Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.,/11, rue Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet
ONLINE SURVEY RFP

Solicitation No. - N° de l'invitation	**Date**
B8815-170230/B	2019-05-27

Client Reference No. - N° de référence du client
B8815-170230

GETS Reference No. - N° de référence de SEAG
PW-$$XL-141-35728

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
141xl.B8815-170230	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2019-07-08

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Miller, Tracey	141xl

Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 858-2651 ( )	(819) 956-2675

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
DEPARTMENT OF CITIZENSHIP AND IMMIGRATION
ATT: SUZANNE ST-DENIS
365 LAURIER AVE W., JETS 19TH FL.
GATINEAU
Quebec
K1A1L1
Canada

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
See Herein	

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Shared Systems Division (XL)/Division des systèmes partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Canada

This page is replaced by the ABE cover sheet issued by PWGSC.

BID SOLICITATION

HOSTED ONLINE SURVEY SOLUTION

FOR

IMMIGRATION, REFUGEES AND CITIZENSHIP CANADA

Table of Content

List of Annexes to the Resulting Contract:

Annex A	Statement of Requirements
Annex B	Evaluation Criteria
Annex C	Basis of Payment
Annex D	Security Requirements Check List
Annex E	Government of Canada Security Control Profile for Cloud-based GC Services
Annex F	Security Screening Requirements
Annex G	Mandatory Security Technical Criteria
Annex H	Point-rated Criteria for Mandatory Security Technical Criteria
Annex I	Bidders Forms

Forms:

Form 1 - Bid Submission Form
Form 2 - Substantiation of Technical Compliance Form
Form 3 - OEM Certification Form
Form 4 - Software Publisher Certification Form
Form 5 - Software Publisher Authorization Form
Form 6 - Declaration Form
Form 7 - List of Names Form

BID SOLICITATION

HOSTED ONLINE SURVEY SOLUTION

FOR

IMMIGRATION, REFUGEES AND CITIZENSHIP CANADA

PART 1 - GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, if applicable, and the basis of selection;

Part 5 Certifications: includes the certifications to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The annexes include the Statement of Requirements and any other annexes.

1.2 Summary

(a) Immigration, Refugees and Citizenship Canada (IRCC) has an initial requirement for a commercially available fully Hosted Online Survey Solution for approximately 100 Client Users.

(b) The Hosted Online Survey Solution must meet all the requirements as stated in Annex A – Statement of Requirements (SOR). The Hosted Online Survey Solution must also include a warranty, and associated documentation. Training services must also be provided, on an as and when requested basis. The bid solicitation is intended to result in the award of a Contract for 1 year, plus 4 one-year irrevocable options allowing Canada to extend the term of the Contract. All components of the Hosted Online Survey Solution must be available to the Client Users 24 hours a day, 7 days a week, 365 days a year, in English and French, and operate at all times in accordance with the Statement of Requirements in the Client's operational environment described in the bid solicitation.

(c) The term **"Client User"** refers to the employees of the Government of Canada, the Minister's office and staff, and other individuals authorized by the Client to perform services in relation to the business and affairs of the Client, including public servants from other departments and contractors or consultants performing work for the Client from time to time. Although Canada may make the Hosted Online Survey Solution available to any or all of the Clients, this bid solicitation does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs.

(d) **Immigration, Refugees and Citizenship Canada (IRCC)** is the Initial Client that will use the **Hosted Online Survey Solution** (the "Software Solution"). However, this bid solicitation will also allow Canada to make the Software Solution available to any department or Crown corporation (as those terms are defined in the Financial Administration Act) or any other party for which the Department of Public Works and Government Services is authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act (each a **"Client"**). Although Canada may make the Software Solution available to any or all the Clients, this bid solicitation does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs. When the Software Solution is made available to Clients other than the Initial Client, any required training will be purchased under a separate contract.

(e) There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organizational security screening or security clauses, Bidders should refer to the Industrial and Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

(f) The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), and the Canadian Free Trade Agreement (CFTA).

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be provided in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

(a) All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the *Standard Acquisition Clauses and Conditions Manual* (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

(b) Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

(c) The 2003 (2017-04-27) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails.

(d) "Subsection 3 of Section 01, Integrity Provisions - Bid of Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:

3. List of Names

a) Bidders who are incorporated or who are a sole proprietorship, including those bidding as a joint venture, have already provided a list of names of all individuals who are directors of the Bidder, or the name of the owner(s), at the time of submitting an arrangement under the Request for Supply Arrangement (RFSA).

b) These Bidders must immediately inform Canada in writing of any changes affecting the list of directors during this procurement process.

(e) Subsection 5(4) of 2003, Standard Instructions - Goods or Services - Competitive Requirements is amended as follows:

(i) Delete: 60 days

(ii) Insert: 365 days

2.2 Submission of Bids

(a) Bids must be submitted only to Public Works and Government Services Canada PWGSC Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation.

(b) Due to the nature of the bid solicitation, bids transmitted by facsimile to PWGSC will not be accepted.

2.3 Former Public Servant

(a) Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPS, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

(b) **Definitions**

For the purposes of this clause, "former public servant" is any former member of a department as defined in the *Financial Administration Act,* R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

(i) an individual;

(ii) an individual who has incorporated;

(iii) a partnership made of former public servants; or

(iv) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c.P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c.S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act,* R.S., 1985, c.C-17, the *Defence Services Pension Continuation Act*, 1970, c.D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c.R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c.R-11, the *Members of Parliament Retiring Allowances Act* , R.S., 1985, c.M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, .C-8.

(c) **Former Public Servant in Receipt of a Pension**

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes ( ) No ( )**

If so, the Bidder must provide the following information, for all FPS in receipt of a pension, as applicable:

(i) name of former public servant;

(ii) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

(d) **Work Force Adjustment Directive**

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes ( ) No ( )**

If so, the Bidder must provide the following information:

(i) name of former public servant;

(ii) conditions of the lump sum payment incentive;

(iii) date of termination of employment;

(iv) amount of lump sum payment;

(v) rate of pay on which lump sum payment is based;

(vi) period of lump sum payment including start date, end date and number of weeks;

(vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

2.4 Enquiries - Bid Solicitation

(a) All enquiries must be submitted in writing to the Contracting Authority no later than 10 calendar days before the bid closing date. Enquiries received after that time may not be answered.

(b) Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as proprietary will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the questions or may request that the Bidder do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

(a) Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Note to Bidders: Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of its choice without affecting the validity of its bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of its choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidder. *Bidders are requested to indicate the Canadian province or territory they wish to apply to any resulting contract in their Bid Submission Form*.

2.6 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Requirements (SOR) contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reasons for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled "Enquiries - Bid Solicitation". Canada will have the right to accept or reject any or all suggestions.

2.7 Volumetric Data

The Client's Volumetric Data is described in Annex C – Basis of Payment, Table 4. The data included in the bid solicitation has been provided to Bidders in order to compare bids during the bid financial evaluation or to assist in the preparation of their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of the Hosted Survey Solution will be consistent with this data. It is provided purely for information purposes.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

(a) If the Bidder chooses to submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 8 of the 2003 standard instructions and as amended in Part 2 - Bidder Instructions, Article 2.1 Standard Instructions, Clauses and Conditions. Bidders are required to provide their bid in a single transmission. The epost Connect service has the capacity to receive multiple documents, up to 1GB per individual attachment.

The bid must be gathered per section and separated as follows:

(i) Section I: Technical Bid

(ii) Section II: Financial Bid

(iii) Section III: Certifications

(iv) Section IV: Additional Information

(b) If the Bidder chooses to submit its bid in hard copies, Canada requests that the Bidder submits its bid in separately bound sections as follows:

(i) Section I: Technical Bid (2 hard copies)

(ii) Section II: Financial Bid (2 hard copies)

(iii) Section III: Certifications (2 hard copies)

(iv) Section IV: Additional Information (2 hard copies)

If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy.

(c) Due to the nature of the bid solicitation, bids transmitted by facsimile will not be accepted.

(d) **Format for Bid:** Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

(i) use 8.5 x 11 inch (216 mm x 279 mm) paper;

(ii) use a numbering system that corresponds to the bid solicitation;

(iii) include a title page at the front of each volume of the bid that includes the title, date, bid solicitation number, bidder's name and address and contact information of its representative; and

(iv) include a table of contents.

(e) **Canada's Policy on Green Procurement:** In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. See the Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Bidders should:

(i) use paper containing fibre certified as originating from a sustainably-managed forest and/or containing a minimum of 30% recycled content; and

(ii) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, and using staples or clips instead of cerlox, duotangs or binders.

(f) **Submission of Only One Bid:**

A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating means being part of the Bidder, not being a subcontractor), Canada will

provide those Bidders with 2 working days to identify the single bid to be considered by Canada. Canada will choose in its discretion which bid to consider.

For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity Is a natural person, corporation, partnership, etc), an entity will be considered to be **"related"** to a Bidder if:

(A) they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);

(B) they are "related persons" or "affiliated persons" according to the *Canada Income Tax Act;*

(C) the entities have now or in the two years before bid closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

(D) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

Individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture.

(g) **Joint Venture Experience:**

Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service, and (b) that the bidder have 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive.

Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit this information during the evaluation period. If the Bidder does not submitted this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

Example: A bidder is a joint venture consisting of members A and B. If a bid solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting either:

- Contracts all signed by A;
- Contracts all signed by B; or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

3.2 Section I: Technical Bid

(a) In their technical bid, Bidders must demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders must demonstrate their capability in a thorough, concise and clear manner for carrying out the work.

(b) The technical bid must address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

(c) **The technical bid consists of the following:**

(i) **Bid Submission Form:** Bidders are requested to include the Bid Submission Form Attachment "1" with their bids. It provides a common form in which bidders can provide information required for evaluation and contract award, such as a contact name and the Bidder's Procurement Business Number, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.

(ii) **Substantiation of Technical Compliance (Attached as Form "2"):** The technical bid must substantiate the compliance of the Bidder and its proposed solution with the specific articles of Annex A (Statement of Requirement) identified in the Substantiation of Technical Compliance Form, which is the requested format for providing the substantiation. The Substantiation of Technical Compliance Form is not required to address any parts of this bid solicitation not referenced in the form. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or product complies is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be declared non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Reference" column of the Substantiation of Technical Compliance Form, where bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the

reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

(iii) **Training Plan:** The Bidder must provide an outline of its proposed draft training plan, which must demonstrate that the Bidder's proposed training meets all the mandatory requirements for training described in Annex A - Statement of Requirements. The training plan must include, at a minimum: course materials that will be provided to participants for 20 hours of training in either French and/or English on line or in person (if in-person then facilities to be made available by the Bidder).

(iv) **Customer Reference Contact Information:**

(A) In conducting its evaluation of the bids, Canada may, but will have no obligation to request that a bidder provide customer references. If Canada sends such a written request, the bidder will have 2 working days to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

(B) These customer references must each confirm ["if"] requested by PWGSC,

1. the information required by Article "Reference Checks" is that the Bidder has used the Software Solution for at least 12 months and is still using it at the bid closing date.

2. the facts identified in the Bidder's bid, as required by Article "Reference Checks" that the Bidder has previously provided the customer with long distance services for at least 60 users for at least 12 months and is still using it at the bid closing date.

(C) The form of question to be used to request confirmation from customer references is as follows:

[Sample Questions to Customer Reference: "Has [the Bidder] provided your organization with the Software Solution for Option A or B?]

_____ Yes, the Bidder has provided my organization with the services described above.

--------- No, the Bidder has not provided my organization with the services described above.

--------- I am unwilling or unable to provide any information about the services described above. For each customer reference, the Bidder must, at a minimum, provide the name and either the telephone number or e-mail address for a contact person. If only the telephone number is provided, it will be used to call to request the e-mail address and the reference check will be done by e-mail.

Bidders are also requested to include the title of the contact person. It is the sole responsibility of the Bidder to ensure that it provides a contact who is knowledgeable about the services the Bidder has provided to its customer and who is willing to act as a customer reference. Crown references will be accepted.

3.3 Section II: Financial Bid

(a) **Pricing:** Bidders must submit their financial bid in accordance with the Basis of Payment in Annex B. The total amount of Applicable Taxes must be shown separately. Unless otherwise

indicated, bidders must include a single, firm, all-inclusive price quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

(b) **All Costs to be Included:** The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option to extend the Contract Period. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.

(c) **Blank Prices:** Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, $0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

(d) **Exchange Rate Fluctuation**

C3011T (2013-11-06), Exchange Rate Fluctuation

3.4 Section III: Certifications

It is a requirement that bidders submit the certifications required under Part 5.

3.5 Section IV: Additional Information

(a) **Bidder's Proposed Site(s) or Premises Requiring Safeguarding Measures**

As indicated in Part 6 under Security Requirements, the Bidder must provide the full address(es) of the Bidder's and proposed individual(s)' site(s) or premises for which safeguarding measures are required for Work Performance.

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

The Company Security Officer (CSO) must ensure through the Industrial Security Program (ISP) that the Bidder and proposal individual(s) hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.

Bidders are requested to indicate this information on their Bid Submission Form.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

(b) An evaluation team composed of representatives of the Client and PWGSC will evaluate the bids on behalf of Canada. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

(c) In addition to any other time periods established in the bid solicitation:

(i) **Requests for Clarifications:** If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

(ii) **Requests for Survey:** If Canada wishes to survey the Bidder's facilities, the Bidder must make its facilities available for this purpose within 2 working days of a request by the Contracting Authority.

(iii) **Requests for Further Information:** If Canada requires additional information in order to do any of the following pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions - Goods or Services - Competitive Requirements:

a. verify any or all information provided by the Bidder in its bid; or

b. contact any or all references supplied by the Bidder (e.g., references named in the résumés of individual resources) to verify and validate any information submitted by the Bidder,

c. the Bidder must provide the information requested by Canada within 2 working days of a request by the Contracting Authority.

(iv) **Extension of Time:** If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

4.2 Technical Evaluation

(a) **Mandatory Technical Criteria:**

(i) Each bid will be reviewed for compliance with the mandatory requirements of the bid solicitation. Any element of the bid solicitation that is identified specifically with the words "must" or "mandatory" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

(ii) The mandatory technical criteria are described in Annex B.

(iii) The Mandatory Security Technical criteria are described in Annex G.

