Government Contact Centre Services (GCCS) Stream 2: Contact Centre as a Service (CCaaS)

Statement of Work Template

Table of Contents

Index of Tables

1 PROJECT MANAGEMENT

(1) The requirements in this section apply to any Work for Service Readiness, Security and Privacy Readiness, Value Added Services, Subscription Service Subscription Service Configuration and Subscription Service Integration in accordance with Service Orders issued for Professional Services..

1.1 Work Project

(2) When and as requested by Canada, the Contractor must conduct and complete portions of the Work as a Work Project.

(3) The Contractor must begin the Work identified by Canada as a Work Project within 10 FGWDs of the request by Canada.

1.1.1 Work Project Meetings

(4) The Contractor must facilitate a weekly meeting for each Work Project (Work Project Meeting) that includes a presentation to review the Work Project Status Report.

(5) The Contractor must facilitate a weekly meeting to review all Work Projects that includes a presentation to review the Project Management Office (PMO) Status Report.

1.1.2 Work Project Reporting

(6) The Contractor must provide the reports for Work Projects in Table 1.

Table 1. Work Project Reports

Report Name	Work Project Status Report
Frequency	2 FGWDs prior to each Work Project Status Meeting
Purpose	The report must present the status of a Work Project.
Description	The report must include: a) minutes from the previous Work Project Review Meeting; b) action items; c) view of Project Schedule milestones; d) current and upcoming Work tasks; e) project issues including assessment of impacts and current escalation status; f) summary of Work Project risks; and g) summary with description of the Project Change Requests.
Report Name	Project Management Office (PMO) Status Report
Frequency	2 FGWDs prior to each PMO Meeting
Purpose	The report must present an overall summary of all Work Projects.
Description	The report must include: a) minutes from the previous PMO Meeting;

	b) action items; c) summary of top 5 issues; and d) view of Master Project Schedule milestones.

1.2 Project Change Requests

(7) The Contractor must create and maintain a log of Project Change Requests for each Work Project and master log for all Work Projects where the format of the log is developed in consultation with Canada and approved by Canada.

(8) The Contractor must review each Project Change Request in consultation with Canada and assess the impacts.

(9) The Contractor must update the Project Schedule if a Project Change Request affects any task or timeline in the Work Project.

(10) Canada is not required to issue a Project Change Request for new Work Projects. The re-allocation of Work between existing Work Projects or between existing Work Projects and new Work Projects will be done in consultation with the Contractor.

1.3 Project Risk Register

(11) The Contractor must create and maintain a Project Risk Register for each Work Project and a master register that summarizes the risks for all Work Projects where the format of the register is developed in consultation with Canada and approved by Canada...

1.4 Project Schedule

(12) The Contractor must create and maintain a Project Schedule for each Work Project and a master schedule that summarizes the Project Schedules for all Work Projects where the format of the schedule is developed in consultation with Canada and approved by Canada.

(13) .A Project Schedule must:

a) not create dependencies on Canada's review and acceptance of Work, unless approved by Canada;

b) limit dependencies to the maximum extent possible;

c) schedule tasks in parallel to the maximum extent possible;

d) provide for deliverables to be submitted progressively (i.e. not all at once);

e) be produced and maintained in Microsoft Project;

f) identify the phases, gates, tasks, deliverables and milestones of the Work including:

g) identify any Project Change Requests that cause changes to the completion date of any major milestone, with numbers assigned that correlate with the numbers assigned to them in the Work Project Status Report.

(14) The Contractor must set a baseline for all task start and end dates in a Project Schedule based on the date of acceptance of the Project Schedule by Canada.

(15) The Contractor must not change the baseline of a Project Schedule for the duration of the Work Project unless approved by Canada. If a change to the Project Schedule is approved by Canada, the Contractor must set a new baseline schedule in a new version of the Project Plan that clearly states that the baseline has been revised.

(16) The Contractor must ensure that resource assignments for a Project Schedule take into consideration the availability and non-availability of each resource (e.g. holidays, training and vacation), such that there is no impact to the completion of Work in the Work Project.

1.5 Project Resource Plan

(17) The Contractor must create and maintain a Project Resource Plan for each Work Project that includes:

a) roles and responsibilities of all resources (primary and backup Key Resources, other resources to the Manager level) to complete the Work for the Work Project including:

i) name and title of the resource;

ii) description of the qualifications of the resource to complete the Work; and

iii) work level allocation (dedicated, part time);

b) a Responsible, Accountable, Consulted, and Informed (RACI) chart to identify the Work by deliverable and Work activities to be completed by each resource, Canada and Client stakeholders to the manager level;

c) a description of the management escalation process (org chart with names and contact information for all resources on the Work Project).

(18) The Contractor must create and maintain a master Project Resource Plan that summarizes the Project Resource Plans for all Work Projects.

2 DOCUMENTATION

(19) The Contractor must define the content and format of documents for Work Deliverables in:

a) in consultation with Canada and subject to Canada's acceptance;

b) English, and in French when requested by Canada;

c) the native format (e.g. Word, Excel, Visio) and in PDF in a format. Where the diagrams are embedded within another document format (e.g. Word), the diagrams must be in a metafile format (not editable) to reduce the size of the documents;

(20) The Contractor must provide all diagrams used for a Work Deliverable as native Visio diagrams to Canada within 5 FGWDs of a request from Canada.

(21) The Contractor must provide user guides, training materials and OEM documentation in both English and French.

(22) The Contractor must ensure that all documentation is kept current and up-to-date at all times.

(23) The Contractor must not make any changes (format, content provided) to an approved Work Deliverable without following the Request Fulfillment processes.

(24) The Contractor must provide an updated Work Deliverable (text and diagrams) to Canada within 20 FGWDs of a request by Canada that reflects all changes to the document in associated Service Requests since the last version of the document.

3 MEETINGS

(25) Meetings must be conducted during business hours (8 am to 5 pm ET) on FGWDs.unless otherwise approved by Canada.

(26) The Contractor must provide agendas for all meetings prior to the meeting (excluding daily meetings) unless otherwise approved by Canada.

(27) Except where Canada specifies otherwise, for each meeting attended by the Contractor, the Contractor is responsible for:

a) coordinating with Canada;

b) coordinating any subcontractor participation (if necessary);

c) providing the minutes, schedules, lists, tests, design analysis and any other pre- and post-review data as appropriate;

d) ensuring that qualified Contractor personnel with knowledge of the issues to be discussed attend the meeting; and

e) ensuring the Contractor personnel representatives have sufficient authority to make expeditious decisions on behalf of the Contractor.

(28) The Contractor must prepare minutes for each meeting during the meeting and review with Canada at the end of the meeting where format for minutes is developed in consultation with Canada and approved by Canada.

4 SECURITY AND PRIVACY READINESS

(29) The Work in this subsection must be completed by the Contractor and accepted by Canada for the Security and Privacy Readiness deliverable at no additional cost to Canada.

4.1 Cloud Guardrail Assessment

(30) The Contractor must complete the Cloud Guardrail Assessment within 30 calendar days following the issuance of the Contract that includes Canadas time to review and assess evidence provided by the Contractor that the cloud guardrails specified at https://github.com/canada-ca/cloud-guardrails have been implemented for the Subscription Service.

(31) Where Canada exceeds 2 FGWDs to assess evidence and provide feedback, Canada will solely determine if the Contractor will be provided with additional time (calendar days) to complete the Cloud Guardrail Assessment.

4.2 Security Assessment

(32) The Contractor must complete a First Party Security Assessment OR a Third Party Security Assessment, as selected by the Contractor, in accordance with the Annex A Security Controls (separate attachment).

4.2.1 First Party Security Assessment

(33) The Contractor must provide Canada with a ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements certification and a ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services and a SOC 2 Type II report completed within the last 12 months of the Contract date.

4.2.2 Third Party Security Assessment

(34) The Contractor must complete a security assessment with an independent third party assurer, qualified under AICPA or CPA Canada and/or an ISO certification regime that conforms to ISO/IEC 17020 quality management system standards, at no additional cost to Canada that will prepare a Security Assessment Report that includes:

a) the legal business name of the Contractor;

b) current date and/or status of certifications and/or SOC 2 Type II report;

c) evidence to demonstrate compliance of the Service with Annex A-5 Security Requirements and other security requirements in the Contract;

d) name and address of the third party assurer that performed the security assessment; and

e) evidence that the third party assurer is qualified under AICPA or CPA Canada, and/or ISO certification regime that conforms to ISO/IEC 17020 quality management system standard.

4.3 Plan of Actions and Milestones

(35) The Contractor must provide a Plan of Actions and Milestones for Canada's approval within 20 FGWDS of a request from Canada that:

a) documents the remedial actions planned by the Contractor to correct security deficiencies identified during the Cloud Guardrail Assessment and Security Assessment and in any subsequent SOC2 Type II report or ISO re-certification; and

b) includes a Project Schedule to complete the remedial actions; and

(36) The Contractor must update the Plan of Actions and Milestones based on the results from security assessments, security impact analyses, and security monitoring activities conducted by the Contractor.

(37) The Contractor must implement the remedial actions identified in the Plan of Actions and Milestones in accordance with the Project Schedule for the initial approved version and any subsequent versions.

4.4 System Security Plan

(38) The Contractor must provide a System Security Plan (SSP) that documents the security controls in place, or planned for meeting, for the security requirements in the contract that:

a) Is consistent with the Contractor's enterprise architecture;
b) explicitly defines the authorization boundary for the Service;
c) describes relationships with or connections to other External Information Systems;
d) provides an overview of the Security Control Requirements for the Service;
e) describes the rationale for security controls including the tailoring and supplementation decisions; and
f) includes a component diagram that clearly shows the Services architecture.

4.5 Operations Security Procedures

(39) The Contractor must provide a Operations Security Procedures (OSP) that documents the following for each connection to a Service:

a) system components;
b) the interface characteristics;
c) security requirements;
d) nature of the information communicated;
e) secure configuration, installation, and operation of the Service;
f) effective use and maintenance of security functions;
g) known Security Vulnerabilities regarding configuration and use of administrative (i.e. privileged) security functions;
h) user-accessible security functions and how to effectively use those security functions;
i) methods for user interaction, which enables individuals to use the CCaaS service in a more secure manner; and
j) user responsibilities for maintaining the security of the CCaaS service and system components..

4.6 Service Incident Response Plan

(40) The Contractor must provide a Security Incident Response Plan that includes:

a) how the Contractor plans to identify, report, and escalate Security Incidents;
b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery;
c) a description of the structure and organization of the Security Incident response capability;
d) a high-level approach for how the Security Incident response capability fits into the Contractor's overall organization;
e) a definition of reportable Security Incidents;
f) a definition of metrics for measuring the Security Incident response capability; and
g) a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.

4.7 Service Contingency Plan

(41) The Contractor must provide a Service Contingency Plan that describes:

a) essential missions and business functions including supporting critical CCaaS system components and associated contingency requirements;
b) a detailed plan and documented processes for restoring Service operations;

c) back up strategies for datacentre facilities, network facilities, operational support systems and data, and key Service components;
d) recovery objectives, restoration priorities, and metrics as per Service Level Agreements (SLAs);
e) contingency roles, responsibilities, and assigned individuals with contact information;
f) process for full Service restoration without deterioration of the security safeguards originally planned and implemented;
g) how essential missions and business functions are maintained despite a Service disruption, compromise, or failure;
h) process(es) for testing the Service Contingency Plan;
i) detailed communications plans with Canada, Canada's Clients and the Contractor's suppliers and sub-contractors;
j) detailed plan and processes for transferring operational, management and administration functionality to a backup operations centre; and
k) steps the Contractor will take if any of its key subcontractors go out of business or are identified by Canada as being subject to security concerns

(42) The Contractor must implement Service Contingency Plan (all processes, procedures, roles, responsibilities etc.) following its acceptance by Canada and prior to completion of Service Readiness.

