without unreasonably effecting business productivity.</p> <p>Low - Little or no effect on SSC and/or Partner timely delivery of their services. Normal work can continue until responding.</p>

Critical Business APPLICATION and SERVICE (CBAS)

PRODUCTION

IMPACTING	WHO	WHERE	IMPACT LEVEL	URGENCY LEVEL	PRIORITY
FULL outage					
Full outage of an identified Critical Business Applications & Services.					
All	Internal User	Mobile	Extensive	Critical	Critical
All	Internal User	Designated Site(s)	Extensive	Critical	Critical
All	Internal User	Non-Designates Site(s)	Extensive	High	Critical
All	Public User	N/A	Extensive	Critical	Critical
All	External Client	N/A	Extensive	Critical	Critical
PARTIAL outage					
Partial outage of a Critical Business Applications & Services impacting one or more Critical functions.					
Significant amount of	Internal User	Mobile	Significant	Critical	Critical
Insignificant amount of	Internal User	Mobile	Significant	High	High
Negligible amount of	Internal User	Mobile	Significant	Medium	Medium
Significant amount of	Internal User	Designated Site(s)	Significant	Critical	Critical
Insignificant amount of	Internal User	Designated Site(s)	Significant	High	High
Negligible amount of	Internal User	Designated Site(s)	Significant	Medium	Medium
Significant amount of	Internal User	Non-Designated Site(s)	Significant	High	High
Insignificant amount of	Internal User	Non-Designated Site(s)	Significant	Medium	Medium
Negligible amount of	Internal User	Non-Designated Site(s)	Significant	Low	Low
Large number amount of	Public User	N/A	Significant	Critical	Critical
Small number amount of	Public User	N/A	Significant	High	High
Multiple	External Client	N/A	Significant	Critical	Critical
Single	External Client	N/A	Significant	High	High
Partial outage of a Critical Business Applications & Services NOT impacting a least one Critical function.					
Significant amount of	Internal User	Mobile	Moderate	Critical	High
Insignificant amount of	Internal User	Mobile	Moderate	High	Medium
Negligible amount of	Internal User	Mobile	Moderate	Medium	Low
Significant amount of	Internal User	Designated Site(s)	Moderate	Critical	High
Insignificant amount of	Internal User	Designated Site(s)	Moderate	High	Medium
Negligible amount of	Internal User	Designated Site(s)	Moderate	Medium	Low
Significant amount of	Internal User	Non-Designated Site(s)	Moderate	High	Medium
Insignificant amount of	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
Negligible amount of	Internal User	Non-Designated Site(s)	Moderate	Low	Low
Large number amount of	Public User	N/A	Moderate	Critical	High
Small number amount of	Public User	N/A	Moderate	High	Medium
Multiple	External Client	N/A	Moderate	Critical	High
Single	External Client	N/A	Moderate	High	Medium
DEGRADED PERFORMANCE					
Degraded performance of one or more Critical Business Applications & Services.					
N/A	Internal User	Mobile	Moderate	Medium	Low
N/A	Internal User	Designated Site(s)	Moderate	Medium	Low
N/A	Internal User	Non-Designated Site(s)	Moderate	Low	Low
Any	Public User	N/A	Moderate	Medium	Low
Multiple	External Client	N/A	Moderate	Critical	High
Single	External Client	N/A	Moderate	High	Medium
Limited or No impact					
Unexpected results produced by a Critical Business Application & Service.					
N/A	Any	N/A	Significant	High	High
Failure of redundant infrastructure not affecting service availability.					
N/A	Any	N/A	Moderate	High	Medium
Single user impacted.					
Single	Internal User	N/A	Minor	Low	Low
Single	Public User	N/A	Minor	Low	Low