(iv) Claims in a bid that a future upgrade or release of any of product included in the bid will meet the mandatory requirements of the bid solicitation, where the upgrade or release is not available at bid closing, will not be considered.

(b) **Point-Rated Technical Criteria:**

(i) Each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly. The point-rated technical criteria are described under “Solution Rated Requirements” in Annex "A" – Statement of Requirements.

(ii) Each bid that meets all the Mandatory Security Technical Criteria described in Annex G will be rated by assigning a score for the Point-Rated Criteria for Security Mandatory Technical Criteria as described in Annex H.

(c) **Reference Checks:**

(i) For reference checks, Canada will conduct the reference check in writing by e-mail. Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day using the e-mail address provided in the bid. Canada will not award any points and/or a bidder will not meet the mandatory experience requirement (as applicable) unless the response is received within 5 working days of the date that Canada's e-mail was sent.

(ii) On the third working day after sending out the reference check request, if Canada has not received a response, Canada will notify the Bidder by e-mail, to allow the Bidder to contact its reference directly to ensure that it responds to Canada within 5 working days. If the individual named by a Bidder is unavailable when required during the evaluation period, the Bidder may provide the name and e-mail address of an alternate contact person from the same customer. Bidders will only be provided with this opportunity once for each customer, and only if the originally named individual is unavailable to respond (i.e., the Bidder will not be provided with an opportunity to submit the name of an alternate contact person if the original contact person indicates that he or she is unwilling or unable to respond). The Bidder will have 24 hours to submit the name of a new contact. That contact will again be given 5 working days to respond once Canada sends its reference check request.

(iii) Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated.

(iv) Points will not be allocated and/or a bidder will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder instead of being a customer of the Bidder itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder.

(v) Whether or not to conduct reference checks is discretionary. However, if PWGSC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all bidders who have not, at that point, been found non-responsive.

(d) **Proof of Proposal Test for Top-Ranked Bid:**

Through the Proof of Proposal (PoP) test, Canada may test the solution proposed in the top-ranked bid (identified after the financial evaluation) to confirm both that it will function as described in the bid and that it meets the technical functionality requirements described in Annex A – Statement of Requirement (SOR). The PoP test will take place at a site in the National Capital Region provided by Canada that recreates the technical environment described in the SOR, if that location is agreed to by the Contracting Authority and if the Bidder assumes all responsibility for recreating the technical environment described in the SOR (it is within the Contracting Authority's sole discretion to determine whether the Bidder has accurately recreated this environment for the test). Canada will pay its own travel and salary costs associated with any PoP test.

After being notified by the Contracting Authority, the Bidder will be given a maximum of 7 working days to start the installation of the proposed solution. The installation must be

completed and functional within 5 working days of the Bidder starting the installation (7.5 hrs/day during normal working hours, to be determined by the Contracting Authority). Canada will then conduct the PoP test. Up to 2 representatives of the Bidder may be present during the PoP test. The representative(s) named in the bid to provide technical support during the PoP test should be available by telephone for technical advice and clarification during the PoP test; however, Canada is not required to delay the PoP test if an individual is unavailable. Once the PoP test has begun, it must be completed within 3 working days. Working days are Monday to Friday during the hours of 9:00 am to 5:00 pm.

Canada will document the results of the PoP Test. If Canada determines that the proposed solution does not meet any mandatory requirement of the bid solicitation, the bid will fail the PoP Test and the bid will be disqualified. Canada may, as a result of the PoP test, reduce the score of the Bidder on any rated requirement, if the PoP test indicates that the score provided to the Bidder on the basis of its written bid is not validated by the PoP test. The Bidder's score will not be increased as a result of the PoP test. If the Bidder's score is reduced as a result of the PoP test, Canada will reassess the ranking of all bidders.

In connection with the PoP testing, the Bidder grants to Canada a limited license to use the Bidder's proposed software solution for testing and evaluation purposes.

If, during the initial installation of the software for the PoP test, the Bidder discovers that there are missing and/or corrupt files for software components identified in the technical bid, the Bidder must cease the installation process and inform the Contracting Authority. If the Contracting Authority determines that the missing and/or corrupt files are for components identified in the technical bid, the Bidder may be permitted to submit to the Contracting Authority the missing files and/or replacements for the corrupt files on electronic media or by referring to a web site where the files can be downloaded. These files must have been commercially released to the public before the bid closing date. Upon receiving the files on electronic media or downloading them from a corporate web site, the Contracting Authority will verify that (i) the files were commercially released to the public before the bid closing date; (ii) the files do not include new releases or versions of the software; (iii) the files belong to software components identified in the technical bid; and (iv) the software will not need to be recompiled to make use of the files. The Contracting Authority will have the sole discretion to decide if the additional files may be installed for the PoP test. Under no circumstances will files required to correct flaws in the software programming or code be permitted. This process can be used only a single time, and only during the initial installation of the software for the PoP test.

4.3 Financial Evaluation

(a) **Mandatory Financial Criteria**

The financial evaluation will be conducted by calculating the Total Bid Price using the Pricing Tables completed by the bidders.

TABLE A - TOTAL BID PRICE (TBP) FOR EVALUATION PURPOSES			
ITEM NO.	**DESCRIPTION**	**FORMULA**	**TOTAL PRICE**

1	For the provision of a commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, maintenance and support services, and training for 100 user licenses as detailed in Table 1 of Annex C.	Total from Table 1 of Annex C	**$**
2	During the initial contract period, for the provision of commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, training, and maintenance and support services for 100 user licenses as detailed in Table 2 of Annex C.	Total from Table 2 of Annex C	**$**
3	During the optional periods of the Contract, for the provision of commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, training, maintenance and support services for 100 user licenses as detailed in Table 3 of Annex C.	Total from Table 3 of Annex C	**$**
4	For the optional additional users as detailed in Table 4 of Annex C.	Total from Table 4 of Annex C	**$**
		Total Bid Price (TBP) - (sum of Column A):	**$**

SACC Manual Clause A0220T (2014-06-26), Evaluation of Price - Bid

SACC Manual Clause A0222T (2014-06-26), Evaluation of Price – Canadian/Foreign Bidders

(b) Formulae in Pricing Tables

If the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a Bidder.

4.4 Basis of Selection

(a) To be declared responsive, a bid must:

(i) comply with all the requirements of the bid solicitation;

(ii) meet all mandatory criteria.

(b) Bids not meeting (i) and (ii) will be declared non-responsive.

(c) The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70% for the technical merit and 30% for the price.

(d) To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70%.

(e) To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30%.

(f) For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

(g) Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

Overall Score is based on 70% Technical and 30% Financial

Formula: Overall Score (by Bidder) / Max. Points on Rated Requirements X 70 = Total 1 (Technical)

Formula: TBP of the Lowest priced responsive proposal / Bidder's Total Bid Price (TBP) X 30 = Total 2 (Financial)

The table below illustrates an **example** where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of technical merit and price, respectively. The total available points equals 135 and the lowest evaluated price is $45,000 (45).

Basis of Selection - Highest Combined Rating Technical Merit (70%) and Price (30%)				
		Bidder 1	**Bidder 2**	**Bidder 3**
Overall Technical Score		115/135	89/135	92/135
Bid Evaluated Price		$55,000.00	$50,000.00	$45,000.00
Calculations	**Technical Merit Score**	115/135 x 70 = 59.63	89/135 x 70 = 46.15	92/135 x 70 = 47.70
	Pricing Score	45/55 x 30 = 24.54	45/50 x 30 = 27	45/45 x 30 = 30
Combined Rating		84.17	73.15	77.7
Overall Rating		1st	3rd	2nd

(h) Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

If more than one bidder is ranked first because of identical overall scores, then the bidder with the best technical score will become the top-ranked bidder.

PART 5 - CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with Bid

Bidders must submit the following duly completed certifications as part of their bid.

(a) **Declaration of Convicted Offences**

As applicable, pursuant to subsection Declaration of Convicted Offences of section 01 of the Standard Instructions, the Bidder must provide with its bid, the completed Declaration Form to be given further consideration in the procurement process.

5.2 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid, but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame provided will render the bid non-responsive.

(a) **Integrity Provisions – List of Names**

Bidders who are incorporated, including those bidding as a joint venture, must provide a complete list of names of all individuals who are currently directors of the Bidder.

Bidders bidding as sole proprietorship, as well as those bidding as a joint venture, must provide the names of the owner(s).

Bidders bidding as societies, firms or partnerships do not need to provide lists of names.

(b) **Federal Contractors Program for Employment Equity - Bid Certification**

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list (http://www.labour.gc.ca/eng/standards_equity/eq/emp/fcp/list/inelig.shtml) available from Employment and Social Development Canada (ESDC) - Labour's website.

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list at the time of contract award.

(c) **Bidder Certifies that All Equipment and Software is "Off-the-Shelf"**

Any equipment and software bid to meet this requirement must be "off-the-shelf" (unless otherwise stated in this bid solicitation), meaning that each item of equipment and software is

commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the equipment or software bid is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the bid closing date. By submitting a bid, the Bidder is certifying that all the equipment and software bid is off-the-shelf.

(d) **Software Publisher Certification and Software Publisher Authorization**

If the Bidder is the Software Publisher for any of the proprietary software products it bids, Canada requires that the Bidder confirm in writing that it is the Software Publisher. Bidders are requested to use the Software Publisher Certification Form included with the bid solicitation. Although all the contents of the Software Publisher Certification Form are required, using the form itself to provide this information is not mandatory. For bidders who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the bid being declared non-responsive.

Any Bidder that is not the Software Publisher of all the proprietary software products proposed in its bid is required to submit proof of the Software Publisher's authorization, which must be signed by the Software Publisher (not the Bidder). No Contract will be awarded to a Bidder who is not the Software Publisher of all of the proprietary software it proposes to supply to Canada, unless proof of this authorization has been provided to Canada. If the proprietary software proposed by the Bidder originates with multiple Software Publishers, authorization is required from each Software Publisher. Bidders are requested to use the Software Publisher Authorization Form included with the bid solicitation. Although all the contents of the Software Publisher Authorization Form are required, using the form itself to provide this information is not mandatory. For Bidders/Software Publishers who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the bid being declared non-responsive.

In this bid solicitation, "Software Publisher" means the owner of the copyright in any software products proposed in the bid, who has the right to license (and authorize others to license/sub-license) its software products.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

In addition to Part 6 – Security, Financial and Other Requirements and Annex D – Security Requirements Check List, the Bidder must comply with Annex E – Government of Canada Security Control Profile for Cloud-based GC Services.

6.1 Security Requirement – For Canadian Supplier:

(a) Before award of a contract, the following conditions must be met:

(i) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

(ii) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses; and

(iii) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

(iv) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

(v) the Bidder must provide the address(es) of proposed site(s) or premises of work performance and document safeguarding as indicated in Part 3 - Section IV, Additional Information.

(b) Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

(c) For additional information on security requirements, Bidders should refer to the Industrial Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

(d) In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

6.2 Security Requirement – For Foreign Suppliers:

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority confirming Bidder compliance with the security requirements for foreign suppliers. The following security requirements apply to the Bidder incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing the Work described in the SOW and is in addition to the Government of Canada Security Control Profile for Cloud-based GC Services (Annex E), and is in addition to those requirements already identified in section 7.5.1 Protection and Security of Data Stored in Databases.

a) The Foreign recipient Bidder must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral

security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

b) The Bidder must provide proof that they are incorporated or authorized to do business in their jurisdiction as indicated in Part 7 - Resulting Contract Clauses.

c) The Bidder must be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business, as indicated in Part 7 - Resulting Contract Clauses, 7.5(b) Security Requirement for Foreign Suppliers, clause (9).

d) The Bidders must provide assurance that it can receive and store **CANADA PROTECTED A and B** information/assets on its site or premises as indicated in Part 7 – Resulting Contract Clauses, Annex E and the listed IT Security Requirements.

e) The Bidder's proposed location of work performance must meet the security requirement as indicated in Part 7 – Resulting Contract Clauses.

f) The Bidder must provide the address(es) of proposed location(s) of work performance and document safeguarding.

g) The successful Bidder's proposed individuals requiring access to **CANADA PROTECTED** information/assets or restricted work sites must EACH hold a valid Criminal Record Check, with favorable results, from a recognized governmental agency or private sector organization **in their country**, as well as a Background Verification, validated by the Canadian DSA.

h) The successful Bidder's proposed individuals must not begin the Work until all requisite security requirements have been met. The approved verifications for the required Criminal Record Check and Background Verifications are listed at Annex F – Security Screening Requirements.

i) In the case of a joint venture Bidder, each member of the joint venture must meet the security and privacy requirements.

j) The Bidders must provide proof that all the databases including the backup database used by organizations to provide the services described in the SOW containing any **CANADA PROTECTED** information, related to the Work, are located in Canada.

k) The successful Bidder MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer **system any CANADA PROTECTED A or B** information/assets until authorization to do so has been confirmed by the Canadian DSA.

l) The Bid must clearly indicate the Work which the Bidder plans to subcontract. All subcontracting arrangements which provide the subcontractor with access to any Personal Information are subject to approval by Canada. The description of subcontracting arrangements should demonstrate how the Bidder will ensure that all requirements, terms, conditions, and clauses of the subcontract are met.

m) In the event that a foreign Bidder is chosen as a supplier for this contract, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Government of Canada Contracting Authority, to ensure compliance with the security provisions

6.3 Financial Capability

(a) SACC Manual clause A9033T (2012-07-16) Financial Capability applies, except that subsection 3 is deleted and replaced with the following: "If the Bidder is a subsidiary of another company, then any financial information required by the Contracting Authority in 1(a)

to (f) must also be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Bidder; however, if the Bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the Bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the Bidder's financial capability because its financial information has been combined with its parent's, Canada may, in its sole discretion, award the contract to the Bidder on the condition that one or more parent companies grant a performance guarantee to Canada."

(b) In the case of a joint venture bidder, each member of the joint venture must meet the financial capability requirements.