4.8 Privacy Management Plan

(43) The Contractor must provide a Privacy Management Plan to Canada that includes:
a) the roles and responsibilities of the Contractor's Privacy resources and how they interface with Canada and Contractor's suppliers;
b) a description of how the Contractor plans to develop and maintain overall privacy awareness on an ongoing basis through various channels (intranet, posters etc.);
c) a description of the Contractor's privacy protection strategies detailing exactly how the Personal Information will be treated over its life cycle;
d) a description of how the Contractor intends to ensure that its staff is trained on privacy and privacy;
e) a description of how the Personal Information will be collected, used, retained, and disclosed only for the purposes of the Work specified in the Contract;
f) a description of how the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;
g) processes for the development and testing of Services without using Canada production data (i.e. real information related to Users);
h) processes to identify, document, review, report, respond, and escalate privacy related Incidents;
i) processes for managing, accessing, collecting, using, disclosing, receiving, creating or disposing of personal information;
j) processes for limiting the retention of personal information and ensuring adherence to the retention requirements of Canada, including backup and archiving of data;
k) role-based access controls to restrict/limit access to operational and administrative information required by authorized Contractor personnel including logging all instances where personnel have had access to operational information;
l) processes to ensure incorporation of specific retention and disposal requirements as determined by Canada's Privacy Impact Assessments (PIA's); and
m) processes to ensure the logging and data capture settings of the information protection and network monitoring devices are appropriately defined to limit the collection of personal information;
n) process for dealing with requests for access to Records under the Access to Information Act and requests for access to Personal Information under the Privacy Act (Access Requests).
o) the privacy breach protocol, and details on how any privacy breaches will be handled;

p) any new measures the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification; and

q) how the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification..

4.9 Privacy Impact Assessment

(44) The Contractor must assist Canada in creating the privacy impact assessment for the Subscription Service in accordance with the TBS Directive on privacy impact assessment (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308).

(45) In particular, with respect to any information that Canada identifies as Personal Information during the Contract Period, the Contractor must provide the following information within 20 FGWDs of a request by the Contracting Authority:

a) business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;

b) a list of the Personal Information used by the Contractor in connection with the Work and the purpose of how each Personal Information item is used by the Contractor in connection with the Work;

c) how the Personal Information is shared and with whom;

d) a list of all locations where hard copies of Personal Information are stored;

e) a list of all locations where Personal Information in machine-readable format is stored (e.g., the location where any server housing a database including any Personal Information is located), including back-ups;

f) a list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by the Contract;

g) any privacy-specific security requirements or recommendations that need to be addressed;

h) a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

i) results of consultations (if any) from a privacy impact assessment review by the Office of the Privacy Commissioner of Canada (OPCC) with signoff by the OPCC.

j) The Contractor must implement recommendations from the privacy impact assessment based on a schedule approved by Canada at no cost to Canada.

k) If changes to Services are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by Canada, the Contractor must provide Canada with sufficient detail on the changes to support an update to the privacy impact assessment, and obtain approval from the Contracting Authority for the anticipated change.

l) The Contractor must provide a privacy awareness communications kit to Contractor resources involved in Services that provides an overview on the use of Personal Information.

5 SERVICE OPERATIONS

(46) The Work in this subsection is applicable to the ongoing operation, administration, management and maintenance of the CCaaS, with the objective of proactively diagnosing and repairing problems before these become service affecting and is included with the Subscription Service unless otherwise indicted in the SOW as requiring a Work Request Notice (WRN).

5.1 Service Desk

(47) The Contractor must provide a Service Desk that performs the following functions:

a) acting as the primary point of contact for Incidents reported by Canada 24 hours per day, 7 days per week, 365 days per year;
b) answering and continuing the subsequent Level 1 and Level 2 dialogue using the official language of Canada (French, English) requested by the caller;
c) interacting with Canada's representatives as designated by Canada's Service Desk;
d) providing a unique and dedicated toll-free telephone number (e.g., 1-800 number) for Canada's authorized representatives to access the Service Desk; and
e) providing a single email address for Canada's authorized representatives to access the Service Desk.

5.2 Operational Service Management

When requested by Canada in a Work Request Notice (WRN), the Contractor must provide 1 dedicated Engineer to provide 24 hours, 7 days per week operations support for:

a) providing general guidance/bestpractice adherence for the configuration and operation of the platform;
b) planned back log activities;
c) performing move, add, change, delete (MACD) functions;
    d) users, stations, workgroups, roles, ACDs, account codes, skills, schedules etc
i) performing configuration enhancements and modification;
j) adding or modifying call flows;
k) coordinating requirement gathering discussions;
l) coordinating formal work order delivery and project execution;
m) project related change control activity;
n) participating in production migration activity and operational handoff;
o) updating operational documentation;
p) management of incident tickets:
    i) troubleshooting and incident triage;
    ii) collection of logs and additional supporting information;
    iii) communication with point of contact for the ticket;
    iv) escalation of issues to higher tier support;
    v) coordination to transition high priority incidents to the Care team;
    vi) participation in calls for P1 and P2 incidents;
    vii) ensure delivery of root cause analysis for all P1 and P2 incidents;
    viii) coordination with Care team to ensure root cause analysis for P3/P4 incidents are provided when requested by Customer;
q) perform daily health checks;
r) real time resolution of issues discovered during health checks;

s) adhoc and historical reporting;

5.3 Service Operations Meetings

(48) The Contractor must facilitate and conduct the Service Review meetings summarized in Table 2Table 2.

Table 2. Service Review Meetings

Meeting Name	Service Management Review Meeting
Frequency	Monthly, or as requested by Canada
Purpose	Review of Incidents, Change Requests, Service Requests, Problems, Service Level Targets and Billing/Invoicing.
Description	The meeting must include a review of: a) issues log from previous meeting; b) action items log from previous meeting; c) Post-Service Request Reports from the previous month; d) Post-Change Request Reports from the previous month; e) Post-Incident Reports from the previous month; f) Service Level Targets and failures from the previous month; g) Service Requests scheduled for the coming month; h) Change Requests scheduled for the coming month; i) issues that have or may affect Service performance; and j) root cause analysis of open Incident Tickets.
Meeting Name	Security Review Meeting
Frequency	Within 1 FGWD of a request by Canada
Purpose	Review of Security Incidents
Description	The meeting must include a review of (for each Security Incident): a) date/time and duration of Security Incident; b) description including whether attack appears to have been successful; c) scope (Service Portal; single or multiple Clients, etc.); d) estimated injury/impact level; e) list of known and suspected Applications affected; f) actions taken; g) apparent source/origin of attack(s); and h) status of mitigations.

5.4 IT Service Management

(49) The Contractor must provide IT Service Management for Services, as described in the following subsections, 24 hours per day, 7 days per week and 365 days per year.

5.4.1 Change Management

(50) The Contractor must create a Change Request for any change that may disrupt Services.

(51) The Contractor must create 1 or more Change Request Tickets for a Change Request.

(52) The Contractor must create an Emergency Change Request for each mitigation measure required to contain a Security Incident.

(53) The Contractor must complete Change Request activity, excluding Emergency Change Requests, in maintenance windows. This includes the outage time to complete the Change Request and any outage time required for back-out of the Change Request. Any outage that extends beyond the maintenance window will be treated as the Service being unavailable and this outage period must be taken into account in the calculation of Service Level Target Service Availability (SLT-SA) and Service Level Target Maximum Time to Restore Service (SLT-MTRS). In such a case, the Contractor must initiate an Incident Ticket and record the time beyond the approved maintenance window as outage time for the Service.

(54) If the execution of a Change Request causes an unplanned impact or outage to a Service, or it is determined that it will exceed the maintenance window approved by Canada, the Contractor must contact Canada immediately. The Contractor must provide a detailed explanation of the impacts and the plan to restore the Service or complete the Change Request as quickly as possible. The Contractor must also initiate an Incident Ticket for any outage not identified in the Change Request.

(55) Any outage to a Service that occurs as a result of an Emergency Change Request initiated by the Contractor will be treated as the Service being unavailable.

(56) The Contractor must enter information in the Change Request Ticket log for a failed Change Request explaining the failure, what the current status is for the environment that was subject to the Change Request and what partial changes were implemented.

(57) The Contractor must provide a Post-Change Request Report to Canada within 5 FGWDs of a failed Change Request.

5.4.2 Request Fulfillment

(58) The Contractor must use Change Management for all changes required for a Service Request.

(59) The Contractor must create 1 or more Service Request Tickets for each Service Request submitted by Canada.

(60) The Contractor must update a Service Request Ticket following a change in Work associated with the Service Request.

(61) The Contractor must provide a Post-Service Request Report to Canada following a failed Service Request.

5.4.3 Release Management

(62) The Contractor must use Change Management for all changes required for a Service Release.

(63) The Contractor must not use Services in production to test a Service Release prior to any changes.

(64) The Contractor must provide a Post-Service Release report to Canada following a failed Service Release that includes a Service Release that:

a) had to be backed out;

b) that caused disruption to the Services, or

c) did not achieve the Contractor's objective and therefore may need to be repeated at a later date.

5.4.4 Event and Incident Management

(65) The Contractor must proactively monitor Services for Incidents 7 days per week, 24 hours per day, 365 days per year.

(66) The Contractor must co-operatively work with Canada, Clients and any other third parties identified by Canada to resolve Incidents.

(67) The Contractor must open an Incident Ticket after detecting an Incident or receiving a notice from Canada reporting an Incident.

(68) The Contractor must update the Incident Ticket log following a change in status for the Incident.

(69) The Contractor must assign the highest priority to Incidents for Applications specified by Canada.

(70) The Contractor must provide Canada with an operational escalation matrix and a management escalation matrix for Incidents that:

a) defines the primary contact for each level of escalation;

b) defines the alternates (of equal authority) for each level of escalation; and

c) contains clear instructions for contacting the primary and alternate escalation authority.

(71) The Contractor must categorize and assign Incidents with a priority level

(72) The Contractor must notify Canada of Incidents, with priority levels specified by Canada,.

(73) The Contractor must provide an estimated time for resolution within the Incident Ticket.

(74) The Contractor must resolve Incidents by taking appropriate action to repair and restore Services as quickly as possible in accordance with the SLT-SA associated with the affected Services.

(75) The Contractor must document in the Incident Ticket activity log all:

a) management and technical escalations for Incidents;

b) interactions with third parties;

c) investigation, troubleshooting and analysis details, resolution activities and communications for Incidents

(76) The Contractor must track and report the outage time of each Incident in the associated Incident Tickets.

(77) The outage time for an Incident must start at the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada, whichever occurs first.

(78) The outage time for an Incident ends at the time that the affected Services are fully restored in relation to that Incident.

(79) The Contractor must not alter the outage time for an Incident Ticket once the Incident Ticket has been closed.

(80) If an Incident Ticket is closed and a subsequent Incident occurs within 24 hours for the same Incident, the Contractor must re-open the original Incident or open a new Incident with a cross reference to the previous Incident, and calculate the outage time for the new Incident using the combined outage time of both Incidents, and record this time in the adjusted outage time field of the Incident Ticket.

(81) The Contractor must identify and document the causal factors (root causes) of all Incidents.

5.4.4.1 Security Incidents

(82) The Contractor must report all suspected or actual Incidents for Security Breaches.

(83) The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious emails) to contain a Security Breach, protect against cyber threats or address vulnerabilities.

(84) The Contractor must provide results of logs and audit records research associated with a Security Breach, based upon criteria specified by Canada, within 72 hours of a request by Canada.

(85) The Contractor must implement an audit and investigation process for Security Breaches that allows only specific, pre-authorized representatives of Canada to request and receive discrete access and information for the purposes of conducting security investigations.