PRODUCTION					
IMPACTING	WHO	WHERE	IMPACT LEVEL	URGENCY LEVEL	PRIORITY
FULL outage					
Full outage of a non Critical Business Applications & Services.					
All	Internal User	Mobile	Significant	High	High
All	Internal User	Designated Site(s)	Significant	High	High
All	Internal User	Non-Designates Site(s)	Significant	Medium	Medium
All	Public User	N/A	Significant	High	High
All	External Client	N/A	Significant	High	High
Full outage of non-Production Environment.					
Multiple	Partner	N/A	Significant	High	High
Single	Partner	N/A	Significant	Medium	Medium
PARTIAL outage					
Partial outage of a non Critical Business Applications & Services.					
Significant amount of	Internal User	Mobile	Moderate	High	Medium
Insignificant amount of	Internal User	Mobile	Moderate	Medium	Low
Negligible amount of	Internal User	Mobile	Moderate	Low	Low
Significant amount of	Internal User	Designated Site(s)	Moderate	High	Medium
Insignificant amount of	Internal User	Designated Site(s)	Moderate	Medium	Low
Negligible amount of	Internal User	Designated Site(s)	Moderate	Low	Low
Significant amount of	Internal User	Non-Designated Site(s)	Moderate	High	Medium
Insignificant amount of	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
Negligible amount of	Internal User	Non-Designated Site(s)	Moderate	Low	Low
Large number amount of	Public	N/A	Moderate	High	Medium
Small number amount of	Public	N/A	Moderate	Medium	Low
Multiple	External Client	N/A	Moderate	Critical	High
Single	External Client	N/A	Moderate	High	Medium
Partial outage of non-Production Environment.					
Multiple	Partner	N/A	Moderate	High	Medium
Single	Partner	N/A	Moderate	Medium	Low
DEGRADED PERFORMANCE					
Degraded performance of one or more Critical Business Applications & Services.					
N/A	Internal User	Mobile	Minor	Low	Low
N/A	Internal User	Designated Site(s)	Minor	Low	Low
N/A	Internal User	Non-Designated Site(s)	Minor	Low	Low
Any	Public	N/A	Minor	Medium	Low
Multiple	External Client	N/A	Minor	Critical	Medium
Single	External Client	N/A	Minor	High	Medium
Any degraded performance of non-Production Environment.					
Multiple	Partner	N/A	Minor	High	Medium
Single	Partner	N/A	Minor	Medium	Low
Limited or No impact					
Unexpected results produced by a non Critical Business Application & Service.					
N/A	Any	N/A	Moderate	High	Medium
Failure of redundant infrastructure not affecting service availability.					
N/A	Any	N/A	Moderate	High	Medium
Single user impacted.					
Single	Internal User	N/A	Minor	Low	Low
Single	Public User	N/A	Minor	Low	Low

NON-Critical Business APPLICATION and SERVICE (NON-CBAS)

PRODUCTION

Network

IMPACTING	WHO	WHERE	IMPACT LEVEL	URGENCY LEVEL	PRIORITY
FULL outage					
Full service outage due to loss of network connectivity or loss of power/hydro at a Data Centre.					
N/A	Any	N/A	Extensive	Critical	Critical
Full service outage due to loss of a vendor managed network connectivity or loss of power/hydro at a site(s).					
N/A	Internal User	Designated Site(s)	Significant	High	High
N/A	Internal User	Non-Designated Site(s)	Significant	Medium	Medium
Full service outage due to loss of a SSC managed network connectivity .					
N/A	Internal User	Designated Site(s)	Extensive	High	Critical
N/A	Internal User	Non-Designated Site(s)	Extensive	Medium	High
Full outage of WIFI network connectivity when LAN network connectivity is unavailable.					
N/A	Internal User	Designated Site(s)	Significant	High	High
N/A	Internal User	Non-Designated Site(s)	Significant	Medium	Medium
Full outage of WIFI network connectivity when LAN network connectivity is available.					
N/A	Internal User	Designated Site(s)	Moderate	High	Medium
N/A	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
PARTIAL outage					
Partial service outage due to loss of network connectivity or loss of power/hydro at a Data Centre.					
N/A	Any	N/A	Significant	High	High
Partial service outage due to loss of a vendor managed network connectivity or loss of power/hydro at a site(s).					
N/A	Internal User	Designated Site(s)	Moderate	High	Medium
N/A	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
Partial service outage due to loss of a SSC managed network connectivity.					
N/A	Internal User	Designated Site(s)	Significant	High	High
N/A	Internal User	Non-Designated Site(s)	Significant	Medium	Medium
Partial outage of WIFI network connectivity					
N/A	Internal User	Designated Site(s)	Moderate	High	Medium
N/A	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
DEGRADED PERFORMANCE					
Degraded performance due to loss of network connectivity or loss of power/hydro at a Data Centre.					
N/A	Any	N/A	Moderate	High	Medium
Degraded performance due to loss of a vendor managed network connectivity or loss of power/hydro at a site(s).					
N/A	Internal User	Designated Site(s)	Minor	Medium	Low
N/A	Internal User	Non-Designated Site(s)	Minor	Low	Low
Degraded performance due to loss of a SSC managed network connectivity.					
N/A	Internal User	Designated Site(s)	Moderate	High	Medium
N/A	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
Degraded performance of WIFI network connectivity					
N/A	Internal User	Designated Site(s)	Minor	High	Medium
N/A	Internal User	Non-Designated Site(s)	Minor	Medium	Low
Limited or No impact					
Network connection failed over to backup connection without any degradation in performance at a site(s).					
N/A	Internal User	Designated Site(s)	Minor	Medium	Low
N/A	Internal User	Non-Designated Site(s)	Minor	Low	Low