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Requirement

a) [Contractor's Name] agrees to supply to the Client a Licensed Software Subscription Services to access the hosted_____ [Name of the Application] that meet all the requirements and specifications contained in the Contract, including the Statement of Requirements, in accordance with and at the prices set out in the Contract. This includes:

i. granting access licenses through the Licensed Software Subscription Services to the _____ [Name of the Application]

ii. providing the Software Documentation;

iii. providing Licensed Software Subscription Services Support during the Contract Period, plus any period during which the Licensed Software Subscription Services are extended pursuant to the irrevocable options granted to Canada below;

iv. deliver back-up data to the Client no less than once a month during the Contract Period and at the end of the Contract Period in a standard format approved by the Technical Authority

v. providing training, as and when requested by Canada described herein, to one or more locations to be designated by Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.

b) **Client**: Under the Contract, the "**Client**" is Immigration, Refugees and Citizenship Canada (IRCC).

c) **Reorganization of Client:** The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

d) **Defined Terms:** Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions. Also, the following words and expressions have the following meanings:

i. any reference to a "**deliverable**" or "**deliverables**" includes, the license to use the Licensed Software (the Licensed Software itself is not a deliverable, because the Licensed Software is only being licensed under the Contract, not sold or transferred).

7.2 Optional Goods and/or Services

(a) The Contractor grants to Canada the irrevocable option to acquire the goods, services or both described at Annex B – Basis of Payment of the Contract under the same terms and conditions and at the prices and/or rates stated in the Contract. The option may only be exercised by the Contracting Authority by notice in writing and will be evidenced, for administrative purposes only, through a contract amendment.

(b) The Contracting Authority may exercise the option at any time before the expiry of the Contract by sending a written notice to the Contractor.

7.3 License to the Software Subscription Services

a) Licensed Software Subscription Services: The Contractor hereby agrees that the Licensed Software Subscription Services will include the use of all Software required to enable the Client to use all the features and functionality, including but not limited the use and access to all agents, host agents, access licenses, drivers, application program interfaces, adapters, connectors, plug-ins, software development tool kits and management console hosted by the Contractor.

b) The Contractor must provide hosted Licensed Software Subscription Services, includes the following software products:

_____

_____

_____

c) Type of License being Granted: Licensed Software Services;

d) Term of the License: Subscription (annual);

e) Initial Requirement:

f) Language of Licensed Software Services: English and French;

g) Media on which Canada's Data must be Delivered: Internet download via Secure Network or HTTPS protocol as requested by Canada;

h) Additional Rights: This Licensed Software Subscription Services includes the right for Canada to use the _____ [Name of the Application], which includes the rights:

i) to access and use all the hosted software products that form part of _____ [Name of the Application] from as many locations (off-site workplaces or work environments "in the field", and in-home work environments for the Client's business purposes) as the Client sees fit;

ii) to use English and French versions (if available, these must be the "Canadian English" and "Canadian French" versions);

iii) to grant access through an internet browser using internet, intranet and extranet environments or any other connections to anyone who uses the services and programs provided by Canada (regardless of their location) to access, view, enter, search, exchange and read information held and created by the Client using the hosted _____ [Name of the Application];

iv) to make this use by way of a network, the Internet, an intranet, an extranet, a virtual private network (VPN), an inter-network, or such other means as may become

possible from time to time so that users have "universal access rights" (i.e., a right to access the Licensed Software Subscription Services by any means from any location as may become possible from time to time), whether their means of access is secure, wireless, mobile or by any other means available from time to time;

v) to make this use regardless of the operating systems, software applications and Application Programming Interface(s) (API) that the Client may be using from time to time; however, Canada acknowledges that the Contractor is not granting any license rights to software other than the Licensed Software Subscription Services; and

vi) to continue to use the Licensed Software Subscription Services regardless of any changes made at any given time, including but not limited to changes in the operating system, other applications, hardware, peripherals or devices with which the Licensed Software Subscription Services operates; however, the Contractor is not required to deliver a new or different version of the Licensed Software Subscription Services to enable the Client Users to continue to use the Licensed Software Subscription Services in a different environment than the one(s) described in the Contract.

i) Representation and Warranty: The Contractor warrants and represents that the Licensed software subscription services meets or exceeds all the Specifications.

j) Licensed Software Subscription Services Maintenance: The Contractor must as part of the Licensed Software Subscription Services" upgrade the hosted _____ [Name of the Application] with the most recent release(s) and version(s) of the software products, to ensure that it meets the requirements of the Contract and Statement of Requirements. These releases(s) and version(s) means all commercially available enhancements, extensions, improvements, upgrades, updates, releases, versions, renames, rewrites, cross-grades, components and back grades or other modifications to the Licensed Software Subscription Services developed by the Contractor or its licensor.

k) Licensed Software Subscription Services Support: This includes the following Technical Hotline Support and Web Support services:

i) Technical Hotline Support: The Contractor must provide the Technical Hotline Support through the Contractor's toll-free hotline at _____, in English and French, 24 hours a day, 7 days a week. The Contractor must answer with a live service agent at the time of the Client's User's initial call within an average of one minute of the call being received by the Contractor. The Contractor's personnel must be qualified and able to respond to the Client's and any Client User's questions and, to the extent possible, be able to resolve user problems over the telephone and provide advice regarding configuration problems. In addition, the Contractor must be able to:

Provide information and advice to Users and Administrators;

Create and transmit Messages on behalf of Client's Users and Administrator to all Contacts if requested by the Client; and

Ensure the resolution of technical problems.

ii) Web Support: The Contractor must provide Canada with technical web support services through a website that must include, as a minimum, frequently asked questions and on-line software diagnostic routines, support tools, and services. The Contractor's website must provide support in English and French. The Contractor's website must be available to Canada's users 24 hours a day, 365 days a year, and must be available 99% of the time. The Contractor's website address is _____.

7.4 License Grant

a) **License Grant**. The Contractor hereby grants to Canada, including to all Canada's Users, a non-exclusive, non-sublicensable, non-assignable, royalty-free, and worldwide license to access and use the Hosted On-Line Survey Solution (the "Software").

b) **Right to Transfer**. Canada may transfer license rights, within the license limits of the Software to any Canadian government department, corporation, or agency as defined in the *Financial Administration Act*, R.S.C. 1985, c. F-11, as amended from time to time, or to any other party for which the Department of Public Works and Government Services Canada has been authorized to act under section 16 of the *Department of Public Works and Government Services Act*, S.C. 1996, c. 16, provided the Contracting Authority informs the Contractor in writing of the transfer within 30 calendar days of the transfer.

c) **Right to License**. The Contractor guarantees

(a) it has the right to grant the rights in this Contract,

(b) it has all necessary consents, and

(c) this Contract contains the only terms between the parties with respect to the Software.

d) **"Shrink-Wrap" or "Click-Wrap" Conditions**. The Contractor agrees that Canada is not bound by and does not accept any "shrink-wrap" or "click-wrap" conditions or any other conditions, express or implied, that are contained in the Software or conditions that may accompany the Software or Work in any manner, regardless of any notification to the contrary.

e) **Software Documentation**

(a) The Contractor guarantees that the Software Documentation contains enough detail to permit a User to access, test and use all features of the Software.

(b) Canada has the right to translate the Software Documentation into English or French. Canada owns any translation and is under no obligation to provide it to the Contractor. Canada will include any copyright and/or proprietary right notice that was part of the original document in any translation. The Contractor is not responsible for technical errors that arise as a result of any translation made by Canada.

(c) The Contractor must maintain, update and provide Canada with access to the Software Documentation throughout the Contract Period. The Software Documentation should reflect the most current release level consistent with the Software accessed under the Contract.

d) **Client**. The initial Client is Immigration, Refugees and Citizenship Canada (IRCC). The Contracting Authority can add additional Clients from time to time, which may include any department or Crown corporation as described in the *Financial Administration Act* (as amended from time to time), and any other party for which the Department of Public Works and Government Services may be authorized to act from time to time under section 16 of the *Department of Public Works and Government Services Act*.

7.5 Software Support Services

Support Services. The Contractor must provide the following support services (collectively the "Support Services").

(a) **Technical Support**. The Contractor must provide (i) telephone support in English and French available during business hours and (ii) web support available 24 hours a day, 365 days a year excepting maintenance downtime not to exceed 1% of the time.

(b) **Maintenance**. The Contractor must apply (i) all upgrades, updates, new releases, and other enhancements; (ii) all extensions and other modifications; (iii) all bug fixes and software patches; and (iv) all application program interfaces (APIs), plug-ins, and applets.

7.5.1 **Error Resolution**

a) **Error Response**. Upon receipt of a report of a failure from Canada, unless provided otherwise in the Contract, the Contractor must use all reasonable efforts to provide Canada within the time frames established in this section, with a correction of the Software Error which caused the failure. All Software Error corrections will become part of the Software and will be subject to the conditions of Canada's license with respect to the Software.

b) **Error Resolution**

(i) **Severity 1**: In the event of total inability to use the Software, resulting in a critical impact on user objectives, then on notification by Canada to the Contractor, the Contractor must begin continuous work on the issue and provide reasonable effort for workaround or solution within 24 hours.

(ii) **Severity 2**: In the event that user operation of the Software is seriously restricted, the Contractor must work during normal business hours to provide reasonable effort for workaround or solution within 72 hours.

(iii) **Severity 3**: In the event that user operation of the Software is limited, but not critical to overall to overall user operations, the Contractor must work during normal business hours to provide reasonable effort for workaround or solution within 14 days.

(iv) **Severity 4**: In the event of all other issues affecting user operation of the Software, the Contractor must work during normal business hours to provide reasonable effort for workaround or solution within 90 days

7.6 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual issued by Public Works and Government Services Canada (PWGSC). The Manual is available on the PWGSC Website: https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual/all.

(a) **General Conditions**:

(i) 2030 (2018-06-21), General Conditions - Higher Complexity - Goods, apply to and form part of the Contract.

(b) **Supplemental General Conditions**:

The following Supplemental General Conditions:

(i) 4008 (2008-12-12), Supplemental General Conditions - Personal Information, apply to and form part of the Contract.

(c) **SACC Manual Clauses**

(i) A9122C (2008-05-12), Protection and Security of Data Stored in Databases; and,

apply to and form part of the Contract.

7.7 Security Requirement

The following security requirements apply and forms part of the Contract.

In addition to 7.5 Security Requirement and Annex D – Security Requirements Check List, the Contractor must comply with Annex E – Government of Canada Security Control Profile for Cloud-based GC Services.

(a) Canadian Contractor

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC**).**

2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CISD/PWGSC.

3. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store **PROTECTED** information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED B.

4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.

5. The Contractor/Offeror must comply with the provisions of the:

   a) Security Requirements Check List and security guide (if applicable), attached at Annex D;

   b) Industrial Security Manual (Latest Edition)

(b) Foreign Contractor

All **CANADA PROTECTED** information/assets, furnished to the **Contractor/Subcontractor** or produced by the **Contractor/Subcontractor**, must be safeguarded as follows:

1. The Foreign recipient **Contractor / Subcontractor** must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

2. Any and/or all Canadian subcontractors must at all times during the performance of the Contract and/or subcontract, hold a valid Designated Organization Screening with approved Document Safeguarding at the level of **PROTECTED B**, issued by the Canadian Industrial Security Directorate CISD/PWGSC.

3. The **Contractor/Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

4. The Foreign recipient **Contractor / Subcontractor** must provide assurance that it can receive and store **CANADA PROTECTED** information/assets on its site or premises as indicated in Part 7 and as listed in the IT Security Requirements.

5. The Foreign recipient **Contractor's / Subcontractor's** location of work performance must meet the security requirements as listed in the IT Security Requirements.

6. The Foreign recipient **Contractor / Subcontractor** must not begin the work, services or performance until the Canadian Designated Security Authority (DSA) is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the Foreign recipient **Contractor / Subcontractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

7. The Foreign recipient **Contractor / Subcontractor** must provide the **CANADA PROTECTED** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.

8. During the period of **Contract/Subcontract**, the **Contractor/Subcontractor** must retain all personal information furnished or produced pursuant to this **Contract/Subcontract**. Upon completion of the Work, the **Contractor/Subcontractor** must return to the Government of Canada, all Personal Information furnished or produced pursuant to this **Contract/Subcontract**, including all Personal Information released to and/or produced by its subcontractors".

9. The **Contractor/Subcontractor** must at all times during the performance of the **Contract/Subcontract** be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business. The **Contractor/Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and Contracting Security Authority and identify the relevant national Privacy Authority. For European **Contractors/Subcontractors**, this will be the national Data Protection Authority (DPA).

10. The **Contractor/Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this **Contract/Subcontract**. This individual will be appointed by the proponent **Contractor's/Subcontractor's** Chief Executive Officer (CEO) or Designated Key Senior Official, defined as an owner, officer, director, executive, and/or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the **Contract/Subcontract**.

11. The Foreign recipient **Contractor/ Subcontractor** must not grant access to **CANADA PROTECTEDA or B** information/assets, except to its personnel subject to the following conditions:

    a. Personnel have a need-to-know for the performance of the **contract / subcontract**;

    b. Personnel have been subject to a Criminal Record Check, with favorable results, from a recognized Governmental agency in **their country** as well as a Background Verification, validated by the Canadian DSA. The approved verifications for the required Criminal Record Check and Background Verification are listed at Annex F;

    c. The Foreign recipient **Contractor / Subcontractor** must ensure that personnel provide consent to share results of the Criminal record Background Check with the Canadian DSA and other Canadian Government Officials, if requested; and

d. The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a Foreign recipient **Contractor / Subcontractor** for cause.

12. The **Contractor/Subcontractor** acknowledges and agrees that its obligations to safeguard, manage, and protect all Personal Information under the **Contract/Subcontract** are in addition to any obligations it has under national privacy legislation of the country(ies) in which it is incorporated or operates.

13. All Personal Information, provided to the **Contractor/Subcontractor** or produced by the **Contractor/Subcontractor**, must:

    a) not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **Contract/Subcontract**, without the prior written consent of Canada. Such consent must be sought from its national DPA, the Contracting Authority and Contracting Security Authority (in collaboration with the Canadian DSA); and

    b) not be used for any purpose other than for the performance of the **Contract/Subcontract** without the prior written approval Canada. This approval must be obtained by contacting its national DPA, the Contracting Authority and Contracting Security Authority (in collaboration with the Canadian DSA).

14. The **Contractor/Subcontractor** must immediately report to its respective national DPA and the Contracting Authority (in collaboration with the Canadian DSA), all cases in which it is known or there is reason to suspect that any Personal Information provided or generated pursuant to this **Contract/Subcontract** have been lost, or in contravention of these security requirements, accessed, used or disclosed to unauthorized persons.

15. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.