(86) The Contractor must ensure the use of proper forensic procedures and safeguards for handling Security Breaches that includes:

a) the maintenance of a chain of custody for both the audit information, and

b) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.

(87) During a Security Incident, the Contractor must reduce the standard response time according to the priority of the Security Incident as specified by Canada..

5.4.5 Configuration Management

(88) The Contractor must perform Configuration Management that includes the configuration of the Services to meet the on-going operational requirements of the Services in accordance with Service Orders for Professional Services.

(89) The Contractor must develop, document, and maintain the current baseline configuration of the Services with traceability back to previous versions.

(90) The Contractor must ensure that only authorized Configuration Items are released and/or implemented for the Services.

(91) The Contractor must log each Configuration Item addition, removal or modification where each log entry in a configuration log file.

(92) The Contractor must maintain daily back-ups of the configuration data and store the most recent copies of the daily backups at an off-site location.

(93) The Subscription Service must allow a master tenant configuration whereby this configuration can be inherited and different business rules can be applied by each of the sub-tenants specified by Canada.

5.5 Security and Privacy

5.5.1 Ongoing Security Assessment

(94) The Contractor must provide a), and b) and c), on an annual basis:

a) a SOC2 Type 2 report;

b) evidence that demonstrates current certification for ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and

c) evidence that demonstrates current certification for ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

5.5.2 Service Contingency Plan

(95) The Contractor must ensure that the Service Contingency Plan is:

a) coordinated with organizational elements responsible for related plans including incident handling teams;

b) communicated and distributed to organizational elements involved with executing the plan; and

c) protected from unauthorized disclosure and modification.

(96) The Contractor must notify Canada immediately upon determining that a disaster or other emergency situation has occurred that affects Services. The notification must include the following information: a brief description, date/time, estimated restore time, and impacted SDPs.

(97) The Contractor must test Service Contingency Plan (all processes, procedures, roles, responsibilities etc.) annually as documented in the approved plan, and provide the test results to Canada within 20 FGWDs of completing the testing.

(98) The Contractor must restore Service functions as part of Service Contingency Plan testing. The restoration exercise must not be performed using production Services unless otherwise approved by Canada.

(99) The Contractor must correct any problems to Services identified during the testing of Service Contingency Plan within 60 FGWDs after completion of the testing.

(100) The Contractor must provide to Canada within 40 FGWDs of a Service Request, evidence not more than 12 months old (e.g., test results, evaluations, and audits, etc.) that Service Contingency Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Service Contingency requirements for Services.

5.5.3 Privacy Management Plan

(101) The Contractor must review the Privacy Management Plan annually and provide a report to Canada within 20 FGWDs of completing the review that summarizes the results of the review and proposed changes. The Contractor must update the Privacy Management Plan within 20 FGWDs of Canada's acceptance of the report.

(102) The Contractor must provide to Canada within 40 FGWDs of a request, evidence not more than 24 months old (e.g., test results, evaluations, and audits) that the Privacy Management Plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Canada's privacy management requirements.

(103) The Contractor must produce a Vulnerability Mitigation Report after completion of remediation activities completed for a Vulnerability Mitigation Plan that includes:

a) a description of the corrective measures implemented; and

b) proof that associated system documentation has been updated to reflect the changes.

(104) The Contractor must mitigate all security deficiencies found in accordance with Canada's security requirements at no additional cost to Canada as a result of vulnerability testing by the Contractor and Canada..

5.6 Reports and Documents

(105) It is Canada's intention to use existing reports provided by the Contractor where possible as determined by Canada. The exact reports will be determined during consultation with Canada before the completion of Service Readiness.

(106) The Contractor must provide reports in English using the ET time zone.

(107) Information in reports representing numbers and dates must be downloadable as numbers and dates, and not formatted as text.

(108) The Contractor must provide all annual reports within 30 FGWDs of the end of the previous 12 months, based on the anniversary of the Contract.

(109) The Contractor must provide all weekly reports within 2 FGWDs of the end of the previous week where the end of a week is 11:59 pm Friday.

(110) The Contractor must provide all monthly reports within 5 FGWDs of the end of the previous month where the end of a month is 11:59 pm on the last FGWD of the month.

(111) The Contractor must provide Canada with all reports provided to other clients of the Contractor for Services using Canada Data.

(112) The Contractor must provide the Service Operations reports summarized in Table 3 according to frequency, purpose, and description.

Table 3. Service Operations Reports

Report Name	Service Management Summary Report
Frequency	Scheduled, Monthly
Purpose	The report must present a summary of the Contractor's performance in delivering the services and meeting Service Level Targets (SLTs).
Description	The report must include: a) total number of Incidents and the total number of SLT exceptions for the monthly period; b) list of all Incidents for the monthly period organized by type, priority, and SLT, identifying Incident Ticket numbers and escalation levels invoked; c) list of SLT exceptions for the monthly period identifying the SLT for each exception and the amount by which the SLT was missed (applies to all types of SLT exceptions whether or not there is an associated Incident Ticket); d) description of the recommendations, corrective actions and timeframes to implement any required changes to resolve chronic Problems or service degradation and/or prevent future SLT exceptions; e) description of Incidents and issues related to the Contractor's services such as the Service Portal and its associated systems, tools and applications (e.g., CMDB, reporting, etc.), including the corrective actions and timeframes to resolve them; f) Service Requests completed/pending; g) Change Requests completed/pending
Report Name	Service Request and Change Request Report
Frequency	Scheduled, Monthly
Purpose	The report must present a detailed summary of all Service Requests planned or completed during the reporting period.
	The report must include: a) Service Requests closed for the weekly period b) Service Requests pending execution c) Change Requests closed for the weekly period, including the following: d) Change Requests pending execution, including the following:
Report Name	Post-Incident Report
Frequency	On-Demand, Within 2 FGWDs of Canada's request
Purpose	This report must provide Canada with an in-depth understanding of any Incident that Canada considers to have had a significant impact on its business. The report must clarify exactly what occurred during the Incident, including the Contractor's actions, as

	well as the Contractor's plans to address any potential recurrence.
Report Name	Post-Change Request Report
Frequency	On-Demand. The FGWD immediately following the execution of any Emergency Change Request and/or within 5 FGWDs of a failed Change Request or Service Release
Purpose	The report must provide Canada with an in-depth understanding of a failed Change Request, or an Emergency Change Request.
Report Name	Post-Service Request Report
Frequency	On-Demand, The FGWD immediately following the execution of any Emergency Service Request and/or within 5 FGWDs of a failed Service Request
Purpose	The report must provide Canada with an in-depth understanding of a failed Service Request, or an Emergency Service Request.
Report Name	Service Release Summary Report
Frequency	Scheduled, Monthly
Purpose	Summary of Service Release Activity
Description	The report must include, for each Service Release in the preceding month: a) time and date of the Service Release; b) purpose of the Service Release; c) description of Service Release activities; d) Enterprise Contact Centre Services components affected; and e) lessons learned (if Service Release failed).
Report Name	Service Ticket Report
Frequency	Real time, as required.
Purpose	A User-definable report that must provide access to Incident Tickets, Problem Tickets, Change Request Tickets and Service Request Tickets based on ticket type selected by Canada and any ticket field over a time period selected by the User..
Description	The report generator must provide: a) ability to search, sort and view tickets; b) ability to download ticket query results using a file naming convention specified by Canada and COTS file format; c) ability to view individual tickets (all fields) in a hierarchical tree fashion where information within a ticket can be viewed in a successive "drill-down" manner (i.e., related tickets) by selecting hyperlinks;

	d) cumulative report detailing for each ticket in the query results: the ticket number, date, priority, associated tickets (where applicable), impacted Enterprise Contact Centre Services, outage time, detailed description of ticket; e) direct access to the CIs from the CMDB involved by selecting a hyperlink in the ticket; and f) ability to generate open or closed ticket summary information, displayed in graphical and tabular format, by year, month, day and hour intervals for number of tickets, and number of tickets by priority level.
Report Name	Privacy Summary Report
Purpose	Personal information that is collected, used, disclosed, retained or disposed of as part of Services
Frequency	Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December)
Description	The report must include the following information: a) a description of any new measures taken by the Contractor to protect the Personal Information (e.g. new software or access controls being used by the Contractor); b) a description of any changes made to the software, the access controls and the operating procedures, which may have privacy implications; c) a list of any corrections made to Personal Information at the request of Canada on behalf of an individual (including the name of the individual, the date of the request, and the correction made); d) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; e) a list with details of any privacy breaches; and a complete copy (attached annex to the report, in a file format specified by Canada) of all the Personal Information stored electronically by the Contractor.
Report Name	Personal Information Report
Purpose	This report must provide a summary of activities for Personal Information
Frequency	Quarterly
Description	The report must include: a) description of any new measures taken by the Contractor to protect the Personal Information (eg. new software or access controls being used by the Contractor); b) description of any changes made to the software, the access controls and the operating procedures, which may have privacy implications; c) list of any corrections made to Personal Information at the request of Canada on behalf of an individual (including the name of the individual, the date of the request, and the correction made); d) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the Contractor; and

	details of any privacy breaches of Personal Information.

5.7 Service Level Targets

(113) The Contractor must monitor, measure, calculate, and report on SLTs 7 days per week, 24 hours per day, 365 days per year, unless otherwise indicated for a specific SLT.

5.7.1 Outage Time

(114) Outage time for a Service begins from the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada, whichever occurs first. The outage time used in the calculations ends when the affected Service is fully restored for the Incident.

(115) The Contractor's lack of proper security clearance (for itself or its personnel) does not excuse it from its obligation to restore the affected Service within the SLT.

(116) In cases where Canada attempts to report an Incident for an outage but the Contractor's Service Desk does not answer the call, the start time for the outage begins at the time Canada placed the call to the Service Desk.

(117) The following events may, with Canada's approval, be excluded from the calculation of outage time for a Service during a review of the Incidents associated with the outage:

a) failure related to a Security Incident where Canada has approved mitigation actions that impact the availability of CCaaS;
b) failure of another Service;
c) scheduled downtime;
d) failure of a Canada Service, including data received from the Canada Service;
e) suspension of Incident Ticket;
f) a Canada Service does not provide sufficient capacity.

5.7.2 Service Level Target for Service Availability

The Service Level Target Service Availability (SLT-SA) for the Subscription Service must be greater than or equal to 99.900%.

(118) The period of measure for SLT-SA is a calendar month (7/24); therefore the total number of minutes in the measurement period will vary based on the number of calendar days in the month.

(119) The Contractor must calculate SLT-SA as follows: ((measurement period – sum of the outage times) / measurement period) x 100.

(120) The outage time for Incidents where a Service does not function in accordance with the Service Design must be included in the calculation of the SLT-SA for that Service.

(121) The outage time for any of the Incidents defined in CCaaS Annexes must be included in the calculation of the SLT-SA for the Service.

(122) The outage time for any of the following Incidents must be included in the calculation of the SLT-SA for Subscription Service:

a) 1 or more Interaction Priority Queues are unable to process Communication Channels interactions as implemented;
a) Real-Time or Historical Reporting is not available for use by Canada;
b) 2 or more Subscription Service Users are unable to register a change of Status; and
c) 1 or more Supervisors are unable to access Subscription Service via their Web browser.

5.7.3 Service Level Target for Service Desk Response

(123) The Service Level Target for Service Desk Response (SLT-SDR) is that the Contractor's Service Desk must answer 80.0% of all telephone calls placed by Canada within 20 seconds. The period of measure for SLT-SDR is the calendar month.