PRODUCTION

Facility

IMPACTING	WHO	WHERE	IMPACT LEVEL	URGENCY LEVEL	PRIORITY
FULL outage					
Full service outage due to loss of power/hydro at a Data Centre.					
N/A	Any	N/A	Extensive	Critical	Critical
Full service outage due to loss of power/hydro at a site(s).					
N/A	Internal User	Designated Site(s)	Significant	High	High
N/A	Internal User	Non-Designated Site(s)	Significant	Medium	Medium
Full outage of commercial/backup power (i.e. generators, UPS, etc...) at a Data Centre.					
N/A	N/A	N/A	Extensive	Critical	Critical
Full outage of cooling equipment at a Data Centre.					
N/A	N/A	N/A	Extensive	Critical	Critical
PARTIAL outage					
Partial service outage due to loss of power/hydro at a Data Centre.					
N/A	Any	N/A	Extensive	Critical	Critical
Partial service outage due to loss of power/hydro at a site(s).					
N/A	Internal User	Designated Site(s)	Moderate	High	Medium
N/A	Internal User	Non-Designated Site(s)	Moderate	Medium	Low
Partial outage of commercial/backup power (i.e. generators, UPS, etc...) at a Data Centre.					
N/A	N/A	N/A	Moderate	Critical	High
Partial outage of cooling equipment at a Data Centre.					
N/A	N/A	N/A	Moderate	Critical	High
DEGRADED PERFORMANCE					
Degraded performance due to loss of power/hydro at a Data Centre.					
N/A	Any	N/A	Moderate	Critical	High
Degraded performance due to loss of power/hydro at a site(s).					
N/A	Internal User	Designated Site(s)	Minor	Medium	Low
N/A	Internal User	Non-Designated Site(s)	Minor	Low	Low
Degraded performance of commercial/backup power (i.e. generators, UPS, etc...) at a Data Centre.					
N/A	N/A	N/A	Moderate	Critical	High
Degraded performance of cooling equipment at a Data Centre.					
N/A	N/A	N/A	Moderate	Critical	High
Limited or No impact					
Operational Health and Safety (i.e Spills, Accidents, Flooding, Security Breach)					
N/A	N/A	N/A	Moderate	Critical	High
Degraded performance of commercial/backup power (generators, UPS, etc...) with confirmed no risk to facility					
N/A	N/A	N/A	Minor	Low	Low
Degraded performance of cooling equipment with confirmed no risk to facility					
N/A	N/A	N/A	Minor	Low	Low

NON-PRODUCTION						
IMPACTING	WHO	WHERE	IMPACT LEVEL	URGENCY LEVEL	PRIORITY	
FULL outage						
Full outage of an identified Critical Business Applications & Services.						
All	Internal User	N/A	Moderate	High	Medium	
All	External Client	N/A	Moderate	High	Medium	
PARTIAL outage						
Partial outage of a Critical Business Applications & Services impacting one or more Critical functions.						
Significant amount of	Internal User	N/A	Moderate	High	Medium	
Insignificant amount of	Internal User	N/A	Moderate	High	Medium	
Negligible amount of	Internal User	N/A	Moderate	Medium	Low	
Multiple	External Client	N/A	Moderate	High	Medium	
Single	External Client	N/A	Moderate	High	Medium	
Partial outage of a Critical Business Applications & Services NOT impacting a least one Critical function.						
Significant amount of	Internal User	N/A	Minor	High	Medium	
Insignificant amount of	Internal User	N/A	Minor	Medium	Low	
Negligible amount of	Internal User	N/A	Minor	Low	Low	
Multiple	External Client	N/A	Minor	High	Medium	
Single	External Client	N/A	Minor	Medium	Low	
DEGRADED PERFORMANCE						
Degraded performance of one or more Critical Business Applications & Services.						
N/A	Internal User	N/A	Minor	Low	Low	
Multiple	External Client	N/A	Minor	High	Medium	
Single	External Client	N/A	Minor	Medium	Low	
Limited or No impact						
Unexpected results produced by a Critical Business Application & Service.						
N/A	Any	N/A	Minor	High	Medium	
Failure of redundant infrastructure not affecting service availability.						
N/A	Any	N/A	Minor	Low	Low	
Single user impacted.						
Single	Internal User	N/A	Minor	Low	Low	