16. The **Contractor and/or any and all subcontractors** must ensure that the appropriate security clauses, as determined by the Canadian DSA, are inserted in all subcontracts that involve access to Personal Information provided to or generated under this Contract and/or subcontract and must ensure that the conditions placed on a subcontractor are no less favorable to Canada than the conditions set out in these security requirements.

17. The Foreign recipient **Contractor / Subcontractor** must ensure that all the databases including the backup database used by organizations to provide the services described in the SOW containing any **CANADA PROTECTED** information, related to the Work, are located within Canada.

18. The **Contractor/Subcontractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system any **PROTECTED A or B** information until authorization to do so has been confirmed by the Canadian DSA.

    See Annex E for Government of Canada Security Control Profile for Cloud-based GC Services.

19. The **Contractor/Subcontractor** must not use the Personal Information for any purpose other than for the performance of the **Contract/Subcontract** without the prior written approval of Canada. This approval must be obtained from the Canadian Designated Security Authority DSA.

20. The Foreign recipient **Contractor / Subcontractor** requiring access to Canadian Government site(s), under this contract, must submit a Request for Site Access to the Departmental Security Officer of the Immigration, Refugees and Citizenship Canada.

21. In the event that a foreign **Contractor/Subcontractor** is chosen as a supplier for this **Contract/Subcontract**, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Contracting Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

22. The Foreign recipient **Contractor / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex D.

(d) **Contractor's Site(s) or Premises Requiring Safeguarding Measures**

The Contractor must diligently maintain up-to-date, the information related to the Contractor's and individual(s) site(s) or premises, where safeguarding measures are required in the performance of the Work, for the following addresses:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

The Company Security Officer (CSO) must ensure through the Industrial Security Program (ISP) that the Contractor and individual(s) hold a valid security clearance at the required level.

7.8 PROTECTION AND SECURITY OF DATA STORED IN DATABASES

1. The **Contractor/Subcontractor** must ensure that all the databases (used by organizations to provide the services described in Annex A – SOW) containing any Personal Information, related to the Work, are located in Canada.
2. The **Contractor/Subcontractor** must control access to all databases on which any data relating to the **Contract/Subcontract** is stored so that only individuals with the appropriate security screening are able to access the database, either by using a password or other form of access control (such as biometric controls).
3. The **Contractor/Subcontractor** must ensure that all databases on which any data relating to the **Contract/Subcontract** is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases, unless those databases are located in Canada
4. The **Contractor/Subcontractor** must ensure that all data relating to the **Contract/Subcontract** is processed only in Canada or in another country approved by the Contracting Authority under subsection 1.
5. The **Contractor/Subcontractor** must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection 1.
6. Despite any section of the General Conditions relating to subcontracting, the **Contractor/Subcontractor** must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the **Contract** unless the Contracting Authority first consents in writing.

7.8.1 PERSONAL INFORMATION

1. Interpretation

a. In the **Contract/Subcontract**, unless the context otherwise requires,

"General Conditions" means the general conditions that form part of the **Contract/Subcontract**;

"Personal Information" means information about an individual, including the types of information specifically described in the *Privacy Act*, R.S. 1985, c. P-21;

"Record" means any hard copy document or any data in a machine-readable format containing Personal Information;

Words and expressions defined in the General Conditions and used in these supplemental general conditions have the meanings given to them in the General Conditions.

b. If there is any inconsistency between the General Conditions and these supplemental general conditions, the applicable provisions of these supplemental general conditions prevail.

2. Ownership of Personal Information and Records

To perform the Work, the **Contractor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The **Contractor/Subcontractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the **Contractor/Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

3. Use of Personal Information

The **Contractor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain, and dispose of the Personal Information and the Records only to perform the Work in accordance with the **Contract/Subcontract**.

4. Collection of Personal Information

1. If the **Contractor/Subcontractor** must collect Personal Information from a third party to perform the Work, the **Contractor/Subcontractor** must only collect Personal Information that is required to perform the Work. The **Contractor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the **Contractor/Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:

   a. that the Personal Information is being collected on behalf of, and will be provided to, Canada;
   b. the ways the Personal Information will be used;
   c. that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;
   d. the consequences, if any, of refusing to provide the information;
   e. that the individual has a right to access and correct his or her own Personal Information;
   f. that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the **Contractor/Subcontractor**.

2. The **Contractor**, its subcontractors, and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

3. If requested by the Contracting Authority, the **Contractor/Subcontractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The **Contractor/Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The **Contractor** must also obtain the Contracting Authority's approval before making any changes to a form or script.

4. At the time it requests Personal Information from any individual, if the **Contractor/Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the **Contractor/Subcontractor** must ask the Contracting Security Authority for instructions.

5. Maintaining the Accuracy, Privacy and Integrity of Personal Information

The **Contractor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The **Contractor/Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the **Contractor/Subcontractor** must:

a. not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;
b. segregate all Records from the **Contractor's/Subcontractor's** own information and records;
c. restrict access to the Personal Information and the Records to people who require access to perform the Work (for example, by using passwords or biometric access controls);
d. provide training to anyone to whom the **Contractor/Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Work. The **Contractor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the **Contractor/Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;
e. if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the **Contractor/Subcontractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;
f. keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);
g. include a notation on any Record(s) that an individual has requested be corrected if the **Contractor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the **Contractor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the **Contractor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the **Contractor/Subcontractor** must do so;
h. keep a record of the date and source of the last update to each Record;

i. maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the **Contractor/Subcontractor** and Canada at any time; and

j. secure and control access to any hard copy Records.

6. Safeguarding Personal Information

The **Contractor/Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the **Contractor/Subcontractor** must:

a. store the Personal Information electronically so that a password (or a similar access control mechanism, such as biometric access) is required to access the system or database in which the Personal Information is stored;

b. ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;

c. not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Contracting Security Authority has first consented in writing;

d. safeguard any database or computer system on which the Personal Information is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information;

e. maintain a secure back-up copy of all Records, updated at least weekly;

f. implement any reasonable security or protection measures requested by Canada from time to time; and

g. notify the Contracting Authority and the Contracting Security Authority immediately of any security breaches; for example, any time an unauthorized individual accesses any Personal Information.

7. Appointment of Privacy Officer

The **Contractor/Subcontractor** must appoint someone to be its privacy officer and to act as its representative for all matters related to the Personal Information and the Records. The **Contractor/Subcontractor** must provide that person's name to the Contracting Authority and the Contracting Security Authority within ten (10) days of the award of the **Contract/Subcontract**.

8. Quarterly Reporting Obligations

Within (30) calendar days of the end of each quarter (January-March; April-June; July-September; October-December), the **Contractor/Subcontractor** must submit the following to the Contracting Authority:

a. a description of any new measures taken by the **Contractor/Subcontractor** to protect the Personal Information (for example, new software or access controls being used by the **Contractor/Subcontractor**;

b. a list of any corrections made to Personal Information at the request of an individual (including the name of the individual, the date of the request, and the correction made);

c. details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the **Contractor/Subcontractor**; and

d. a complete copy (in an electronic format agreed to by the Contracting Authority and the **Contractor/Subcontractor** of all the Personal Information stored electronically by the **Contract/Subcontract**.

9. Threat and Risk Assessment

Within ninety (90) calendar days of the award of the **Contract/Subcontract** and, if the **Contract/Subcontract** lasts longer than one year, within thirty (30) calendar days of each anniversary date of the **Contract/Subcontract**, the **Contractor/Subcontractor** must submit to the Contracting Authority and the Contracting Security Authority a threat and risk assessment, which must include:

a. a copy of the current version of any request for consent form or script being used by the **Contractor/Subcontractor** to collect Personal Information;

b. a list of the types of Personal Information used by the **Contractor/Subcontractor** in connection with the Work;

c. a list of all locations where hard copies of Personal Information are stored;

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

e. a list of every person to whom the **Contractor/Subcontractor** has granted access to the Personal Information or the Records;

f. a list of all measures being taken by the **Contractor/Subcontractor** to protect the Personal Information and the Records;

g. 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

h. an explanation of any new measures the **Contractor/Subcontractor** intends to implement to safeguard the Personal Information and the Records.

10. Audit

Canada may audit the **Contractor's/Subcontractor's** compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the **Contractor/Subcontractor** must provide Canada (or Canada's authorized representative) with access to its premises and to the Personal Information and Records at all reasonable times. If Canada identifies any deficiencies during an audit, the **Contractor/Subcontractor** must immediately correct the deficiencies at its own expense.

(a) **Accounts and Records**. The Contractor must keep proper accounts and records of the cost of performing the Work and of all expenditures or commitments made by the Contractor in connection with the Work, including all invoices, receipts and vouchers. The Contractor must retain records, including bills of lading and other evidence of transportation or delivery, for all deliveries made under the Contract.

(b) **Time Records**. If the Contract includes payment for time spent by the Contractor, its employees, representatives, agents or subcontractors performing the Work, the Contractor must keep a record of the actual time spent each day by each individual performing any part of the Work.

(c) **Retention of Records**. Unless Canada has consented in writing to its disposal, the Contractor must retain all the information described in this section for six years after it receives the final payment under the Contract, or until the settlement of all outstanding claims and disputes, whichever is later. During this time, the Contractor must make this information available for audit, inspection and examination by the representatives of Canada, who may make copies and take extracts. The Contractor must provide all reasonably required facilities for any audit and inspection and must furnish all the information as the representatives of Canada may from time to time require to perform a complete audit of the Contract.

(d) **Government Audit**. The amount claimed under the contract is subject to government audit both before and after payment is made. If an audit is performed after payment, the Contractor agrees to repay any overpayment immediately on demand by Canada. Canada may hold back, deduct and set off any credits owing and unpaid under this section from any money that Canada owes to the Contractor at any time (including under other contracts). If Canada does not choose to exercise this right at any given time, Canada does not lose this right

11. Statutory Obligations

a. The **Contractor/Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, *Access to Information Act*, R.S. 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The **Contractor/Subcontractor** agrees to comply with any requirement established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

b. The **Contractor/Subcontractor** acknowledges that its obligations under the **Contract/Subcontract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the **Contractor/Subcontractor** believes that any obligations in the **Contract/Subcontract** prevent it from meeting its obligations under any of these laws, the **Contractor/Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **Contract/Subcontract** and the specific obligation under the law with which the **Contractor/Subcontractor** believes it conflicts.

12. Disposing of Records and Returning Records to Canada

The **Contractor/Subcontractor** must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Work involving the Personal Information is complete, the **Contract/Subcontract** is complete, or the **Contract/Subcontract** is terminated, whichever of these comes first, the **Contractor/Subcontractor** must return all Records (including all copies) to the Contracting Authority.

13. Legal Requirement to Disclose Personal Information

Before disclosing any of the Personal Information pursuant to any applicable legislation, regulation, or an order of any court, tribunal or administrative body with jurisdiction, the **Contractor/Subcontractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

14. Complaints

Canada and the **Contractor/Subcontractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

15. Exception

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the **Contractor** or any of its subcontractors, agents, or representatives, or any of their employees

7.9 Contract Period

a) **Contract Period:** The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

The "**Initial Contract Period**", which begins on the date the contract is awarded and ends 1 year later and;

b) **Option to Extend the Contract**:

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 4 additional 1-year period(s) under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least 5 calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

7.10 Delivery Date

Please see Annex A – Statement of Requirement, section 5.

7.11 Authorities

a) **Contracting Authority**

The Contracting Authority for the Contract is:

Name: Tracey Miller
Title: Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Directorate: Software and Shared Systems Procurement Directorate (SSSPD) -STAMS
Address: Place Du Portage, Phase III, 4C1
11 rue Laurier,
Gatineau, Quebec K1A 0S5, Canada
Telephone: (613) 858-2651
E-mail address: tracey.miller@pwgsc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

b) **Technical Authority**

The Technical Authority for the Contract is:

Name:
Title:
Organization:
Address:
Telephone:
Facsimile:
E-mail address:

In this person's absence, the Technical Authority is:

Name:
Title:
Organization:
Address:
Telephone:
Facsimile:
E-mail address:

Note to bidders: *Information will be completed by the Contracting Authority at Contract Award.*

The Technical Authority [is the representative of the department or agency for whom the Work is being carried out under the Contract and] is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

c) **Contractor's Representative**

Note to bidders: *Information will be completed by the Contracting Authority at Contract Award.*

7.12 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a Public Service Superannuation Act (PSSA) pension, the Contractor has agreed that this information will be reported on departmental web sites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.13 Payment

a) **Basis of Payment**

1. Licensed Software Subscription Services: For the Licensed Software Subscription Services (including the Software Documentation, Maintenance and Support), all as detailed in the Contract, Canada will pay the Contractor, in advance the firm all inclusive lot price(s), set out in Annex C, GST/HST extra upon acceptance of Licensed Software Subscription Services by the Technical Authority and in accordance with the Method of Payment stated below in paragraph (c).

2. Optional Additional Licensed Software Subscription: For the option to increase the number of Licensed Software Subscription that will be serviced under the Licensed Software Subscription Services, if Canada exercises its option, Canada will pay the Contractor the firm all inclusive lot price(s) set out in Annex C, GST/HST extra. If the number of Licensed Software Subscription are increased during the Contract Period or during any of the Option Periods, Canada will pay the applicable price for the number of Contacts divided by 365, then multiplied by the number of days remaining in that specific period.

3. Optional Additional Software Licenses: For additional licenses for additional Users to use the Licensed Software, if Canada exercises its option, Canada will pay the Contractor the firm price set out in Annex C, FOB destination, including all customs duties, Applicable Taxes extra.

4. Travel and Living Expenses: Canada will not pay for any travel or living expenses associated with the performing the Work.

5. Competitive Award: The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

6. Purpose of Estimates: All estimated costs contained in the Contract are included solely for the administrative purposes of Canada and do not represent a commitment on the part of Canada to purchase goods or services in these amounts. Any commitment to purchase specific amounts or values of goods or services is described elsewhere in the Contract.

b) **Limitation of Expenditure**

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

c) **Right of Set-Off**.

When making a payment to the Contractor, Canada may deduct any amount payable to Canada by the Contractor under this or any other current contract

d) **Method of Payment – Advanced Payment for Licensed Software Subscription Services**

Canada will make the advance payment to the Contractor for Licensed Software Subscription Services within 30 days after receiving a complete invoice (and any required substantiating documentation), or within 30 days of any date specified in the Contract for making that advance payment, whichever is later.