(124) The SLT-SDR must be calculated as follows:

(125) ((number of calls answered within 20.0 seconds + number of calls abandoned within 20.0 seconds) / (total number of calls answered + total number of abandoned calls)) x 100

(126) The calculation of time to answer a call by the Service Desk begins when a caller starts waiting in queue for a Contractor's Service Desk agent and ends when the Contractor's

(127) Service Desk agent, a live person, answers the caller. Although the Contractor may use voice scripts and menu options acceptable to Canada, the calculation of time to answer a call excludes any time spent by callers listening to and making menu selections in the Contractor's Interactive Voice Response system prior to waiting in queue for the Contractor's Service Desk agent. An abandoned call to the Service Desk is a call that is connected to the Contractor's telephone system but that the Calling Party terminates before a Service Desk agent answers the call.

5.8 Analytics

(128) Contact Centre data (including but not limited to outbound calling, workforce management, service request, incident, release, change, audit data, agent data, CCaaS performance data, IVR utilization, queue data, call data) must be provided to Canada in a format defined by the Contractor in consultation with Canada and subject to Canada's acceptance, as and when required, at no cost to Canada.

(129) Data to be provided at the level sufficient to support invoicing and audit requirements upon Canada request.

(130) Data to be provided at the level sufficient to support internal chargeback requirements upon Canada request.

5.9 Equivalency Arrangements

5.9.1 Product Roadmaps

(131) Canada acknowledges that each Party benefits from open communication. Included in the fees paid to the Contractor, the Contractor shall provide Canada with subject matter expertise support to assist in assessment of product release material including online demo support, user interface impacts, training needs analysis and technical support. This will allow Canada to communicate functional capability enhancements to Government users.

(132) Release material must be provided unfiltered to Canada.

(133) On an annual basis (September 30) and upon Canada request, the Contractor must provide the IP Owner's most current roadmap of anticipated product enhancements/upgrades and anticipated delivery dates. The roadmap shall include functional capabilities in as much detail as requested by Canada. Potential pricing must be identified.

5.9.2 Forums

(134) The IP Owner shall provide Canada with access to the user community such as online message boards, newsgroups, chat rooms, support (technical and troubleshooting), Wikis, blogs and/or other interactive forums that can be accessed and contributed to by certain registered users of Canada. The level of access granted to these communities, as well as toll free telephone support, will be at an equivalent service level as if Canada had contracted directly with the IP Owner.

5.9.3 Support

(135) In the event of an underlying system issue with the service provided by the IP Owner, at the discretion of Canada, the Contractor will include Canada in all interactions with the IP Owner including, but not limited to, meetings, records of decision, and correspondence relating to opening of ticket(s), root cause analysis, resolution/rollback plan and status updates against the plan.

(136) The Contractor shall ensure that IP Owner is bound, and will abide, by the terms for the functional capability outlined in this statement of work. For greater clarity, the level of support provided by the Contractor to the Contractor shall be no less than the level of support provided by the Contractor to Canada.

6 SUBSCRIPTION SERVICE

To be completed for each Requirement.

7 VOICE SERVICES

To be completed for each Requirement.

8 WORK DELIVERABLES

To be completed for each Requirement.

9 TRAINING

To be completed for each Requirement.

10 PROFESSIONAL SERVICES

To be completed for each Requirement

Services de centre de contact du gouvernement (GCCS) Volet 2 : Centre de contact en tant que service (CCaaS)

Modèle d'énoncé de travail

Table des matières

Index des tableaux

1 GESTION DE PROJET

(1) Les exigences dans cette section s'appliquent à tout travail pour la préparation des services, la préparation en matière de sécurité et de protection des renseignements personnels, les services à valeur ajoutée, le service d'abonnement ainsi que la configuration et l'intégration du service d'abonnement, conformément aux commandes de services émises pour les services professionnels.

1.1 Projet de travail

(2) L'entrepreneur doit réaliser et achever toute partie du travail à titre de projet de travail à la demande du Canada.

(3) L'entrepreneur doit entamer les travaux désignés par le Canada à titre de projet de travail dans les dix jours ouvrables du gouvernement fédéral (JOGF) suivant la demande du Canada.

1.1.1 Réunions de projet de travail

(4) L'entrepreneur doit animer une réunion hebdomadaire pour chaque projet de travail (réunion de projet de travail), qui comprend une présentation pour l'examen du rapport d'étape sur le projet de travail.

(5) L'entrepreneur doit animer une réunion hebdomadaire pour examiner tous les projets de travail, qui comprend une présentation pour l'examen du rapport d'étape du bureau de gestion du projet (BGP).

1.1.2 Rapports sur le projet de travail

(6) L'entrepreneur doit présenter les rapports décrits dans le tableau 1 pour les projets de travail :

Tableau 1. Rapports sur le projet de travail

Nom du rapport	Rapport d'étape sur le projet de travail
Fréquence	2 JOGF avant chaque réunion sur l'état du projet de travail
Objet	Le rapport doit présenter l'état d'avancement d'un projet de travail.
Description	Ce rapport doit comprendre : a) le compte rendu de la réunion précédente d'examen du projet de travail; b) les mesures de suivi; c) l'aperçu des jalons du calendrier du projet; d) les tâches actuelles et futures; e) les difficultés du projet, y compris l'évaluation des répercussions et l'état actuel du recours hiérarchique; f) un résumé des risques du projet de travail; g) un résumé avec une description des demandes de modification du projet.
Nom du rapport	Rapport d'étape du bureau de gestion du projet (BGP)
Fréquence	2 JOGF avant chaque réunion du BGP
Objet	Le rapport doit présenter un résumé global de tous les projets de travail.
Description	Ce rapport doit comprendre : a) un compte rendu de la précédente réunion du BGP;

	b) les mesures de suivi; c) un résumé des cinq principaux problèmes; d) l'aperçu des jalons du calendrier maître du projet.

1.2 Demandes de changement de projets

(7) L'entrepreneur doit créer et tenir à jour un registre des demandes de changement pour chaque projet de travail et un registre principal pour tous les projets de travail, dont les formats sont déterminés en consultation avec le Canada et approuvés par le Canada.

(8) L'entrepreneur doit examiner chaque demande de modification du projet en consultation avec le Canada et en évaluer l'incidence sur le projet de travail.

(9) L'entrepreneur doit mettre à jour le calendrier du projet si une demande de modification du projet a une incidence sur une tâche ou une échéance du projet de travail.

(10) Le Canada n'est pas tenu d'émettre une demande de modification du projet pour les nouveaux projets de travail. La redistribution du travail entre les projets de travail en cours ou entre ces derniers et les nouveaux projets de travail se fera en consultation avec l'entrepreneur.

1.3 Registre des risques du projet

(11) L'entrepreneur doit créer et tenir à jour un registre des risques du projet pour chaque projet de travail et un registre principal qui résume les risques de tous les projets de travail, dont les formats sont élaborés en consultation avec le Canada et approuvés par le Canada.

1.4 Calendrier du projet

(12) L'entrepreneur doit créer et tenir à jour un calendrier pour chaque projet de travail et un calendrier maître qui résume le calendrier de tous les projets de travail, dont les formats sont élaborés en consultation avec le Canada et approuvés par le Canada.

(13) Un calendrier de projet doit :

a) ne pas dépendre de l'examen et de l'acceptation des travaux par le Canada, à moins d'approbation par ce dernier;

b) restreindre le plus possible les liens de dépendance;

c) coordonner l'exécution de tâches en parallèle dans la mesure du possible;

d) permettre la présentation progressive des produits livrables (c.-à-d. pas tous en même temps);

e) être produit et tenu à jour avec Microsoft Project;

f) définir les phases, les points de contrôle, les tâches, les livrables et les jalons des travaux, y compris :

g) déterminer toutes les demandes de changement du projet qui provoquent des changements à la date d'achèvement de tout jalon important, avec des numéros attribués correspondant aux numéros qui leur sont attribués dans le rapport d'étape du projet de travail.

(14) L'entrepreneur doit fixer des dates de référence pour le début et la fin de chaque tâche dans un calendrier de projet en fonction de la date d'acceptation du calendrier par le Canada.

(15) L'entrepreneur ne doit pas modifier le calendrier de référence du projet pour la durée du projet de travail, à moins d'en avoir reçu l'approbation par le Canada. Si un changement au calendrier du projet est approuvé par le Canada, l'entrepreneur doit établir un nouveau calendrier de référence dans une nouvelle version du plan du projet qui indique clairement que la base de référence a été révisée.

(16) L'entrepreneur doit s'assurer que l'attribution des ressources dans le calendrier du projet tient compte de la disponibilité ou non de chaque ressource (p. ex. congés, formation et vacances) pour ne pas nuire à la réalisation des travaux du projet.

1.5 Plan des ressources du projet

(17) L'entrepreneur doit créer et tenir à jour un plan des ressources pour chaque projet de travail, qui comprend les éléments suivants :

a) les rôles et les responsabilités de toutes les ressources (les ressources clés et leurs remplaçants, y compris les ressources au niveau des gestionnaires) pour achever les travaux du projet, y compris :

i) le nom et le titre de la ressource;

ii) la description des qualifications de la ressource pour la réalisation des travaux;

iii) le type de travail attribué (spécialisé, temps partiel);

b) un tableau RACI (responsable, agent tenu de rendre compte, consulté et informé) pour cerner les travaux par produit livrable et les activités de travail à réaliser par chaque ressource, le Canada et les intervenants clients au niveau des gestionnaires;

c) une description du processus de renvoi aux paliers de direction (organigramme avec les noms et les coordonnées de toutes les ressources liées au projet de travail).

(18) L'entrepreneur doit créer et tenir à jour un plan principal des ressources du projet qui résument les plans de cette nature pour tous les projets de travail.

2 DOCUMENTS

(19) L'entrepreneur doit définir le contenu et le format des documents pour les produits livrables :

a) en consultation avec le Canada et sous réserve de son acceptation;

b) en français et en anglais lorsque le Canada le demande;

c) dans le format original [p. ex., Word, Excel ou Visio] et dans le format PDF. Lorsque les diagrammes sont intégrés dans un document d'un autre format (p. ex. Word), ils doivent être un métafichier (non modifiable) pour réduire la taille des documents;

(20) L'entrepreneur doit fournir au Canada tous les diagrammes utilisés pour un produit livrable en les créant dans Visio, dans les cinq JOGF suivant une demande du Canada.

(21) L'entrepreneur doit fournir en anglais et en français les guides de l'utilisateur, le matériel de formation et les documents du BGP.

(22) L'entrepreneur doit s'assurer que tous les documents sont tenus à jour en tout temps.

(23) Pour apporter une modification à un produit livrable approuvé (format, contenu), l'entrepreneur doit suivre le processus de traitement des demandes.

(24) L'entrepreneur doit fournir un produit livrable à jour (texte et diagrammes) au Canada, dans les 20 JOGF suivant sa demande, qui indique tous les changements au document dans les demandes de service associées depuis la dernière version du document.

3 RÉUNIONS

(25) Les réunions doivent avoir lieu durant les heures de travail (de 8 h à 17 h, heure de l'Est, pendant les JOGF, à moins d'approbation contraire par le Canada.

(26) L'entrepreneur doit fournir un ordre du jour avant chaque réunion (sauf les réunions quotidiennes), à moins d'approbation contraire par le Canada.

(27) Sauf indication contraire par le Canada, pour chaque réunion à laquelle il participe, l'entrepreneur est responsable des tâches suivantes :

a) assurer la coordination avec le Canada;

b) assurer la coordination de la participation des sous-traitants (s'il y a lieu);

c) fournir le procès-verbal, les calendriers, les listes, les essais, les analyses de conception et toute autre donnée découlant d'un examen préalable ou ultérieur, le cas échéant;

d) s'assurer que le personnel compétent de l'entrepreneur ayant connaissance des questions qui feront l'objet des discussions participe à la réunion;

e) s'assurer que les représentants de l'entrepreneur ont suffisamment d'autorité pour prendre rapidement des décisions au nom de l'entrepreneur.

(28) L'entrepreneur doit préparer un procès-verbal de chaque réunion pendant la réunion et le réviser à la fin de la réunion avec le personnel du Canada. Le format du procès-verbal doit être déterminé en consultation avec le Canada et approuvé par lui.