NON-PRODUCTION						
IMPACTING	WHO	WHERE	IMPACT LEVEL	URGENCY LEVEL	PRIORITY	
FULL outage						
Full outage of a non Critical Business Applications & Services.						
All	Internal User	N/A	Minor	High	Medium	
All	External Client	N/A	Minor	High	Medium	
PARTIAL outage						
Partial outage of a non Critical Business Applications & Services.						
N/A	Internal User	N/A	Minor	Medium	Low	
Multiple	External Client	N/A	Minor	High	Medium	
Single	External Client	N/A	Minor	Medium	Low	
DEGRADED PERFORMANCE						
Degraded performance of one or more Critical Business Applications & Services.						
N/A	Internal User	N/A	Minor	Low	Low	
N/A	External Client	N/A	Minor	Medium	Low	
Limited or No impact						
Unexpected results produced by a non Critical Business Application & Service.						
N/A	Any	N/A	Minor	Medium	Low	
Failure of redundant infrastructure not affecting service availability.						
N/A	Any	N/A	Minor	Low	Low	
Single user impacted.						
Single	Internal User	N/A	Minor	Low	Low	

Critical Business APPLICATION and SERVICE (CBAS)

NON-Critical Business APPLICATION and SERVICE (NON-CBAS)

TERMINOLOGY AND DEFINITIONS

Full Outage	<ul style="list-style-type: none"> ▪The impacted application/service is unavailable. ▪The site(s) have no connectivity in the case of network service outage. ▪The application/service performance is degraded to a level where business impact is severe. ▪The site(s) have no power in the case of power/hydro outage.
Partial Outage	<ul style="list-style-type: none"> ▪One or more functions of the impacted application/service is unavailable. ▪The impacted application/service is partially available to users, including intermittency. ▪The application/service performance is degraded to a level where business impact is considerable. ▪The site(s) have intermittent external connectivity due to network or power/hydro problems.
Degraded Performance	<ul style="list-style-type: none"> ▪All of the functions of the impacted application/service is operational, however, the performance is slower than normal. ▪Although performance may be slow, business impact is minimal. ▪Business activities can still be performed with slower than normal performance. (Thresholds may need to be defined, however, common sense prevails in most cases)
Limited or No impact	<ul style="list-style-type: none"> ▪Impacts only a single user. ▪Failure of a redundant infrastructure.

Severe	Degree of impact is extremely damaging or widespread in scope. Very high risk level.
Considerable	Degree of impact is damaging or large in scope. High risk level.
Significant	A number of internal users high enough to cause considerable impact to the business.
Insignificant	A number of internal users low enough to cause a manageable impact to the business.
Negligible	A limited number of internal users causing a minimal to no impact to the business.
Single	A single internal user causing no impact to the business.
Large number of	A number of public users high enough to cause considerable impact to public confidence or corporate reputation.
Small number of	A number of public users low enough to cause a manageable impact to public confidence or corporate reputation.
SSC Partner	Other government department that SSC provides services to. (examples: CRA, CBSA, ESDC, IRCC, RCMP, PSPC, PCH, etc.)
Vendors	Third-party suppliers from whom SSC gets products and services. (examples: Bell, Telus, Allstream, BlackBerry, IBM, McAfee, etc.)
External Clients	Other non Canadian Government businesses that depend on and/or make use of services offered by SSC or Partners.
Public user	Canadian Citizens
Internal user	SSC and Partner Employees (includes: employees/contractors/students)
Site	Physical location, Buildings (not to be confused with Web sites)
Unexpected results	Application Data (not system files) that the Partner is responsible for, showing unexpected results, but application is fully functional.
Mobile	Blackberry (BB10), MTDi, Secure Remote Access (SRA).
Non-Production Environment	Refers to the non-production infrastructures as a whole (service offered by SSC) as opposed to the applications and services themselves.