If Canada disputes an invoice for any reason, Canada will pay the Contractor the undisputed portion of the invoice, as long as the undisputed items are separate line items on the invoice and are owing. In the case of disputed invoices, the invoice will only be considered to have been received for the purposes of the section of the General Conditions entitled "Interest on Overdue Accounts" once the dispute is resolved.

The Contractor acknowledges that this is an advance payment and that, despite anything to the contrary in the Contract, Canada will perform acceptance procedures for the services only after the services have been performed, regardless of whether the payment has already been made. The Contractor agrees that any advance payments authorized and paid under the terms of the Contract are not considered acceptance of the services for which the payment is made. Also, payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or any of the Work, if the Work performed later proves to be unacceptable.

(e) **Method of Payment - Single Payment**

H1000C (2008-05-12), Single Payment

(f) **Method of Payment - Advance Payment**

Canada will pay the Contractor in advance for the maintenance and support services if:

(A) An accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

(B) All such documents have been verified by Canada.

Payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or any of the Work, if the Work performed later proves to be unacceptable.

(g) **Discretionary Audit**

The following are subject to government audit before or after payment is made:

The amount claimed under the Contract, as computed in accordance with the Basis of Payment, including time charged.

The accuracy of the Contractor's time recording system.

The estimated amount of profit in any firm-priced element, firm time rate, firm overhead rate, or firm salary multiplier, for which the Contractor has provided the appropriate certification. The purpose of the audit is to determine whether the actual profit earned on a single contract if only one exists, or the aggregate of actual profit earned by the Contractor on a series of negotiated contracts containing one or more of the prices, time rates or multipliers mentioned above, during a particular period selected, is fair and reasonable based on the estimated amount of profit included in earlier price or rate certification(s).

Any firm-priced element, firm time rate, firm overhead rate, or firm salary multiplier for which the Contractor has provided a price certification. The purpose of such audit is to determine whether the Contractor has charged anyone else, including the Contractor's most favoured customer, lower prices, rates or multipliers, for like quality and quantity of goods or services.

a. Any payments made pending completion of the audit must be regarded as interim payments only and must be adjusted to the extent necessary to reflect the results of the said audit. If there has been any overpayment, the Contractor must repay Canada the amount found to be in excess. At the time of any audit, the parties will negotiate in good faith to determine which documentation supplied by the Contractor is to remain confidential.

b. Audited materials, regardless of format, disclosed to the Client or Canada by the Contractor must be kept confidential if marked confidential and agreed upon pursuant to the paragraph above.

(a) Service Availability Levels and Credits

(i) **Service Availability:** The Hosted Online Survey Solution must be available twenty-four hours a day, seven days a week with the exception of Scheduled Maintenance periods or any events or occurrences due to the products, services, and/or actions of 3rd parties beyond the Contractor's reasonable control.

(ii) Scheduled Maintenance will only be performed after a minimum of 1 working day notice. The Contractor may perform maintenance on some or all of the Hosted Online Survey Solution in order to upgrade hardware or software that operates or supports the Hosted Online Survey Solution, implement security measures, or address any other issues it deems appropriate for the continued operations of the Hosted Online Survey Solution.

(iii) Notwithstanding the Excusable Delays provisions of the General Conditions, the Contractor shall be take all necessary steps to ensure that Canada shall not be denied access to the services for more than four (4) hours in the event there is any event, including an event contemplated by the Excusable Delays provisions of the General Conditions, impacting Contractor infrastructure necessary to provide the services. Contractor shall maintain the capability to resume provisions of the services from an alternative location and via an alternative telecommunications route in the event of an event that renders the Contractor's primary infrastructure unusable or unavailable. If Contractor fails to restore services within

four (4) hours of the initial disruption, Canada may declare Contractor to be in default of this Contract and Canada may seek alternate services, which would have been otherwise provided under this Contract, for third parties. Contractor shall reimburse Canada for all costs reasonably incurred by Canada in obtaining such services, with payment to be made within thirty (30) calendar days of Canada's written request for such payment.

(iv) **Service Credits:** At Canada's request, the Contractor will calculate the Client's Service Availability during a given calendar month. If the Contractor has failed to meet the Service Availability in a given calendar month, Canada will be entitled to a credit in the following:

Service Availability Interruption	**Service Credit**
Less than 0.99% of hours in a calendar month	No Credit
1% to 3.99% of hours in a calendar month	5%
4% to 5.99% of hours in a calendar month	10%
6% to 11.99% of hours in a calendar month	25%
12% of hours or more hours in a calendar month	50%

The credit amount that Canada is entitled to for any Service Availability Interruption in a given calendar month will be calculated as follows: the applicable Service Credit percentage for the Service Availability Interruption times the estimated monthly rate (prorated from the applicable annual rate paid by Canada at the time).

The length of a Service Availability Interruption will be measured from the time an interruption is reported by the Client until the Contractor has taken the necessary steps to restore the Service Availability.

(v) **Corrective Measures:** If credits are payable under this Article for two consecutive months or for three months in any 12-month period, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Client and the Contracting Authority and 20 working days to rectify the underlying problem.

(vi) **Termination for Failure to Meet Availability:** In addition to any other rights it has under the Contract, Canada may terminate the Contract for default in accordance with the General Conditions by giving the Contractor three months' written notice of its intent, if any of the following apply:

a. the total amount of credits for a given quarter (3 month-period) reach a level of 10% of the total billing for that quarter; or

b. the corrective measures required of the Contractor described above are not met.

This termination will be effective when the three-month notice period expires, unless Canada determines that the Contractor has implemented the corrective measures to Canada's satisfaction during those three months.

(vii) **Credits Apply during Entire Contract Period:** The Parties agree that the credits apply throughout the Contract Period, including during implementation.

(viii) **Credits represent Liquidated Damages:** The Parties agree that the credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

(ix) **Canada's Right to Obtain Payment:** The Parties agree that these credits are a liquidated debt. To collect the credits, Canada has the right to hold back, draw back, deduct or set off from and against any money Canada owes to the Contractor from time to time.

(x) **Canada's Rights & Remedies Not Limited:** The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

(xi) **Audit Rights:** The Contractor's calculation of credits under the Contract is subject to verification by government audit, at the Contracting Authority's discretion, before or after payment is made to the Contractor. The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately credited to Canada in the Contractor's invoices. If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year). If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

7.14 Invoicing Instructions

a) The Contractor must submit invoices in accordance with the information required in the General Conditions.

b) The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment provision.

c) By submitting invoices (other than for any items subject to an advance payment), the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.

d) The Contractor must provide the original of each invoice to the Technical Authority, and a copy to the Contracting Authority.

7.15 Certifications

The continuous compliance with the certifications provided by the Contractor in its bid and the ongoing cooperation in providing additional information are conditions of the Contract. Certifications are subject to verification by Canada during the entire period of the Contract. If the Contractor does not comply with any certification, or fails to provide the additional information, or if it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

7.16 Federal Contractors Program for Employment Equity - Default by Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE

becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.17 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

7.18 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the following list, the wording of the document that first appears on the list has priority over the wording of any document that appears later on the list:

(a) these Articles of Agreement, including any individual SACC Manual clauses incorporated by reference in these Articles of Agreement;

(b) supplemental general conditions, in the following order:

(i) 4008 (2008-12-12), *Supplemental General Conditions - Personal Information*, apply to and form part of the Contract.

(c) general conditions 2030 (2018-06-21), Higher Complexity – Goods;

(d) Annex A, Statement of Requirement;

(e) Annex B, Evaluation Criteria;

(f) Annex C, Basis of Payment;

(g) Annex D, Security Requirements Check List;

(h) Annex E, Government of Canada Security Control Profile for Cloud-based GC Services

(i) Annex F, Privacy and Security Requirements

(j) Annex G, Security Screening Requirements

(k) Annex H, Point-rated Criteria for Mandatory Security Technical Criteria

(l) Annex I, Bidder Forms

(m) the Contractor's bid dated _____, as clarified on "or" as amended on _____, not including any software publisher license terms and conditions that may be included in the bid, not including any provisions in the bid with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the bid.

7.19 Foreign Nationals (Canadian Contractor)

SACC Manual clause A2000C (2006-06-16)Foreign Nationals (Canadian Contractor)

7.20 Foreign Nationals (Foreign Contractor)

SACC Manual clause A2001C (2006-06-16) Foreign Nationals (Foreign Contractor)

7.21 Insurance Requirements

SACC Manual clause G1005C (2016-01-28) Insurance Requirements

7.22 Limitation of Liability - Information Management/Information Technology

This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the ontract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this Article, even if it has been made aware of the potential for those damages.

First Party Liability:

The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:

1. any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";

2. physical injury, including death.

The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (i)(A) above.

The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

a) any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

b) any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated by Canada either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of 0.25 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the cell titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1M.

In any case, the total liability of the Contractor under subparagraph (v) will not exceed the total estimated cost (as defined above) for the Contract or $1M, whichever is more.

If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using

the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

Third Party Claims:

Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

If Canada is required, as a result of joint and several liability or joint and solidarily liable, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite Sub-article (i), with respect to special, indirect, and consequential damages of third parties covered by this Section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

The Parties are only liable to one another for damages to third parties to the extent described in this Sub-article (c).

7.23 Joint Venture Contractor

(a) The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members:

(b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:

i. _____ has been appointed as the "representative member" of the joint venture Contractor and has full authority to act as agent for each member regarding all matters relating to the Contract;

ii. by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and

iii. all payments made by Canada to the representative member will act as a release by all the members.

(c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.

(d) All the members are jointly and severally or solidarily liable for the performance of the entire Contract.

(e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

(f) The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

Note to Bidders: *This Article will be deleted if the Bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

7.24 Training

a) **Providing Training:** Training must include instructions and course materials in both English and French to be completed within one month after full COTS has been installed on IRCC networks.

The course material must include Installation Manual, Administrator Manual, User Manual and Training Manual offered online via the Software Solution and Microsoft Word and PDF.

b) Providing Software Training:

i. The Contractor must provide online training on the software products that form part of the Software Solution.

ii. The training must be provided within 1 month following contract award.

iii. The training, including both the instruction and the course materials, must be provided in both French and English.

iv. Before providing any training, at least 10 working days in advance of the first training session, the Contractor must submit the course syllabus and schedule, the training materials, and the names and qualifications of the instructions to the Technical Authority for approval.

c) **Finalization of Draft Training Plan:** Within 5 working days of the Contract being awarded, Canada will provide any comments it has regarding the draft training plan submitted by the Contractor as part of its bid. The Contractor must update the training plan to reflect Canada's comments within 10 working days and resubmit it to Canada for approval.

7.25 Safeguarding Electronic Media

a) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.26 Access to Canada's Property and Facilities

Canada's property, facilities, equipment, documentation, and personnel are not automatically available to the Contractor. If the Contractor would like access to any of these, it is responsible for making a request to the Technical Authority. Unless expressly stated in the Contract, Canada has no obligation to provide any of these to the Contractor. If Canada chooses, in its discretion, to make its property, facilities, equipment, documentation or personnel available to the Contractor to

perform the Work, Canada may require an adjustment to the Basis of Payment and additional security requirements may apply.

7.27 No Suspension of Services

The Contractor must not suspend any part of the Services where (a) Canada is reasonably disputing any amount due to Contractor; or, (b) any unpaid but undisputed amount due to Contractor is less than ninety (90) business days in arrears.

7.28 Transition Services at End of Contract Period

(g) The Contractor acknowledges that it is important to Canada to be able to continue to access Software Maintenance and Support Services for the Licensed Software after the Term of Contract. The Contractor agrees that, in the period leading up to the end of the Contract Period (during last Option Period) or at Canada's written request during the Contract Period, it will make all reasonable efforts to assist Canada in the transition from the Contract to a new contract with another supplier or to Canada and that there will be no charge for the services below other than those charges set out in the Basis of Payment. The Contractor is hereby granting Canada, the following irrevocable options:

(h) Licensed Software Subscription Services Pricing Stability

The Contractor accordingly offers to continue to provide Software Maintenance and Support Services at reasonable annual rates and on all of the other terms and conditions set out in this Contract, subject to execution by the parties of a formal contract(s) therefore. For each of the 2 years that follow the Term of Contract, the Contractor hereby offers annual rates that are the lesser of:

i) the Contractor's then current published rates; and

ii) the previously contracted rates adjusted by the percentage difference in the Consumer Price Index (CPI) as determined by Statistics Canada, for the 12 month period immediately preceding the date on which the price change is to be effective; and

iii) 1% more than the annual rates provided to Canada in the preceding year under this Contract or under any extension entered into pursuant to this Article;

(i) and the Contractor's obligations under this Article shall survive termination or expiry of this Contract.

(j) **Transition to Another Successor Contractor:**

i) As applicable, either at the end of Contract Period (end of the final exercised Option Period) or upon termination, at Canada's written request, the Contractor must transfer, using a secure mechanism approved by Canada, all Hosted Online Survey Solution's data and metadata to Canada in an accessible, machine-readable and usable format acceptable to Canada at no additional cost to Canada within forty calendar days of a request by Canada or such longer period as the parties may agree. The data and metadata will be considered received upon sign-off by the Project Authority. The sign-off will certify that the data and metadata that has been received is accessible, machine-readable and usable by Canada.

ii) The Contractor agrees, after successful transfer of Canada's data, to destroy all data that resides with Contractor and to provide a Certification of completion.

7.29 Termination for Convenience

With respect to Section 30 of General Conditions 2035, if applicable, or Section 32 of 2030, if applicable, subsection 4 is deleted and replaced with the following subsections 4, 5 and 6:

1. The total of the amounts, to which the Contractor is entitled to be paid under this section, together with any amounts paid, due or becoming due to the Contractor must not exceed the Contract Price.

2. Where the Contracting Authority terminates the entire Contract and the Articles of Agreement include a Minimum Work Guarantee, the total amount to be paid to the Contractor under the Contract will not exceed the greater of

   (a) the total amount the Contractor may be paid under this section, together with any amounts paid, becoming due other than payable under the Minimum Revenue Guarantee, or due to the Contractor as of the date of termination, or

   (b) the amount payable under the Minimum Work Guarantee, less any amounts paid, due or otherwise becoming due to the Contractor as of the date of termination.

3. The Contractor will have no claim for damages, compensation, loss of profit, allowance arising out of any termination notice given by Canada under this section except to the extent that this section expressly provides. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated at the date of the termination.