4 PRÉPARATION EN MATIÈRE DE SÉCURITÉ ET DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

(29) Le travail décrit dans cette sous-section doit être réalisé par l'entrepreneur et accepté par le Canada pour le produit livrable de préparation en matière de sécurité et de protection des renseignements personnels, sans coût supplémentaire pour le Canada.

4.1 Évaluation des mesures de sécurité du nuage

(30) L'entrepreneur doit évaluer les mesures de sécurité du nuage dans les 30 jours civils suivant l'attribution du contrat, ce qui comprend le temps donné au Canada pour examiner et évaluer les preuves fournies par l'entrepreneur que les mesures de sécurité du nuage précisées à la page https://github.com/canada-ca/cloud-guardrails ont été mises en place pour le service d'abonnement.

(31) Si le Canada prend plus de 2 JOGF pour évaluer les preuves fournies par l'entrepreneur et donner une réponse, le Canada décidera seul s'il accorde à l'entrepreneur du temps additionnel (jours civils) pour achever l'évaluation des mesures de sécurité du nuage.

4.2 Évaluation de sécurité

(32) L'entrepreneur doit faire une évaluation de sécurité par une première partie OU une évaluation de sécurité par une tierce partie, à son choix, conformément aux contrôles de sécurité de l'annexe A (pièce jointe).

4.2.1 Évaluation de sécurité par une première partie

(33) L'entrepreneur doit fournir au Canada une certification ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences, et une certification ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage, et un rapport SOC 2 de type II rédigé dans les 12 mois précédant la date du contrat.

4.2.2 Évaluation de sécurité par une tierce partie

(34) L'entrepreneur doit faire faire une évaluation de sécurité par un certificateur tiers indépendant, agréé par l'AICPA ou CPA Canada et/ou un régime de certification ISO qui respecte la norme ISO/IEC 17020 relativement aux systèmes de gestion de la qualité, sans coût supplémentaire pour le Canada, afin de préparer un rapport d'évaluation de sécurité comprenant :

a) la dénomination sociale de l'entreprise;
b) la date actuelle et/ou l'état des certifications et/ou un rapport SOC 2 de type II;
c) une preuve de conformité du service à l'annexe A-5 Exigences de sécurité et aux autres exigences de sécurité dans le contrat;
d) le nom et l'adresse du certificateur tiers indépendant qui a réalisé l'évaluation de sécurité;
e) la preuve que le certificateur tiers indépendant est agréé par l'AICPA ou CPA Canada et/ou un régime de certification ISO qui respecte la norme ISO/IEC 17020 relativement aux systèmes de gestion de la qualité.

4.3 Plan d'action avec jalons

(35) Dans les 20 JOGF suivant une demande du Canada, l'entrepreneur doit soumettre à l'approbation du Canada un plan d'action avec jalons qui :

a) documente les mesures correctives prévues par l'entrepreneur pour corriger les lacunes de sécurité révélées par l'évaluation des mesures de sécurité du nuage et l'évaluation de sécurité et dans tout rapport SOC 2 de type II subséquent ou recertification ISO;
b) comprend un calendrier de mise en œuvre des mesures correctives.

(36) L'entrepreneur doit mettre à jour le plan d'action et les jalons adoptés d'après les résultats des

évaluations de sécurité, des analyses des incidences sur la sécurité, et des activités de surveillance de la sécurité qu'il accomplit.

(37) L'entrepreneur doit mettre en œuvre les mesures correctives ciblées dans le plan d'action avec jalons, conformément au calendrier du projet, pour la version initiale approuvée et toutes les versions ultérieures.

4.4 Plan de sécurité du système

(38) L'entrepreneur doit présenter un plan de sécurité du système (PSS) qui documente les contrôles de sécurité en place ou prévus pour respecter les exigences de sécurité dans le contrat et qui :

a) est compatible avec l'architecture d'entreprise de l'entrepreneur;
b) établit de façon explicite la limite des autorisations relatives au service;
c) décrit les relations ou les liens avec d'autres systèmes d'information externes.
d) présente un aperçu des exigences de contrôle de sécurité du service;
e) décrit la justification des contrôles de sécurité, y compris des décisions en matière de personnalisation et de suppléments;
f) comprend un diagramme des composantes qui illustre clairement l'architecture des services.

4.5 Procédures de sécurité des opérations

(39) L'entrepreneur doit présenter des procédures de sécurité des opérations (PSO) qui documentent ce qui suit pour chaque connexion à un service :

a) les composants du système;
b) les caractéristiques de l'interface;
c) les exigences relatives à la sécurité;
d) la nature de l'information communiquée;
e) la configuration, l'installation et l'exploitation sécurisées du service;
f) l'utilisation et l'entretien efficaces de fonctions de sécurité;
g) les vulnérabilités connues en ce qui concerne la configuration et l'utilisation des fonctions de sécurité administrative (c.-à-d. privilégiées);
h) les fonctions de sécurité accessibles à l'utilisateur, et la façon de les utiliser efficacement;
i) les méthodes d'interaction de l'utilisateur qui lui permettent d'utiliser de façon plus sécuritaire les services d'accès au réseau téléphonique public commuté (RTPC) du gouvernement (SARG);
j) les responsabilités de l'utilisateur concernant le maintien des SARG et des composants du système.

4.6 Plan d'intervention en cas d'incident relatif au service

(40) L'entrepreneur doit fournir un plan d'intervention en cas d'incident de sécurité, qui comprend :

a) la façon dont l'entrepreneur compte détecter, signaler et acheminer les incidents de sécurité;
b) une feuille de route pour la mise en œuvre de la capacité d'intervention en cas d'incident de sécurité, y compris la préparation, la détection, l'analyse, le contrôle et la récupération;
c) une description de la structure et de l'organisation de la capacité d'intervention en cas d'incident de sécurité;
d) une approche d'ensemble de la façon dont la capacité d'intervention en cas d'incident de sécurité s'intègre dans l'organisation générale de l'entrepreneur;
e) une définition des incidents de sécurité à signaler;
f) une définition des mesures servant à évaluer la capacité d'intervention en cas d'incident de sécurité;
g) une définition des ressources et du soutien de la direction nécessaires pour maintenir et faire évoluer la capacité d'intervention en cas d'incident de sécurité.

4.7 Plan de continuité des services

(41) L'entrepreneur doit fournir un plan de continuité des services qui décrit :

a) les missions essentielles et les fonctions opérationnelles qui comprennent le soutien des composantes essentielles du système des SARG et des exigences d'urgence associées;
b) un plan détaillé et des processus documentés pour le rétablissement des opérations des services;
c) les stratégies de sauvegarde pour les installations des centres de données, les installations du réseau, les systèmes de soutien opérationnel et les données, et les principales composantes de service;
d) les objectifs de la reprise, les priorités de la restauration et les mesures selon les ententes sur les niveaux de service (ENS);
e) les rôles et les responsabilités des personnes chargées d'intervenir en cas d'urgence, avec leurs coordonnées;
f) le processus de plein rétablissement des services sans détérioration des mesures de protection de la sécurité initialement prévues et mises en œuvre;
g) les manières d'assurer la continuité des missions et des fonctions opérationnelles essentielles malgré une interruption des services, une compromission ou une panne;
h) les processus de mise à l'essai du plan de continuité des services;
i) les plans de communication détaillés avec le Canada, ses clients et les fournisseurs et les sous-traitants de l'entrepreneur;
j) le plan et les processus détaillés de transfert des fonctions d'exploitation, de gestion et d'administration à un centre des opérations secondaire;
k) les mesures que l'entrepreneur prendra si un de ses sous-traitants clés fait faillite ou s'il fait l'objet de préoccupations de sécurité par le Canada.

(42) L'entrepreneur doit mettre en œuvre le plan de continuité des services (l'ensemble des processus, procédures, rôles, responsabilités, etc.) après son acceptation par le Canada et avant que les services soient prêts à être fournis.

4.8 Plan de gestion des renseignements personnels

(43) L'entrepreneur doit présenter au Canada un plan de gestion des renseignements personnels, qui décrit :

a) les rôles et les responsabilités des ressources de l'entrepreneur affectées à la protection des renseignements personnels et les liens qu'elles entretiendront avec le Canada et les fournisseurs de l'entrepreneur;
b) la façon dont l'entrepreneur prévoit élaborer et maintenir un programme général de sensibilisation à la protection des renseignements personnels de façon continue, par divers moyens (intranet, affiches, etc.);
c) les stratégies détaillées de protection des renseignements personnels de l'entrepreneur qui sont employées pour traiter ces renseignements tout au long de leur cycle de vie;
d) les mesures qu'entend prendre l'entrepreneur pour que son personnel ait une formation sur les renseignements personnels et la gestion connexe;
e) la façon dont les renseignements personnels seront recueillis, utilisés, stockés et divulgués uniquement aux fins des travaux énoncés dans le contrat;
f) les méthodes employées pour restreindre l'accès aux renseignements personnels et aux dossiers aux personnes autorisées (selon le principe du besoin de connaître) aux fins d'exécution des travaux prévus au contrat;
g) les processus d'élaboration et de mise à l'essai des services sans utiliser de données de production du Canada (c.-à-d. des renseignements réels sur les utilisateurs);
h) les processus de détection, de documentation, d'examen, de rapport, de réponse et de renvoi aux échelons supérieurs des incidents liés à la protection de la vie privée;
i) les processus de gestion, de consultation, de collecte, d'utilisation, de divulgation, de réception, de création ou d'élimination des renseignements personnels;
j) les processus visant à limiter la durée de conservation des renseignements personnels et à assurer le respect des exigences du Canada en matière de conservation, incluant la sauvegarde et l'archivage des données;

k) les contrôles d'accès en fonction du rôle utilisés pour restreindre l'accès aux renseignements opérationnels et administratifs exigés par les membres autorisés du personnel de l'entrepreneur et pour enregistrer tous les cas où les membres du personnel ont consulté des renseignements opérationnels;

l) les processus d'intégration d'exigences particulières de conservation et d'élimination de renseignements personnels fondées sur l'évaluation des facteurs relatifs à la vie privée (EFVP) par le Canada;

m) les processus faisant en sorte que les paramètres de consignation et de saisie des données des dispositifs de protection des renseignements et de surveillance du réseau sont déterminés de manière appropriée afin de restreindre la collecte de renseignements personnels;

n) le processus pour traiter les demandes d'accès à des dossiers présentées en vertu de la *Loi sur l'accès à l'information* et les demandes d'accès à des renseignements personnels présentées en vertu de la *Loi sur la protection des renseignements personnels* (demandes d'accès);

o) le protocole à suivre en cas d'atteinte à la vie privée et la façon de traiter une telle situation.

p) toute nouvelle mesure que l'entrepreneur entend mettre en œuvre pour protéger les renseignements personnels et les dossiers en fonction de leur classification de sécurité;

q) les mesures que l'entrepreneur entend prendre pour que les rapports renfermant des renseignements personnels soient stockés ou transmis de façon sûre, en fonction de leur classification de sécurité.

4.9 Évaluation des facteurs relatifs à la vie privée

(44) L'entrepreneur doit aider le Canada à réaliser l'évaluation des facteurs relatifs à la vie privée (EFVP) pour le service d'abonnement, conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308).

(45) En particulier, concernant tout renseignement que le Canada considère comme personnel pendant la période du contrat, l'entrepreneur doit fournir l'information suivante dans les 20 JOGF suivant une demande de l'autorité contractante :

a) les processus opérationnels, les flux de données et les procédures de collecte, de transmission, de traitement, de stockage, d'élimination et de consultation des renseignements, y compris les renseignements personnels;

b) la liste des renseignements personnels qu'il utilise en rapport avec les travaux et les fins auxquelles il emploie chaque type de renseignements;

c) les modalités de partage des renseignements personnels et les destinataires des renseignements;

d) la liste de tous les emplacements où des exemplaires papier des renseignements personnels sont conservés;

e) la liste de tous les endroits où les renseignements personnels lisibles par machine sont conservés (p. ex., l'emplacement des serveurs qui hébergent des bases de données contenant des renseignements personnels), y compris les copies de sauvegarde;

f) la liste de toutes les mesures prises par l'entrepreneur pour protéger les dossiers et les renseignements personnels outre celles qui sont exigées en vertu du contrat;

g) les exigences ou les recommandations relatives à la sécurité et à la protection des renseignements personnels à suivre;

h) une explication détaillée des menaces réelles ou potentielles touchant les renseignements personnels ou les dossiers, accompagnée d'une évaluation des risques associés à ces menaces et la pertinence des mesures de protection prises contre ces risques;

i) les résultats des consultations (le cas échéant) découlant d'un examen de l'EFVP par le Commissariat à la protection de la vie privée du Canada (CPVP) et approuvés par ce dernier;

j) L'entrepreneur doit mettre en œuvre les recommandations découlant de l'EFVP selon un calendrier approuvé par le Canada, sans frais pour ce dernier.

k) Si des changements prévus aux services ont une incidence sur l'utilisation, la collecte, le traitement, la transmission, le stockage ou l'élimination de renseignements personnels, ou lorsque le Canada en fait la demande, l'entrepreneur doit transmettre à ce dernier suffisamment

d'information sur les changements pour justifier une mise à jour de l'EFVP et faire approuver les changements prévus par l'autorité contractante.

l) L'entrepreneur doit fournir à son personnel de prestation des services une trousse de sensibilisation à la protection des renseignements personnels qui donne un aperçu de leur utilisation.

5 EXPLOITATION DES SERVICES

(46) Le travail décrit dans cette sous-section s'applique à l'exploitation, l'administration, la gestion et la tenue à jour continues des CCAAS dans le but de diagnostiquer et corriger de manière proactive les problèmes avant qu'ils nuisent aux services. Ce travail est inclus dans le service d'abonnement, à moins que l'ET indique qu'un avis de demande de travail (ADT) est requis.

5.1 Bureau de service

(47) L'entrepreneur doit fournir un bureau de service qui effectue les fonctions suivantes :

a) servir de principal point de contact pour les incidents signalés par le Canada 24 heures par jour, 7 jours par semaine et 365 jours par année;

b) répondre aux appels et poursuivre le dialogue de niveau 1 et de niveau 2 qui s'ensuit en utilisant la langue officielle du Canada (le français ou l'anglais) demandée par l'appelant;

c) interagir avec les représentants du Canada désignés par le bureau de service du Canada;

d) fournir un numéro de téléphone sans frais, unique et réservé (par exemple, un numéro 1 800) afin de permettre aux représentants autorisés du Canada de communiquer avec le bureau de service;

e) fournir une adresse électronique unique permettant aux représentants autorisés du Canada de communiquer avec le bureau de service.

5.2 Gestion des services opérationnels

Quand le Canada le demande par un ADT, l'entrepreneur doit fournir un soutien aux opérations 24 heures par jour, 7 jours par semaine par un ingénieur spécialiste pour :

f) donner des conseils généraux et assurer le respect des pratiques exemplaires pour la configuration et l'exploitation de la plateforme infonuagique;

g) réaliser les activités prévues de rattrapage des retards;

h) effectuer les fonctions de déplacement, d'ajout, de changement et de suppression;

  i) utilisateurs, stations, groupes de travail, rôles, DAA, codes de comptes, compétences, calendriers, etc.;

i) améliorer et modifier la configuration;

j) ajouter ou modifier les flux d'appels;

k) coordonner les discussions de collecte des exigences;

l) coordonner l'exécution des ordres de travail officiels et l'exécution du projet;

m) réaliser les activités de contrôle des changements liés aux projets;

n) participer aux activités de migration de la production et au transfert des opérations;

o) mettre à jour la documentation sur l'exploitation;

p) gérer les billets d'incident :

  i) dépanner et trier les incidents;

  ii) recueillir les registres et l'information à l'appui supplémentaire;

  iii) communiquer avec le point de contact pour le billet;

  iv) renvoyer les problèmes à un soutien de niveau supérieur;

  v) coordonner la transition des incidents hautement prioritaires à l'équipe de soutien;

  vi) participer aux appels pour les incidents P1 et P2;

  vii) assurer la livraison de l'analyse des causes fondamentales pour tous les incidents P1 et P2;

  viii) assurer la coordination avec l'équipe de soutien pour que l'analyse des causes fondamentales des incidents P3/P4 soit fournie au client sur demande;

q) faire des vérifications de santé quotidiennes;

r) résoudre en temps réel les problèmes détectés durant les vérifications de santé;

s) produire des rapports ponctuels et rétrospectifs.

5.3 Réunions sur l'exploitation des services

(48) L'entrepreneur doit animer et diriger les réunions d'examen des services résumées dans le tableau 2.

Tableau 2. Réunions d'examen des services

Nom de la réunion	Réunion d'examen de la gestion des services
Fréquence	Mensuellement, ou à la demande du Canada
Objet	Examen des incidents, des demandes de changement, des demandes de service, des problèmes, des cibles de niveaux de service et de la facturation
Description	La réunion portera notamment sur : a) le registre des problèmes de la réunion précédente; b) le registre des mesures de suivi de la réunion précédente; c) les rapports post-demande de service du mois précédent; d) les rapports post-demande de changement du mois précédent; e) les rapports post-incident du mois précédent; f) les cibles de niveaux de service et les échecs du mois précédent; g) les demandes de service prévues le mois suivant; h) les demandes de changement prévues le mois suivant; i) les problèmes qui ont nui ou peuvent nuire au rendement des services; j) l'analyse des causes fondamentales des billets d'incident non résolus.
Nom de la réunion	Réunion d'examen de la sécurité
Fréquence	Dans un JOGF suivant une demande du Canada
Objet	Examen des incidents de sécurité
Description	Pour chaque incident de sécurité, la réunion doit comprendre un examen des éléments suivants : a) la date, l'heure et la durée de l'incident de sécurité; b) sa description, en indiquant si l'attaque semble avoir réussi; c) sa portée (portail de services, un seul client ou plusieurs, etc.); d) l'estimation du préjudice et du niveau d'impact; e) la liste des applications touchées connues et suspectées; f) les mesures prises; g) la source ou l'origine apparente de l'attaque; h) le résultat des mesures d'atténuation.

5.4 Gestion des services de TI

(49) L'entrepreneur doit assurer une gestion des services des technologies de l'information pour les services, comme décrit dans les sous-sections suivantes, 24 heures par jour, 7 jours par semaine et 365 jours par année.

5.4.1 Gestion du changement

(50) L'entrepreneur doit faire une demande de changement pour apporter tout changement qui peut perturber les services.

(51) L'entrepreneur doit créer un billet ou plus par demande de changement.

(52) L'entrepreneur doit faire une demande de changement d'urgence pour chaque mesure d'atténuation requise pour contenir un incident de sécurité.

(53) L'entrepreneur doit réaliser l'activité de demande de changement dans les fenêtres d'entretien, sauf les demandes de changement d'urgence. Cela inclut le temps de panne prévu pour réaliser la demande de changement et le temps de panne requis pour sortir de la demande de changement. Toute panne de service qui s'étend au-delà de la fenêtre d'entretien sera considérée comme une indisponibilité de service, et cette période doit être incluse dans le calcul de CNS-DS (cible de niveau de service pour la disponibilité du service) et de CNS-TMRS (cible de niveau de service pour un temps maximum afin de restaurer le service). Dans ce cas, l'entrepreneur doit créer un billet d'incident et enregistrer le temps au-delà de la fenêtre d'entretien approuvée comme un temps de panne du service.

(54) Si l'exécution d'une demande de changement entraîne une incidence ou une interruption imprévue d'un service ou s'il est déterminé qu'elle dépassera la fenêtre d'entretien approuvée par le Canada, l'entrepreneur doit communiquer immédiatement avec le Canada. L'entrepreneur doit fournir une explication détaillée des incidences et du plan pour restaurer le service ou compléter la demande de changement aussi vite que possible. L'entrepreneur doit également créer un billet d'incident pour toute panne non signalée dans la demande de changement.

(55) Toute panne de service qui résulte d'une demande de changement d'urgence faite par l'entrepreneur sera traitée comme une indisponibilité de service.

(56) Pour une demande de changement rejetée, l'entrepreneur doit entrer dans le registre des billets de demande de changement l'information expliquant le rejet, l'état actuel de l'environnement visé par la demande et les changements partiels apportés.

(57) L'entrepreneur doit fournir au Canada un rapport post-demande de changement dans les 5 JOGF suivant l'échec d'une demande de changement.

5.4.2 Exécution des demandes

(58) L'entrepreneur doit avoir recours à la gestion du changement pour tous les changements requis par une demande de service.

(59) L'entrepreneur doit créer au moins un billet pour chaque demande de service soumise par le Canada.

(60) L'entrepreneur doit mettre à jour un billet de demande de service suivant la modification des travaux associés à la demande de service.

(61) L'entrepreneur doit fournir un rapport post-demande de service au Canada suivant l'échec d'une demande de service.

5.4.3 Gestion des versions

(62) L'entrepreneur doit avoir recours à la gestion du changement pour tous les changements requis par une version de service.

(63) L'entrepreneur ne doit pas utiliser les services en production pour tester une version de service avant tout changement.

(64) L'entrepreneur doit fournir au Canada un rapport postérieur à l'échec d'une version de service qui :

a) doit être retirée;
b) a perturbé les services, ou
c) n'a pas atteint l'objectif de l'entrepreneur et qui peut donc avoir besoin d'être répétée ultérieurement.

5.4.4 Gestion des événements et des incidents

(65) L'entrepreneur doit surveiller de manière proactive les services pour détecter les incidents 7 jours par semaine, 24 heures par jour et 365 jours par année.

(66) L'entrepreneur doit collaborer avec le Canada, les clients et toute autre tierce partie désignée par le Canada, pour résoudre les incidents.

(67) L'entrepreneur doit créer un billet d'incident après avoir détecté un incident ou avoir reçu un avis du Canada signalant un incident.

(68) L'entrepreneur doit mettre à jour le registre des billets d'incident à la suite d'un changement de statut de l'incident.

(69) L'entrepreneur doit accorder la plus haute priorité aux applications désignées par le Canada.

(70) L'entrepreneur doit fournir au Canada une matrice opérationnelle de renvoi des incidents aux échelons supérieurs et une matrice de renvoi des incidents à la direction qui :
a) désignent la personne-ressource principale à chaque niveau de renvoi;
b) désignent les substituts (d'égale autorité) à chaque niveau de renvoi;
c) contiennent des instructions claires pour communiquer avec ces personnes.

(71) L'entrepreneur doit classer les incidents et leur attribuer un niveau de priorité.

(72) L'entrepreneur doit aviser le Canada des incidents selon les degrés de priorité définis par le Canada.

(73) L'entrepreneur doit fournir une estimation du temps de résolution dans le billet d'incident.

(74) L'entrepreneur doit résoudre les incidents en prenant les mesures appropriées pour réparer et restaurer les services aussi rapidement que possible, conformément aux CNS-DS associés aux services touchés.

(75) L'entrepreneur doit documenter, dans le registre des activités des billets d'incidents, l'ensemble des éléments suivants :
a) les renvois des incidents à la direction ou au soutien technique;
b) les interactions avec les tierces parties;
c) les détails relatifs à l'enquête, au dépannage, à l'analyse, aux activités de résolution et aux communications concernant les incidents.

(76) L'entrepreneur doit faire le suivi de la durée de l'interruption liée à chaque incident et l'inscrire dans les billets d'incident correspondants.