ANNEX A

STATEMENT OF REQUIREMENT

1. Objective:

The Contractor must deliver a commercial-off-the-shelf Hosted Online Survey Solution (herein known as "the Software Solution") on behalf of the Government of Canada (GC), which includes online survey software, data analysis and reporting software and on an as-and-when-requested basis, to implement and provide technical support. The Software Solution must allow Canada to conduct online surveys, consultations and public opinion research with both internal and external stakeholders (GC employees, contractors, and the public, including both Canadians and non-Canadians). The Software Solution must enable Clients to gather information that can be used to inform and evaluate GC policies, programs and services.

2. Background:

Immigration, Refugees and Citizenship Canada (IRCC) develops and implements policies, programs and services related to Canada's immigration, refugees, citizenship, integration and passport program. IRCC's Communications Branch is responsible for conducting public opinion research, consultations and citizen engagement, and program evaluations. These activities enable IRCC to comply with support the Policy on Communications and Federal Identity and the Policy on Results. These activities are often facilitated via online survey, data analysis, and reporting software, to ensure the timely and cost-effective collection of information and enable the subsequent analysis of results. Since 2010, the Client has used online software to conduct surveys among employees, clients, other government departments, service providers and the general public.

3. Scope of Work:

IRCC anticipates that it may initially acquire user licenses for 100 users, including maintenance and support services for 1 year, with the options to add additional users, renew maintenance and support services, and order training and professional services on an as-and-when requested basis. The Software Solution must include the following functionality:

- Enable Clients to design and implement surveys;
- Secure password authentication;
- Standardized question and questionnaire features;
- Enable the electronic collection of data;
- Enable the analysis of data;
- Enable reporting of data findings;
- Enable data input and export.

The Software Solution must:

- Be a managed service that consists of:
    - The required hardware platforms and storage to support the Software Solution.
    - Any required network, security & platform software/services (e.g. Operating Systems, Databases, Directories, Firewalls) to support the Software Solution and the required application software to support the Software Solution.
    - The required services to implement and configure the Software Solution, inclusive of importing existing data in the Software Solution.
    - The required services to maintain the Software Solution inclusive of software releases, upgrades and bug fixes, as they become available.

- Technical support for the Software Solution.

- Be hosted on and store all data on the Contractor's secure servers in Canada;
- Be compliant with Web Content Accessibility Guidelines (WCAG 2.0) level AA and have a secure connection via HTTPS protocol using SSL encryption;
- Be scalable and handle a minimum of 100 concurrent users as well as handle a minimum of 2 million completed survey responses per year;
- Allow Users to design surveys using a drag and drop interface with basic and advanced questionnaire structures, allowing for rapid survey creation;
- Allow Users to customize survey templates and URLs to comply with GC policies and guidelines;
- Create an administration control panel where the Client can manage all user information within their department (including secure password authentication and assigning access permissions);
- Generate individual and aggregate response data and allow Users to export reports;
- Capture the general location of the IP address and the specific location must be masked, as per following guidelines http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26761 (Date: 2013-01-31)
- Allow Users to work in the official language of their choice (English and French);
- Allow surveys to be configured so that respondents can take the survey in the official language of their choice (English and French)

l)

4. Deliverables:

The Contractor must provide the following:

Deliverable	Associated Schedule	Format
Software and Licenses	The Software Solution must meet all mandatory requirements by the bid closing date. The Contractor must provide all required licenses to access the Software Solution within 5 business days of the contract award date.	Everything required for the Software Solution to work.
Start-up Meeting	Within 5 business days of the contract award date.	In-person or by teleconference/web conference.
Project Management Documentation: Project Management Plan Project Schedule Implementation Strategy and Plan Departmental template within online survey platform Migration Strategy and Plan	Within 15 business days of the contract award date.	Microsoft Word or PDF.
User Guides: Installation Manual Administrator Manual	Within 20 business days of the contract award date.	Online via the Software Solution and Microsoft Word and PDF.

User Manual Training Manual		
Training	Within 20 business days of the contract award date.	Teleconference/web conference.
Status Meeting	Within 60 business days of the contract award date.	In-person of by teleconference/web conference.

5. Travel:

There is no travel associated with this requirement. Travel expenses, if any, are the sole responsibility of the Contractor.

ANNEX B
EVALUATION CRITERIA

1. Mandatory Requirements

Bidders are to provide product documentation that confirms their response. Any references by the Bidder to websites must be documented with printed copies of the referenced pages and contained within the proposal or the response may be considered non-compliant and, therefore, give no further consideration.

	Mandatory Requirement	Bid reference page and paragraph	Contractor explanation of how the criterion is met
M1	The Software Solution must be a managed service which has the required hardware platforms and storage to support the Software Solution and does not require software installation beyond previously listed browsers.		
M2	The Software Solution must be a managed service with any required network, security & platform software/services (e.g. Operating Systems, Databases, Directories, Firewalls) to support the Software Solution and the required application software to support the Software Solution. No software should need to be installed to use the service and at a minimum the Software Solution must have the updated versions of the following: 1.1 Internet Explorer version 11 and up. 1.2 Firefox version 64 and up. 1.3 Chrome version 71 and up. 1.4 Safari version 10 and up.		
M3	The Software Solution must be a managed service that can import existing data in the Software Solution.		
M4	The Software Solution must be a managed service with the required services to maintain the Software Solution inclusive of software releases, upgrades and bug fixes, as they become available. This includes technical support for the Software Solution.		
M5	The Software Solution and all of Canada's data must be hosted on the Contractor's dedicated secure servers within Canada.		
M6	The Software Solution must be compliant with Web Content Accessibility Guidelines (WCAG) 2.0, level AA.		
M7	The Software Solution must have the functionality to permit the administrators to upload templates.		

M8	The Software Solution must permit secure data exchanges between the application and a client workstation, and a secure connection via HTTPS protocol using SSL encryption.		
M9	The Vendor cannot remove data from the Software solution without notifying the Client via e-mail.		
M10	The Software Solution must be the most up-to-date version of the software to protect data stored against access to third parties (e.g. latest versions, updates, patches).		
M11	Capture the general location of the IP address and the specific location must be masked, as per following guidelines http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26761 (Date: 2013-01-31)		
M12	The Software Solution must handle a minimum of 100 password-protected user accounts concurrently without any degradation in performance or user experience.		
M13	The Software Solution must be capable of handling a minimum 2 million survey completes per year.		
M14	The Software Solution must allow access via username and password.		
M15	The Software Solution must permit the Client to create and manage all user permissions that the Client deems required for the creation and management of user accounts.		
M16	The Software Solution must allow the Client to: 1.1 create new accounts, delete accounts, modify status in groups and modify permissions. 1.2 have full access to surveys created by other users. 1.3 view and print individual responses.		
M17	The Software Solution must provide the ability to control various types of user access permissions including: 1.1 view or not to view survey. 1.2 right to delete or not delete surveys (including all associated responses, data, versions, history of edits). 1.3 right to modify or not modify. 1.4 right to translate or not to translate.		

	1.5 right to distribute or not distribute. 1.6 right to export results or not export results. 1.7 right to generate reports or not to generate reports. 1.8 right to perform system administrator tasks.		
M18	The Software Solution must not limit the number of surveys, survey questions, features or custom filters.		
M19	The Software Solution must allow users to send an unlimited number of individual or bulk e-mails, email invitations and reminders through secure email invite links, including the following: 1.1 send out test and reminder emails. 1.2 view status of invites and email sent (in real time). 1.3 customize "From/Reply-To" email address and "From" name. 1.4 merge address book fields to email invite. 1.5 create QR codes. 1.6 generate, track responses and export customizable invitation codes. 1.7 export API.		
M20	The Software Solution must not limit the number of invitations.		
M21	The Software Solution must permit the customization of a template.		
M22	The Software Solution must have the capacity to host separate surveys simultaneously in different templates.		
M23	The Software Solution must allow users to send an unlimited number of individual or bulk e-mails.		
M24	The Software Solution must permit e-mails to send out initial invitations to potential respondents.		
M25	The Software Solution must have an automatic "opt-out" option feature to all future invitations and prevent future invitations from being sent out to those who have opted out.		
M26	The Software Solution must have the ability to toggle surveys between active and inactive.		

M27	The Software Solution must provide unique or customized URLs for surveys in English and French, which would remain functional should the survey be transferred from one user to another.		
M28	The Software Solution must permit images, videos and logos to be imbedded into the questionnaire.		
M29	The Software Solution must allow respondents to download their completed survey.		
M30	The Software Solution must track the number of partially complete and completed surveys.		
M31	The Software Solution must generate a response rate.		
M32	The Software Solution must provide the fieldwork dates and times for responses as well as an average number of responses each day.		
M33	The Software Solution must archive, or be configured to archive data in a separate file.		
M34	The Software Solution must allow respondents to complete surveys on a mobile device and smartphone.		
M35	The Software Solution must include a basic questionnaire structure that includes the following sections at a minimum: 1.1 section headings/text sections. 1.2 text response fields (e.g. must validate/mandate formatting such as integers, maximum word count, phone numbers). 1.3 multiple choice. 1.4 insert images, graphics and videos. 1.5 dropdown and checkbox questions. 1.6 Yes/No and Other: Specify boxes. 1.7 making responses to questions optional/required; 1.8 open text response options (e.g. short text/single line and multiple line) with functionality for the Client to set a maximum work limit; 1.9 progress bar showing percentage of questionnaire completed.		
M36	The Software Solution must include an advanced questionnaire		

	structure that includes the following sections at a minimum: 1.1 date/time. 1.2 drill-downs. 1.3 score display. 1.4 timer. 1.5 ranking (e.g. dragging and dropping selections into categories/order). 1.6 slider (e.g. rate something 1-10 by sliding a dial on a scale). 1.7 multi-type question (e.g. multiple choice, dropdown, side-by-side, and text response).		
M37	The Software Solution must permit built-in grid questions (e.g. text response grid, multiple choice grid, dropdown grid, and checkbox grid).		
M38	The Software Solution must permit certain questions to be mandatory and/or have opt-out features and the ability to edit and personalize configuration (e.g. customizable end pages, error messages and button texts).		
M39	The Software Solution must allow for the development of survey logic including the following: 1.1 item/question skip. 1.2 branching (e.g. ability to customize the survey according to the responses to specific questions). 1.3 piping (e.g. ability to carry a respondent's answer from one question to the next depending on the options selected). 1.4 looping (e.g. ability for questions to be repeated multiple times for a respondent). 1.5 rotation and randomization, which may be based on response variables, language, invitation codes, IP address or other administrative data.		
M40	The Software Solution must include dynamic logic (e.g. ability to hide questions or page).		
M41	The Software Solution must permit the preview and pre-test of surveys.		
M42	The Software Solution must permit on-line and off-line usage with the ability to distinguish responses between the 2 modes.		

M43	The Software Solution must maintain and store a history of edits, up to 5 years, with the ability to track versions of the survey as well as revert to a previous version if needed.		
M44	The Software Solution must permit responses to be edited and saved if a respondent exits and then re-enters the survey.		
M45	The Software Solution must provide a web-based user interface.		
M46	The Solution must permit the use of the complete English and French language character sets.		
M47	The Software Solution must allow, or can be configured to allow users to work in the official language of their choice: English and French (including the ability to view all screens, collect responses and access technical support in English of French). Respondents must be able to start and toggle in between languages while completing the survey without the loss of any response data.		
M48	The Software Solution must provide, or can be configured to provide, technical support in English or French.		
M49	The Software Solution must allow, or can be configured to allow users to work in multiple additional languages (e.g. characters from right to left such as Spanish, left to right such as Arabic and Chinese characters). The Contractor must make languages available within 30 days of request.		
M50	The Software Solution must generate custom and filter results based on the criteria specified by the users.		
M51	The Software Solution must allow users to design and program the appearance of surveys in HTML/CSS.		
M52	The Software Solution must generate cross-tabulations, summary statistics and frequency tables, as well as mean, mode and variance for each question.		
M53	The Software Solution must permit the users to download individual and aggregate response data.		
M54	The Software Solution must allow, or can be configured to allow users to export reports in Excel (.xlsx and .csv) and Word.		
M55	The Software Solution must be able to save and print standardized and ad hoc reports.		
M56	The Software Solution must permit dashboard analysis tool.		

M57	The Contractor must provide the following documentation in the form of User Guides: 1.1 Administrator Manual. 1.2 Installation Manual. 1.3 User Manual. 1.4 Training Manual. 1.5 Migration Strategy and Plan.		
M58	The Contractor must provide the documentation in electronic form (PDF and online)		
M59	The Contractor must provide 20 hours of training (which will be provided on-site or remotely via internet meeting).		
M60	The Contractor must be able to provide all training in English and French.		
M61	The Contractor must have a dedicated account representative at the Vice-President or equivalent level.		
M62	The Contractor's technical support/help desk must have a guaranteed response time within 2 hours of requesting help during regular working hours.		
M63	The Contractor must have a back-up system in the event of a power outage.		
M64	The Contractor must provide a 48 hour notice of a planned outage and within 1 hour after any unplanned outages.		
M65	The contractor must be able to disable or provide functionality that allows Canada to disable, the serving or display of any third party commercial advertisement or solicitation on any pages or screens of the services, displaying content created by or under the control of Canada.		

I. Point-Rated Requirements

	Rated requirement	Rated Point Value	Points obtained	Bidder Responses/Document Reference
R1	The Software Solution should have the ability to alert the Client when a survey is generated by a user.	Yes – 4 points No – 0 points		
R2	The Software Solution should have the ability to track the last site visited by the user.	Yes – 4 points No – 0 points		
R3	The Software Solution should have the capacity to create custom URLs for surveys. (2 points) Have the URLs remain functional should a survey be transferred from one user to another. (2 points) The custom URLs should be functional in both English and French of the survey. (6 points)	Custom URLS Yes – 2 points No – 0 points URLS remain functional Yes – 2 points No – 0 points Bilingual URLS Yes – 6 points No – 0 points		
R4	The Software Solution should allow respondents to download the survey and their survey responses in a printable format (e.g. Word, PDF).	Yes – 4 points No – 0 points		
R5	The Software Solution should have the capacity to provide documents to respondents (provided via survey).	Yes – 4 points No – 0 points		
R6	The Software Solution should have the capacity to allow respondents to upload documents via survey.	Yes – 4 points No – 0 points		
R7	The Software Solution should have the capacity to support image file types (.jpg, .gif, .png).	Yes – 4 points		

		No – 0 points		
R8	The Software Solution should have the capacity to support video file types (.mpg, .avi, .mov, .qt, .asf, .wmv, .mp4).	Yes – 4 points No – 0 points		
R9	The Software Solution should have the capacity to support Office file types (.doc, .docs, .ppt, .pptx, .xls, .xslx).	Yes – 4 points No – 0 points		
R10	The Software Solution should have the capacity to support spreadsheet file type.	Yes – 4 points No – 0 points		
R11	The Software Solution should have the capacity to allow users to collect responses online and offline. For offline responses, the Software Solution should allow for responses to be uploaded into the survey to be analyzed with data gathered online. The user should be able distinguish between online/offline responses if needed.	Yes – 4 points No – 0 points		
R12	The Software Solution should have the ability to save options/scales for later use (without cookies). The questions and variables should be stored in the system and easily selected for re-use at a later date, in multiple surveys and in multiple languages.	Yes – 4 points No – 0 points		
R13	The Software Solution should have the capacity to generate multiple collectors from the same survey (e.g. the user should be able to develop multiple unique links for the same survey in order to distinguish data by whichever variable the collector represents, data segmentation). The Software Solution should be able to do the following: users should be able to label each collector so as to easily identify the variable being represented (2 points) each collector created should include different links for the English and French versions of each survey, where applicable (2 points) users should be able to create an unlimited number of collectors (2 points) o) p) users should be able to use the collector as a variable when developing survey logic (2 points)	Label Collectors Yes - 2 points No – 0 points Each collector – EN/FR Links		

	q) r) Users should have the ability to merge collectors for analysis. (2 points)	Yes – 2 points No – 0 points Unlimited number of collectors Yes – 2 points No – 0 points Ability to use collectors as a variable Yes – 2 points No – 0 points Ability to merge collectors Yes – 2 points No – 0 points		
R14	The Software Solution should have the ability to perform formatting on a report before exporting it.	Yes – 4 points No – 0 points		
R15	The Software Solution should have the capacity to identify a group of respondents within the same survey.	Yes – 4 points No – 0 points		
R16	The Software Solution should allow users to export reports in Microsoft Word, SAS, SPSS, PowerPoint and PDF.	Export to Microsoft Word Yes – 2 points No – 0 points Export to SAS Yes – 2 points No – 0 points		

		Export to SPSS Yes – 2 points No – 0 points Export to PowerPoint Yes – 2 points No – 0 points Export to PDF Yes – 2 points No – 0 points		
R17	The Software Solution should have the capacity for a reporting link (URL) that allows for results to be shared.	Yes – 4 points No – 0 points		
R18	The Contractor must obtain approval from the Client before modifying the period for which back-ups are kept.	Yes – 4 points No – 0 points		

II. Constraints

Department	Policy	Policy Requirement	Constraint	Additional
Treasury Board of Canada	*Standard on Web Accessibility*	TBS Policy on Web Accessibility requires that Government of Canada applications accessed through a web browser be compliant the WCAG 2.0 standard, and within that standard, CIC requires that the website conform to the CIC external website template	Build and install a customized WCAG 2.0 compliant survey template that replicates the design of the Departmental website, and white labeling	Should the TBS Policy on Web Accessibility be updated to reflect new standards, the contractor will agree to make necessary updates to the website free of charge and in a timely fashion. Surveys must be accessible to those with visual impairments (i.e. must be accessible through screen-readers or related technologies).
Treasury Board of Canada	*Privacy Act*, R.S. 1985, c. P-21	Protection against illegal or unsanctioned access to personal information.	A valid security clearance in the form of a certification that is granted by the Canadian Industrial Security Directorate (CISD) of Public Works and Government Services Canada.[1]	Secure connection via HTTPS protocol using TLS Version 1.2 encryption A managed hosting service on an external secure server. Software is located on a server that allows secure connections via an HTTPS protocol using SSL encryption. CISD Clearance The contractor must hold CISD clearance.
Treasury Board of Canada	*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5	Protection against illegal or unsanctioned access to personal information.	A valid security clearance in the form of a certification that is granted by the Canadian Industrial Security Directorate (CISD) of Public Works and	Secure connection via HTTPS protocol using TLS version 1.2 encryption A managed hosting service on an external secure server. Software is located on a server that allows secure connections via an HTTPS protocol using TLS version 1.2

[1] The supplier must have previously held a valid CISD. As each CISD is specific to each contract, the winning bidder will be notified that it must obtain a new CISD which will pertain to the new contract with CIC. Until the new CISD clearance is obtain, the contract will not be fully awarded to the winning bidder.

			Government Services Canada.[2]	encryption. CSID Clearance The contractor must hold CISD clearance.
Treasury Board of Canada	*Privacy Act*, R.S. 1985, c. P-21	Protection against legally-sanctioned access. (e.g., in the United States under provisions of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act,* known as USA PATRIOT Act: see the Treasury Board Secretariat's overview)	The supplier must ensure that all the databases containing any information related to the survey are stored on servers and back-up servers located solely in Canada	All databases must be located in Canada. The supplier must ensure that all data relating to the survey is processed only in Canada or in another country approved by the client under paragraph 2) a). The supplier must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada.
Treasury Board of Canada	*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5	Protection against legally-sanctioned access. (e.g., in the United States under provisions of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act,* known as USA PATRIOT Act: see the Treasury Board Secretariat's overview)	The supplier must ensure that all the databases containing any information related to the survey are stored on servers and back-up servers located solely in Canada	All databases must be located in Canada. The supplier must ensure that all data relating to the survey is processed only in Canada or in another country approved by the client under paragraph 2) a). The supplier must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada.

[2] IBID.

Treasury Board of Canada	Communications Policy of the Government of Canada	Communicate in English and in French	The online software must be able to provide surveys that can be accessed in both GoC official languages (English and French).	Ubiquitous aspects of surveys (e.g. "next" and "back" buttons, "submit" buttons, thank you messages, etc.) must be provided in English and French.
Treasury Board of Canada	Protected information refers to specific provisions of the *Access to Information Act* and the *Privacy Act* and applies to sensitive personal, private, and business information.	Protection against *grave* injury, such as loss of reputation or competitive advantage.	The online software must safeguard personal information at the level of Protected B	**7.5** Protected information Protected B: Compromise could result in *grave* injury, such as loss of reputation or competitive advantage. CSE document ITSP.40.111 provides guidance for protecting data at rest: https://www.cse-cst.gc.ca/en/node/1831/html/26515 (Date: 08/02/2016) CSE document ITSP.40.062 provides guidance for protecting data in transit: https://www.cse-cst.gc.ca/en/node/1830/html/26507 (Date: 08/02/2016) CSE document ITSP.40.006 provides guidance for data sanitization and disposal: https://www.cse-cst.gc.ca/en/node/2206/html/27963 (Date: 01/07/2017)

ANNEX C

BASIS OF PAYMENT

TABLE 1 – INITIAL REQUIREMENT		
Item No. **(A)**	**Initial Deliverables Description** **(B)**	**Lot Price** **(C)**
1	For the provision of a commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, training, and warranty, for 100 user licenses as detailed in Annex A - Statement of Requirement.	$0.00
	Total for Table 1 (sum of Column C):	$0.00

TABLE 2 **HOSTED ONLINE SURVEY SOLUTION**		
Item No. **(A)**	**Description** For access to the Hosted Online Survey Solution, as described in Annex C, Table 1 – Initial Requirement. Including online survey software, warranty, customer support services, for 100 user licenses as detailed in Annex A - Statement of Requirement**.** **(B)**	**Lot Price** **(C)**
1	Contract Year 1: Hosted Online Survey Solution as per Description	$0.00
	Total for Table 2 (sum of Column C):	$0.00

TABLE 3 **OPTION YEARS FOR HOSTED ONLINE SOLUTION**		
Item No. **(A)**	**DESCRIPTION** For access to the Hosted Online Survey Solution, as described in Annex C, Table 1 – Initial Requirement. Including online survey software, warranty, customer support services, for 100 user licenses as detailed in Annex A - Statement of Requirement **(B)**	**Lot Price** **(C)**
1	Option Year 1: Hosted Online Survey Solution as per Description - Date to be determined.	$0.00
2	Option Year 2: Hosted Online Survey Solution as per Description - Date to be determined.	$0.00
3	Option Year 3: Hosted Online Survey Solution as per Description - Date to be determined.	$0.00
4	Option Year 4: Hosted Online Survey Solution as per Description - Date to be determined.	$0.00
	Total for Table 3 (sum of Column C):	$0.00

TABLE 4

OPTIONAL GRANT OF USE FOR ADDITIONAL USERS TO ACCESS AND USE THE HOSTED ONLINE SOLUTION

ITEM NO.	DESCRIPTION Optional Licenses for Additional Users to the Hosted Online Solution, including Maintenance and Support Services.	Cost Per Additional User (A)	Estimated Number of users for Evaluation Purposes Only (B)	Extended Price for Evaluation Purposes (C) = (A x B)
1	Initial Contract Period	$0.00	100	**$**0.00
2	Option Year 1	$0.00	100	**$**0.00
3	Option Year 2	$0.00	100	$0.00
4	Option Year 3	$0.00	100	$0.00
5	Option Year 4	$0.00	100	$0.00
			Total for 4 (sum of Column C):	$0.00

TABLE A - TOTAL BID PRICE (TBP) FOR EVALUATION PURPOSES			
ITEM NO.	**DESCRIPTION**	**FORMULA**	**TOTAL PRICE**
1	For the provision of a commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, professional services, maintenance and support services for 100 user licenses as detailed in Table 1 of Annex C.	Total from Table 1 of Annex C	**$**
2	During the initial contract period, for the provision of commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, professional services, maintenance and support services for 100 user licenses as detailed in Table 2 of Annex C.	Total from Table 2 of Annex C	**$**
3	During the optional periods of the Contract, for the provision of commercial off-the-shelf Hosted Online Survey Solution, including online survey software, data analysis, reporting software, professional services, maintenance and support services for 100 user licenses as detailed in Table 3 of Annex C.	Total from Table 3 of Annex C	**$**
4	For the optional additional users as detailed in Table 4 of Annex C.	Total from Table 4 of Annex C	**$**
		Total Bid Price (TBP) - (sum of Column A):	**$**

ANNEX D

SECURITY REQUIREMENTS CHECK LIST

SEE ATTACHED

ANNEX E

Government of Canada Security Control Profile for Cloud-based GC Services

SEE ATTACHED

ANNEX F

Security Screening Requirements

The Foreign recipient **Contractor / Subcontractor** must perform a security screening of all its personnel who will need access to **Canadian restricted sites and/or CANADA PROTECTED A or B** information/assets:

a) Identity Check:

i. Copies of two of valid original pieces of government issued identity documentation, one of which must include a photo
ii. Surname (last name)
iii. Full given names (first name) – underline or circle usual name used
iv. Family name at birth
v. All other names used (aliases)
vi. Name changes
    1. Must include the name they changed from and the name they changed to, the place of change and the institution changed through
vii. Sex
viii. Date of birth
ix. Place of birth (city, province/state/region, and country)
x. Citizenship(s)

b) Residency Check:

i. The last five (5) years of residency history starting from most recent with no gaps in time.
    1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates.

c) Educational Check:

i. The educational establishments attended and the corresponding dates.

d) Employment History Check:

i. The last five (5) years of employment history starting from most recent with no gaps in time.

e) Criminal Records Check:

i. Proof of criminal record check report, using fingerprint verification with favorable results for each country the person has resided during the last five (5) years.

f) Credit Check:

s) i. Credit check report conducted as part of employment screenings.

Annex G

Mandatory Security Technical Criteria

Each bid will be reviewed for compliance with the following mandatory technical criteria. Bids that do not comply with each and every mandatory technical criteria will be declared non-responsive and not considered further.

No.	Evaluation Area	Bid Submission Requirements	Evaluation Criteria
M2	Data Residency and Personnel	The Bidder must clearly demonstrate its data residency compliance and provide a data center deployment plan(s) which should include specifics on: i. location(s) (country and city) of primary data center(s); ii. location(s) (country and city) of secondary data center(s) and backup centers; iii. location(s) (country and city) of all the infrastructure components (including, but not limited to, database servers, SANS, application servers); and iv. location(s) (country and city) of the SOC, NOC and the Service Desk. The Bidder must clearly demonstrate its business entities and personnel location compliance and provide:	The Bidder must demonstrate that the datacenters, software, middleware, the Service Desk, SOC and NOC infrastructure and Data for the entire reside within Canada and/or countries with which Canada has international bilateral industrial security instruments (IBISI). The Bidder must demonstrate that the personnel for the entire , including SOC, NOC and Service Desk be physically located and operate within Canada, countries with which Canada has IBISI, or within countries belonging to EU or NATO. The Bidder must demonstrate that all business entities be physically located, be legally authorized to operate and to do business and be registered, where the local legislation requires such registration, within Canada, countries with which Canada has IBISI, European Union and/or NATO countries.

		i. location(s) (country and city) of all business entities performing Work under the Contract; and ii. location(s) of all personnel performing the Work under the Contract.	
M2		The bidder must implement safeguards to ensure that all publicly accessible government websites and web services are configured to provide service only through a secure connection, in accordance with Section 6.2.4 of the Policy on the Management of Information Technology and the Policy on Government Security. Bidder must implement a secure web connection that: • is configured for HTTPS • has HSTS enabled • implements TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, as outlined in CSE's o ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites o ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B	

		Information • disables known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062 • disables known-weak ciphers (e.g. RC4 and 3DES)	

Annex H

Point-Rated Criteria for Security Mandatory Technical Criteria

Bids which meet all the mandatory technical criteria will be evaluated and scored as specified in the table and scales below and the scoring grid in section 1 – "Evaluation Summary". Each point-rated criterion should be addressed separately.