(77) La durée de l'interruption liée à un incident commence au moment où l'incident est détecté par l'entrepreneur ou est signalé à l'entrepreneur par le Canada, selon la première occurrence.

(78) La durée de l'interruption liée à un incident se termine au moment où le service est entièrement restauré en ce qui concerne cet incident.

(79) L'entrepreneur ne doit pas modifier la durée de l'interruption dans un billet d'incident une fois que celui-ci a été fermé.

(80) Si un billet d'incident est fermé et qu'un incident ultérieur se produit dans les 24 heures pour le même incident, l'entrepreneur doit rouvrir le billet d'origine ou ouvrir un nouveau billet avec une référence qui renvoie au billet précédent et calculer la durée de l'interruption pour le nouvel incident en utilisant la durée combinée des deux incidents, et enregistrer cette durée dans le champ du temps de panne

ajusté du billet d'incident.

(81) L'entrepreneur doit déterminer et consigner les facteurs de causalité (causes fondamentales) de chaque incident.

5.4.4.1 Incidents de sécurité

(82) L'entrepreneur doit déclarer toutes les atteintes à la sécurité suspectées ou réelles en tant qu'incidents de sécurité.

(83) L'entrepreneur doit mettre en place des mesures d'atténuation (par exemple des pare-feux, des signatures personnalisées de services de détection et de prévention d'intrusion, la suppression des courriels malveillants) afin de maîtriser un incident de sécurité, d'assurer une protection contre les menaces cybernétiques et d'éliminer les vulnérabilités.

(84) L'entrepreneur doit fournir les résultats de recherche dans les registres et les dossiers de vérification associés à un incident de sécurité, d'après les critères précisés par le Canada, dans les 72 heures suivant une demande du Canada.

(85) L'entrepreneur doit mettre en œuvre un processus de vérification et d'enquête pour les incidents de sécurité qui ne permet qu'à des représentants du Canada désignés et préautorisés de demander et d'obtenir un accès discret à l'information pour mener des enquêtes de sécurité.

(86) L'entrepreneur doit utiliser des procédures et des mesures de protection judiciaires appropriées pour le traitement des incidents de sécurité, qui comprennent :

a) le maintien d'une chaîne de possession de l'information sur la vérification;

b) une collecte, une conservation et une présentation de preuves qui démontrent leur intégrité.

(87) Pendant un incident de sécurité, l'entrepreneur doit réduire le délai d'intervention standard en fonction de la priorité de l'incident définie par le Canada.

5.4.5 Gestion de la configuration

(88) L'entrepreneur doit gérer la configuration, y compris celle des services, pour remplir les exigences opérationnelles continues des services conformément aux ordres de services professionnels.

(89) L'entrepreneur doit développer, consigner et maintenir la configuration de base courante des services et pouvoir retracer celle des versions précédentes.

(90) L'entrepreneur doit s'assurer que seuls les éléments de configuration autorisés sont utilisés ou mis en œuvre pour les services.

(91) L'entrepreneur doit consigner tout ajout, toute modification ou toute suppression d'un élément de configuration dans une entrée d'un fichier journal de configuration.

(92) L'entrepreneur doit tenir des sauvegardes quotidiennes des données de configuration et en stocker les copies les plus récentes dans une installation hors site.

(93) Le service d'abonnement doit permettre une configuration de locataire principal, qui peut être transmise à des sous-locataires désignés par le Canada, qui peuvent appliquer différentes règles opérationnelles.

5.5 Sécurité et protection des renseignements personnels

5.5.1 Évaluation continue de la sécurité

(94) L'entrepreneur doit fournir a), et b) et c), sur une base annuelle:

a) un rapport SOC 2 de type II;

b) la preuve d'une certification en vigueur ISO/IEC 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences;

c) la preuve d'une certification en vigueur ISO/IEC 27017:2015 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage.

5.5.2 Plan de continuité des services

(95) L'entrepreneur doit s'assurer que le plan de continuité des services est :

a) coordonné avec les éléments organisationnels responsables des plans associés, y compris les équipes de gestion des incidents;

b) communiqué et distribué aux éléments organisationnels participant à l'exécution du plan;

c) protégé de toute divulgation ou modification non autorisée.

(96) L'entrepreneur doit signaler immédiatement au Canada toute catastrophe ou toute autre situation d'urgence ayant des répercussions sur les services. L'avis doit inclure l'information suivante : une brève description de la situation, la date et l'heure, le temps de restauration estimé et les points de prestation de services touchés.

(97) L'entrepreneur doit mettre à l'essai annuellement le plan de continuité des services (l'ensemble des processus, procédures, rôles, responsabilités, etc.), comme consigné dans le plan approuvé, et présenter les résultats au Canada dans les 20 JOGF suivant la fin des essais.

(98) L'entrepreneur doit restaurer les fonctions du service dans le cadre de sa mise à l'essai du plan de continuité des services. L'exercice de rétablissement ne doit pas être effectué à l'aide des services de production, à moins d'une autorisation par le Canada.

(99) L'entrepreneur doit corriger tout problème du service décelé au cours de la mise à l'essai du plan de continuité des services dans les 60 JOGF suivant la fin de l'essai.

(100) L'entrepreneur doit fournir au Canada, dans les 40 JOGF suivant une demande, la preuve que le plan de continuité du service a été convenablement mis en œuvre, qu'il fonctionne comme prévu, qu'il produit les résultats escomptés et remplit les exigences en matière de continuité du service. La preuve peut prendre la forme de résultats de tests, d'évaluations, de vérifications ou autres, et ne peut dater de plus de 12 mois.

5.5.3 Plan de gestion des renseignements personnels

(101) L'entrepreneur doit réviser annuellement le plan de gestion des renseignements personnels et présenter au Canada, dans les 20 JOGF suivant la fin de la révision, un rapport qui résume les résultats de la révision et propose des changements. L'entrepreneur doit actualiser le plan de gestion des renseignements personnels dans les 20 JOGF suivant l'acceptation du rapport par le Canada.

(102) L'entrepreneur doit fournir au Canada, dans les 40 JOGF suivant une demande, la preuve que le plan de gestion des renseignements personnels a été convenablement mis en œuvre, qu'il fonctionne comme prévu, qu'il produit les résultats escomptés et remplit les exigences du Canada en matière de gestion des renseignements personnels. La preuve peut prendre la forme de résultats de tests, d'évaluations, de vérifications ou autres, et ne peut dater de plus de 24 mois.

(103) L'entrepreneur doit produire un rapport sur l'atténuation des vulnérabilités après la réalisation des activités de correction dans le cadre d'un plan d'atténuation des vulnérabilités. Ce rapport comprend :

a) une description des mesures correctives mises en œuvre;

b) une preuve que les documents connexes sur le système ont été mis à jour en fonction des changements.

(104) L'entrepreneur doit atténuer toutes les lacunes en sécurité détectées à la suite des tests de vulnérabilité réalisés par l'entrepreneur et le Canada, conformément aux exigences de sécurité du Canada et sans coût additionnel pour ce dernier.

5.6 Rapports et documents

(105) Le Canada a l'intention d'utiliser les rapports fournis par l'entrepreneur lorsque possible, selon la décision du Canada. Les rapports exacts seront déterminés durant une consultation avec le Canada avant que les services soient prêts à être fournis.

(106) L'entrepreneur doit présenter des rapports rédigés en anglais, et se référer à l'heure de l'Est.

(107) Les dates et les chiffres tirés du rapport doivent s'afficher en format numérique plutôt que sous forme de texte.

(108) L'entrepreneur doit fournir tous les rapports annuels dans les 30 JOGF suivant la fin des 12 mois précédents en fonction de l'anniversaire du contrat.

(109) L'entrepreneur doit fournir tous les rapports hebdomadaires dans les 2 JOGF suivant la fin de la semaine précédente, qui se termine vendredi à 23 h 59.

(110) L'entrepreneur doit fournir tous les rapports mensuels dans les 5 JOGF suivant la fin du mois précédent, qui se termine à 23 h 59 le dernier JOGF du mois.

(111) L'entrepreneur doit fournir au Canada tous les rapports fournis à ses autres clients pour les services utilisant des données du Canada.

(112) L'entrepreneur doit fournir les rapports sur les opérations de service décrits dans le Tableau 3 conformément à leur fréquence, leur objet et leur description.

Tableau 3. Rapports sur les opérations des services

Nom du rapport	Rapport sommaire de gestion du service
Fréquence	Planifiée, mensuelle
Objet	Le rapport doit présenter un résumé du rendement de l'entrepreneur dans la prestation des services et l'atteinte des CNS.
Description	Ce rapport doit comprendre : a) le nombre total d'incidents et le nombre total d'exceptions aux CNS pour le mois de référence; b) La liste de tous les incidents pour le mois de référence, organisés par type, priorité et CNS, en indiquant les numéros de billets d'incident et les niveaux de renvoi au palier supérieur invoqués; c) la liste des exceptions aux CNS pour le mois visé, précisant la CNS pour chaque exception et l'écart par rapport à la CNS (s'applique à tous les types d'exceptions aux CNS, qu'il y ait ou non un billet d'événement correspondant); d) une description des recommandations, des mesures correctives et des délais de mise en œuvre des changements nécessaires pour résoudre les problèmes chroniques ou la dégradation des services et/ou pour prévenir les exceptions futures aux CNS; e) une description des incidents et des problèmes liés aux services de l'entrepreneur, comme le service de portail et les systèmes, outils et applications connexes (p. ex. la BDGC, la production de rapports, etc.), y compris les mesures correctives et les délais nécessaires de résolution; f) les demandes de service réglées ou en attente; g) les demandes de changements réglées ou en attente.
Nom du rapport	Rapport sur les demandes de service et les demandes de changement
Fréquence	Planifiée, mensuelle
Objet	Le rapport doit présenter un rapport détaillé de toutes les demandes de service prévues ou réglées durant la période de référence.
	Ce rapport doit comprendre :

	a) les demandes de service fermées durant la période de référence; b) les demandes de service en attente d'exécution; c) les demandes de changement fermées durant la période de référence; d) les demandes de changement en attente d'exécution.
Nom du rapport	Rapport d'incident
Fréquence	Sur demande, dans les 2 JOGF suivant la demande du Canada
Nom du rapport	Rapport post-demande de changement
Fréquence	Sur demande. Remis le JOGF suivant immédiatement l'exécution de toute demande de changement d'urgence et/ou dans les 5 JOGF de l'échec d'une demande de changement ou d'une version de service.
Objet	Le rapport doit donner au Canada une compréhension approfondie de l'échec d'une demande de changement, ou d'une demande de changement d'urgence.
Nom du rapport	Rapport post-demande de service
Fréquence	Sur demande. Remis le JOGF suivant immédiatement l'exécution de toute demande de service d'urgence et/ou dans les 5 JOGF de l'échec d'une demande de service.
Objet	Le rapport doit donner au Canada une compréhension approfondie de l'échec d'une demande de service, ou d'une demande de service d'urgence.
Nom du rapport	Rapport sommaire de version de service
Fréquence	Planifiée, mensuelle
Objet	Résumé des activités liées aux versions de service
Description	Le rapport doit inclure, pour chaque version de service du mois précédent : a) l'heure et la date de la mise à jour; b) le but de la mise à jour; c) la description des activités de mise à jour; d) les parties des services du centre de contact de l'entreprise qui sont touchées; e) les leçons retenues (si la mise à jour a échoué).
Nom du rapport	Rapport de billet de service
Fréquence	En temps réel, au besoin
Objet	Ce rapport définissable par l'utilisateur doit fournir l'accès aux billets d'incident, de problèmes, de demande de changement, de demande de service, d'après le type de billet choisi par le Canada et tout champ de billet pendant une période choisie par l'utilisateur.
Description	Le générateur de rapports doit fournir : a) la capacité d'effectuer des recherches dans l'information, de la trier et de consulter les billets; b) la capacité de télécharger les résultats de recherche de billets dans un fichier de format commercial et suivant la convention d'appellation précisée par le

	Canada; c) la capacité de voir chaque billet (tous les champs) dans une structure hiérarchique où l'information de chaque billet est accessible en mode « zoom avant » (pour billets connexes) en sélectionnant des hyperliens; d) un rapport cumulatif détaillant pour chaque billet dans les résultats de la recherche : le numéro du billet, la date, la priorité, les billets associés (s'il y a lieu), les services du centre de contact de l'entreprise qui sont touchés, la durée de la panne, une description détaillée du billet; e) un accès direct aux éléments de configuration de la BDGC concernée en cliquant un hyperlien dans le billet; f) la capacité de générer l'information sommaire au sujet des billets ouverts ou fermés, présentée sous forme de tableau et de graphique, par année, mois, jour et heure, pour un certain nombre de billets par niveau de priorité.
Nom du rapport	Rapport sommaire sur la protection des renseignements personnels
Objet	Renseignements personnels recueillis, utilisés, divulgués, conservés ou éliminés dans le cadre des services
Fréquence	Dans un délai de trente (30) jours civils suivant la fin de chaque trimestre (janvier-mars, avril-juin, juillet-septembre, octobre-décembre)
Description	Le rapport doit comprendre les renseignements suivants : a) une description de toute nouvelle mesure prise par l'entrepreneur pour protéger les renseignements personnels (p. ex., un nouveau logiciel ou de nouveaux contrôles d'accès utilisés par l'entrepreneur); b) une description de tous les changements apportés aux logiciels, aux contrôles d'accès et aux procédures opérationnelles, qui pourraient avoir des répercussions sur la protection des renseignements personnels; c) une liste des corrections apportées aux renseignements personnels à la demande du Canada au nom d'un individu concerné (comprenant le nom de la personne, la date de la demande et la correction apportée); d) les détails de toute plainte reçue d'individus concernant la manière dont leurs renseignements personnels sont recueillis ou traités par l'entrepreneur; e) une liste détaillée de tous les cas d'atteinte à la vie privée; et une copie (jointe en annexe au rapport, dans un format de fichier précisé par le Canada) de l'ensemble des renseignements personnels conservés électroniquement par l'entrepreneur.
Nom du rapport	Rapport sur les renseignements personnels
Objet	Ce rapport doit fournir un résumé des activités liées aux renseignements personnels.
Fréquence	Trimestrielle
Description	Ce rapport doit comprendre : une description de toute nouvelle mesure prise par l'entrepreneur pour protéger les renseignements personnels (p. ex., un nouveau logiciel ou de nouveaux contrôles d'accès utilisés par l'entrepreneur); une description de tous les changements apportés aux logiciels, aux contrôles d'accès et aux procédures opérationnelles, qui pourraient avoir des répercussions sur la protection des renseignements personnels;

	une liste des corrections apportées aux renseignements personnels à la demande du Canada au nom d'un individu concerné (comprenant le nom de la personne, la date de la demande et la correction apportée); les détails de toute plainte reçue d'individus concernant la manière dont leurs renseignements personnels sont recueillis ou traités par l'entrepreneur; les détails de tous les cas d'atteinte à la vie privée.
Objet	Ce rapport doit donner au Canada une compréhension approfondie de tout incident qui, selon lui, a eu une incidence importante sur ses activités. Le rapport doit clarifier ce qui est arrivé exactement durant l'incident, y compris les actions de l'entrepreneur, et préciser les plans de l'entrepreneur pour prévenir toute récurrence du problème.

5.7 Cibles de niveau de service

(113) L'entrepreneur doit surveiller, calculer, et déclarer les cibles de niveau de service 24 heures par jour, 7 jours par semaine et 365 jours par année, sauf indication contraire pour une CNS précise.

5.7.1 Temps de panne

(114) Le temps de panne d'un service commence au moment (heure de début) où l'incident est détecté par l'entrepreneur ou signalé à l'entrepreneur par le Canada, selon la première éventualité. Le temps de panne utilisé dans les calculs se termine lorsque le service touché est entièrement rétabli après l'incident.

(115) L'entrepreneur qui manque d'une habilitation de sécurité appropriée (pour son personnel ou lui-même) n'est pas dégagé de son obligation de rétablir le service concerné en respectant les CNS.

(116) Dans les cas où le Canada tente de signaler un incident de panne, mais que le bureau de service de l'entrepreneur ne prend pas l'appel, l'heure de début de la panne commence au moment où le Canada a fait un appel au bureau de service.

(117) Les événements suivants peuvent, avec l'approbation du Canada, être exclus du calcul du temps de panne pour un service durant un examen des incidents associés à la panne :

a) une défaillance liée à un incident de sécurité pour lequel le Canada a approuvé des mesures d'atténuation qui ont une incidence sur la disponibilité des CCAAS;
b) la défaillance d'un autre service;
c) un temps d'arrêt prévu;
d) la défaillance d'un service du Canada, y compris la réception des données;
e) la suspension d'un billet d'incident;
f) un service du Canada ne fournit pas une capacité suffisante.

5.7.2 Cible de niveau de service pour la disponibilité du service (CNS-DS)

La CNS-DS pour le service d'abonnement doit être supérieure ou égale à 99,900 %.

(118) La période utilisée pour mesurer la CNS-DS est un mois civil (7 jours par semaine, 24 heures par jour). Par conséquent, le nombre total de minutes au cours de la période de mesure varie en fonction du nombre de jours civils dans un mois donné.

(119) L'entrepreneur doit calculer la CNS-DS comme suit : ([période de mesure – somme des temps de panne]/période de mesure) x 100.

(120) Le temps de panne pour les incidents où un service ne fonctionne pas comme prévu doit être inclus dans le calcul de la CNS-DS pour ce service.

(121) Le temps de panne pour tous les incidents définis dans les annexes des CCA doit être inclus dans le calcul de la CNS-DS pour ce service.

(122) Le temps de panne des incidents suivants doit être inclus dans le calcul de la CNS-DS pour le service

d'abonnement :

a) une file de priorité d'interaction (ou plus) ne peut pas traiter les interactions des canaux de communication comme mis en œuvre;
a) le Canada ne peut produire de rapports rétrospectifs ou en temps réel;
b) deux utilisateurs du service d'abonnement (ou plus) ne peuvent enregistrer un changement de statut;
c) un superviseur (ou plus) ne peut accéder au service d'abonnement via leur navigateur Web.

5.7.3 Cible de niveau de service pour le délai de réponse du centre de service (CNS-DRCS)

(123) La CNS applicable au délai de réponse du centre de service (CNS-DRCS) stipule que le centre de service de l'entrepreneur doit répondre dans un délai de 20 secondes à 80,0 % de tous les appels faits par le Canada. La période de mesure de la CNS-DRCS est le mois civil.

(124) La CNS-DRCS doit être calculée comme suit :

(125) [(nombre total d'appels répondus dans les 20,0 secondes + nombre d'appels abandonnés dans les 20,0 secondes)/(nombre total d'appels répondus + nombre total d'appels abandonnés)] x 100

(126) Le calcul du délai de réponse du centre de service commence au moment où un appelant est mis en attente avant de parler à un agent du centre de service de l'entrepreneur et se termine au moment où un tel agent y répond en personne. Bien que l'entrepreneur puisse utiliser des scripts vocaux et des options de menu acceptables pour le Canada, le calcul du délai de réponse à un appel exclut le temps passé par les appelants à écouter et à sélectionner les options du menu du système de réponse vocale interactif de l'entrepreneur avant d'être mis en attente pour parler à un agent de son centre de service. Un appel abandonné au centre de service est un appel transmis au système téléphonique de l'entrepreneur et auquel le demandeur met fin avant qu'un agent du centre de service lui réponde.

(127) Service Desk agent, a live person, answers the caller. Although the Contractor may use voice scripts and menu options acceptable to Canada, the calculation of time to answer a call excludes any time spent by callers listening to and making menu selections in the Contractor's Interactive Voice Response system prior to waiting in queue for the Contractor's Service Desk agent. An abandoned call to the Service Desk is a call that is connected to the Contractor's telephone system but that the Calling Party terminates before a Service Desk agent answers the call.

5.8 Analyse

(128) Les données du Centre de contact (y compris, mais sans s'y limiter, les appels sortants, la gestion de l'effectif, la demande de service, l'incident, la libération, le changement, les données de vérification, les données de rendement de l'agent, les données de rendement du CCaaS, l'utilisation des RVI, les données de file d'attente, les données d'appel) doivent être fournies au Canada dans un format défini par l'entrepreneur en consultation avec le Canada et sous réserve de l'acceptation du Canada, au besoin, sans frais pour le Canada

.

(129) Les données doivent être fournies au niveau suffisant pour appuyer les exigences en matière de facturation et de vérification à la demande du Canada .

(130) Données à fournir au niveau suffisant pour appuyer les exigences internes en matière de rétrofacturation à la demande du Canada .

5.9 Ententes d'équivalence

5.9.1 Feuilles de route des produits

(131) Le Canada reconnaît que chaque Partie bénéficie d'une communication ouverte. Inclus dans les honoraires payés à l'entrepreneur, l'entrepreneur doit fournir au Canada un soutien spécialisé en la matière pour l'aider à évaluer le matériel de lancement de produits, y compris le soutien de démonstration en ligne, les impacts de l'interface utilisateur, l'analyse des besoins de formation et le soutien technique. Cela permettra au Canada de communiquer les améliorations de la capacité fonctionnelle aux utilisateurs du gouvernement .

(132) Le matériel de rejet doit être fourni non filtré au Canada.

(133) Sur une base annuelle (30 septembre) et à la demande du Canada, l'entrepreneur doit fournir la

feuille de route la plus à jour du propriétaire de la PI sur les améliorations et les mises à niveau prévues des produits et les dates de livraison prévues. La feuille de route doit inclure les capacités fonctionnelles avec autant de détails que le Canada le demande. Les prix potentiels doivent être identifiés .

5.9.2 Forums

(134) Le propriétaire de la PI doit fournir au Canada l'accès à la communauté des utilisateurs, comme les babillards électroniques en ligne, les groupes de discussion, les salons de clavardage, le soutien (technique et dépannage), les wikis, les blogues et/ou d'autres forums interactifs auxquels certains utilisateurs inscrits du Canada peuvent accéder et auxquels ils peuvent contribuer. Le niveau d'accès accordé à ces collectivités, ainsi que le soutien téléphonique sans frais, seront à un niveau de service équivalent comme si le Canada avait conclu un contrat directement avec le propriétaire de la PI.

5.9.3 Pris en Charge

(135) En cas de problème de système sous-jacent avec le service fourni par le propriétaire de la PI, à la discrétion du Canada, l'entrepreneur inclura le Canada dans toutes les interactions avec le propriétaire de la PI, y compris, mais sans s'y limiter, les réunions, les comptes rendus de décision et la correspondance concernant l'ouverture des billets, l'analyse des causes profondes, le plan de résolution / restauration et les mises à jour de l'état par rapport au plan.

(136) L'entrepreneur doit s'assurer que le propriétaire de la PI est lié et respectera les modalités de la capacité fonctionnelle décrites dans le présent énoncé des travaux. Pour plus de clarté, le niveau de soutien fourni par l'entrepreneur à l'entrepreneur ne doit pas être inférieur au niveau de soutien fourni par l'entrepreneur au Canada.

6 SERVICE D'ABONNEMENT

À remplir pour chaque besoin.

7 SERVICES TÉLÉPHONIQUES

À remplir pour chaque besoin.

8 PRODUITS LIVRABLES

À remplir pour chaque besoin.

9 FORMATION

À remplir pour chaque besoin.

10 SERVICES PROFESSIONNELS

À remplir pour chaque besoin.