Scale 2 – Generic Scale	
0	**Not Addressed -** Bidder's information submitted was not relevant to the criterion or failed to submit response.
1	**Minimally Addressed** – The bid demonstrates little understanding of the solicitation requirements and the proposed approach does not address important factors. Proposed approach has significant weaknesses and is not likely to meet solicitation requirements and does not demonstrate technical value to Canada. Bid poses a perceived large residual risk* to Canada.
2	**Partially Addressed** – The bid demonstrates some understanding of the solicitation requirements and the proposed approach addresses some important factors. Proposed approach has weaknesses and is not likely to meet solicitation requirements or be effective and does not demonstrate good technical value to Canada. Bid poses a perceived medium residual risk* to Canada.
3	**Satisfactorily Addressed** – The bid demonstrates adequate understanding of the solicitation requirements and the proposed approach addresses most factors. Proposed approach has minor weaknesses and is likely to meet solicitation requirements and provides good technical value to Canada. Bid poses a perceived medium-low residual risk* to Canada.
4	**Very Well Addressed** – The bid demonstrates a very good understanding of the solicitation requirements and the proposed approach addresses all important factors. Proposed approach has no significant weaknesses, is likely to meet solicitation requirements, and is likely to be effective, yield very good results and provides very good technical value to Canada. Bid poses a perceived low residual risk* to Canada.
5	**Excellently Addressed** – The bid demonstrates an excellent understanding of the solicitation requirements and the proposed approach addresses all important factors. Proposed approach has no apparent weaknesses, is likely to meet solicitation requirements, and is likely to be effective, yield excellent results and provides excellent technical value to Canada. Bid poses very little or no apparent residual risk* to Canada.

*Residual risk is defined as the risk that remains after the Bidder's risk mitigations are considered.

For each Criterion, Bidders will be scored on a 0-5 rating guide using one of the applicable scale. Scores will be distributed as follows:

0 – receives 0% of the points assigned to a criterion

1 – receives 20% of the points assigned to a criterion

2 – receives 40% of the points assigned to a criterion

3 – receives 60% of the points assigned to a criterion

4 – receives 80% of the points assigned to a criterion

5 – receives 100% of the points assigned to a criterion

For example, if a bid obtains a 3 in the evaluation of R-2.1, then the Bidder's score for that criterion would be calculated as follows:

Score of 3 = 60%

Weight of criteria R.2.1 – Implementation Plan = 730 points

Therefore, 60% x 730 points = 438 points

No.	Evaluation Area	Bid Submission Requirements	Evaluation Criteria
R5			
R5.1	IT Security Policies and Procedures (Controls)	The Bidder must demonstrate its ability to comply with the IT security requirements by maintaining policies and procedures that support IT security throughout the Contract by providing evidence of any existing policies and procedures that support the security control families described in Annex E – Government of Canada Security Control Profile for Cloud-based GC Services. The Bidder must describe how its policies and procedures align to the security control families by providing the following information on current policies and procedures: (a) name of policy and/or procedure (b) its purpose (c) its scope (d) the roles and responsibilities that are described within the policy and/or procedure (e) how it ensures coordination among organizational entities (f) how it ensures compliance within the organization Note: The Bidder must provide sufficient detail with regard to its policies and procedures in order for Canada to evaluate this response in full	Canada will evaluate the degree to which the Bidder's response demonstrates thoroughness and effectiveness in achieving the level of security represented by the security control families described in Annex E – Government of Canada Security Control Profile for Cloud-based GC Services. Canada will evaluate the degree to which the Bidder's response demonstrates effective policy and procedural support for IT Security including technical, operational and maintenance security areas, including the Bidder's anticipated subcontractors where appropriate.

R5.2	IT Security Topology Diagram	The Bidder must provide an IT security topology diagram which should include the following components: i. interfaces - separate bullet for each category ii. web iii. applications iv. databases v. security devices vi. system management vii. backup infrastructure The Bidder must provide one or more of the following, which define information systems components and functions to be separated by boundary protection devices: i. Information system design documentation; ii. Information system architecture.	Canada will evaluate the degree to which the Bidder's IT security topology diagram demonstrates that the overall design provides a secure environment.
R5.3	Security Organization	The Bidder must describe the experience of the security organization that will be responsible in ensuring the security of the proposed solution, including the name of each person, their role & description of their duties, their experience, and certifications.	Canada will evaluate the degree to which the Bidder demonstrates that the security organization: (a) experience of the personnel supporting ; (b) roles and the description of the duties of the personnel; (c) relevancy of the current and valid certifications of the personnel in that role; and (d) the plan on how the personnel stay current with security trends.

R5.4	Data Segregation	The Bidder must provide its proposed approach to data segregation, that should include: i. information system design documentation; ii. information system architecture; and iii. process and procedures to support data segregation .	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to data segregation: (a) provides logical or physical data segregation management (b) provides a breadth of data segregation for Canada's data throughout all aspects of the system's functionalities and system administration.
R5.5	Disposal and Sanitization	The Bidder must provide its proposed approach to the disposal and sanitization of Canada's data, including: i. a plan for hard-drive sanitation or an action plan if the system is hosted in a virtual environment that will ensure Canada's data is not obtainable; ii. a plan for data disposal; iii. system disposal processes and procedures; iv. a plan for destruction of duplicate records that may be stored in a records management system or backups; and v. the process it plans to follow when the system is no longer required and is being decommissioned.	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to the disposal and sanitization of Canada's data meets, or effectively mitigates the risk where it does not meet, the requirements for disposal and sanitization of data and IT assets as outlined in Annex E – Government of Canada Security Control Profile for Cloud-based GC Services. Canada will evaluate the degree of the strengths, weaknesses and risks of the proposed approach.

R5.6	Continuous Monitoring Service	The Bidder must provide its proposed approach to continuous monitoring of and include the following components: i. The strategy for continuous monitoring ii. Established measures, metrics, and status monitoring and control assessments frequencies; iii. Details of data collection and its reporting aspects; iv. Analysis methods of the data gathered and Report findings accompanied by recommendations; v. Response mechanisms to assessment findings to include making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority; and vi. Review and update cycles to support continuous improvement and maturing measurement capabilities.	Canada will evaluate the degree to which the Bidder demonstrates that its proposed approach to continuous monitoring of provides: (a) High operational visibility; (b) strong, effective, and efficient change control management; (c) adherence to incident response duties as outlined in Annex E – Government of Canada Security Control Profile for Cloud-based GC Services of the solicitation; and (d) adherence to monitoring requirements outlined in Annex E – Government of Canada Security Control Profile for Cloud-based GC Services of the solicitation.

R5.7	Industry IT Security Certification	The Bidder must provide proof of its security certification(s) and applicable audit standards for its proposed solution in the form of a copy of a valid certificate or audit standard and describe how the certification or audit standard was assessed and obtained (e.g.: 3rd party, self-assessment) for each IT Security certification and audit standard held, such as: i. FedRAMP; ii. Cloud Security Alliance – STAR; iii. COBIT; iv. ISO 27001; v. PCI DSS; vi. CMM; and vii. others. The Bidder must also stipulate if the certification or audit standard applies to the whole solution or to a specified portion of their solution.	Canada will evaluate the degree to which the Bidder demonstrates: (a) the relevancy of the role of the member of the Bidder's team (e.g. Joint-Venture member, subcontractor) who holds the certification; (b) rigor in how the certifications were obtained; and (c) the relevancy of the Bidder's certifications to this solicitation.
R5.8	Identity, Credential and Access Management	The Bidder must provide details on its proposed solution's Identity, Credential and Access Management level of assurance capabilities with respect to TBS Standard on Identity and Credential Assurance. The Bidder should identify the level of assurance and demonstrate how it meets the requirements of that level.	Canada will evaluate the degree to which the Bidder demonstrates its solution aligns with the identity and credential assurance requirements defined in the TBS Standard on Identity and Credential Assurance found at http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776. and http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776 .

ANNEX I

BIDDER FORMS

(Form 1) **BID SUBMISSION FORM**		
Bidder's full legal name ***[Note to Bidders:** Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder**.]***		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name:	
	Title:	
	Address:	
	Telephone #:	
	Fax #:	
	Email:	
Bidder's Procurement Business Number (PBN) *[see the Standard Instructions 2003]* [***Note to Bidders:** Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]*		
Jurisdiction of Contract: Province or Territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Former Public Servants See the Article in Part 2 of the bid solicitation entitled "Former Public Servant" for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "	

(Form 1)

BID SUBMISSION FORM

	Is the Bidder a FPS who received a lump sum payment under the terms of the terms of the Work Force Adjustment Directive? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "	
Canadian Content Certification As described in the solicitation, bids with at least 80% Canadian content are being given a preference. *[For the definition of Canadian goods and services, consult the PWGSC SACC clause A3050T]*	On behalf of the Bidder, by signing below, I confirm that *[check the box that applies]:*	
	At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)	
	Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)	
Hardware: *(Contracting Authority should only insert when Supplemental General Conditions 4001 have been inserted in Part 7).*	Toll-Free Telephone Number for maintenance services:	
	Website for maintenance services:	
Licensed Software Maintenance and Support: *(Contracting Authority should only insert when supplemental General Conditions 4004 has been inserted in Part 7).*	Toll-free Telephone Access:	
	Toll-Free Fax Access:	
	E-Mail Access:	
	Website address for web support:	
Security Clearance Level of Bidder **[include both the level and the date it was granted]** [**Note to Bidders:** *Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]*		

On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:

1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation;
2. This bid is valid for the period requested in the bid solicitation;
3. All the information provided in the bid is complete, true and accurate; and
4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.

(Form 1) **BID SUBMISSION FORM**	
Signature of Authorized Representative of Bidder	_____

(Form 2)

SUBSTANTIATION OF TECHNICAL COMPLIANCE FORM

Article of Statement of Work that requires substantiation by the Bidder	Bidder Substantiation	Reference to additional Substantiating Materials included in Bid
Mandatory Requirements		
M1		
M2		
M3		
M4		
M5		
M6		
M7		
M8		
M9		
M10		
M11		
M13		
M14		
M15		
M16		
M17		
M18		
M19		
M20		
M21		
M22		
M23		
M24		
M25		
M26		
M27		
M28		

M29		
M30		
M31		
M32		
M33		
M34		
M35		
M36		
M37		
M38		
M39		
M40		
M41		
M42		
M43		
M44		
M45		
M46		
M47		
M48		
M49		
M50		
M51		
M52		
M53		
M54		
M55		
M56		
M57		
M58		
M59		
M60		
M61		
M62		
M63		
M64		

M65		
M66		
M67		
Point-Rated Requirements		
R1		
R2		
R3		
R4		
R5		
R6		
R7		
R8		
R9		
R10		
R11		
R12		
R13		
R14		
R15		
R16		
R17		

(Form 3)

OEM CERTIFICATION FORM

This confirms that the original equipment manufacturer (OEM) identified below has authorized the Bidder named below to provide and maintain its products under any contract resulting from the bid solicitation identified below.

Name of OEM _____

Signature of authorized signatory of OEM _____

Print Name of authorized signatory of OEM _____

Print Title of authorized signatory of OEM _____

Address for authorized signatory of OEM _____

Telephone no. for authorized signatory of OEM _____

Fax no. for authorized signatory of OEM _____

Date signed _____

Solicitation Number _____

Name of Bidder _____

(Form 4)
SOFTWARE PUBLISHER CERTIFICATION FORM
(to be used where the Bidder itself is the Software Publisher)

The Bidder certifies that it is the software publisher of all the following software products and that it has all the rights necessary to license them (and any non-proprietary sub-components incorporated into the software) on a royalty-free basis to Canada pursuant to the terms set out in the resulting contract:

[Bidders should add or remove lines as needed]

(Form 5)
SOFTWARE PUBLISHER AUTHORIZATION FORM
(to be used where the Bidder is not the Software Publisher)

This confirms that the software publisher identified below has authorized the Bidder named below to license its proprietary software products under the contract resulting from the bid solicitation identified below. The software publisher acknowledges that no shrink-wrap or click-wrap or other terms and conditions will apply, and that the contract resulting from the bid solicitation (as amended from time to time by its parties) will represent the entire agreement, including with respect to the license of the software products of the software publisher listed below. The software publisher further acknowledges that, if the method of delivery (such as download) requires a user to "click through" or otherwise acknowledge the application of terms and conditions not included in the bid solicitation, those terms and conditions do not apply to Canada's use of the software products of the software publisher listed below, despite the user clicking "I accept" or signalling in any other way agreement with the additional terms and conditions.

This authorization applies to the following software products:

_____

_____

[Bidders should add or remove lines as needed]

Name of Software Publisher (SP) _____

Signature of authorized signatory of SP _____

Print Name of authorized signatory of SP _____

Print Title of authorized signatory of SP _____

Address for authorized signatory of SP _____

Telephone no. for authorized signatory of SP _____

Fax no. for authorized signatory of SP _____

Date signed _____

Solicitation Number _____

Name of Bidder _____

(Form 6)
DECLARATION FORM

This declaration form must be submitted as part of the bidding process. Please complete and submit in a **sealed envelope labelled "Protected**" to the attention of Integrity, Departmental Oversight Branch, PWGSC, 11 Laurier Street, Place du Portage, Phase III, Tower A, 10A1, Room 108, Gatineau (Québec) Canada K1A 0S5. Include the sealed envelope with your bid submission. This form is considered "Protected B" when completed.	
Complete Legal Name of Company:	
Company's address:	
Company's Procurement Business Number (PBN):	
Bid Number:	
Date of Bid: (YY-MM-DD)	

Have you ever, as the bidder, your affiliates or as one of your directors, been convicted or have pleaded guilty of an offence in Canada or similar offence elsewhere under any of the following provisions [1] :			
	Yes	**No**	**Comments**
Financial Administration Act 80(1) d): False entry, certificate or return 80(2): Fraud against Her Majesty 154.01: Fraud against Her Majesty **Criminal Code** 121: Frauds on the government and contractor subscribing to election fund 124: Selling or Purchasing Office 380: Fraud – committed against Her Majesty 418: Selling defective stores to Her Majesty	☐	☐	
In the last 3 years, have you, as the bidder, your affiliates or one of your directors, been convicted or have pleaded guilty of an offence in Canada or elsewhere under any of the following provisions [1]:			
Criminal Code 119: Bribery of judicial officers,... 120: Bribery of officers 346: Extortion 366 to 368: Forgery and other offences resembling forgery 382: Fraudulent manipulation of stock exchange transactions 382.1: Prohibited insider trading 397: Falsification of books and documents 422: Criminal breach of Contract 426: Secret commissions 462.31 Laundering proceeds of crime 467.11 to 467.13: Participation in activities of criminal organization **Competition Act** 45: Conspiracies, agreements or arrangements between competitors 46: Foreign directives 47: Bid rigging 49: Agreements or arrangements of federal financial institutions	☐	☐	

[1] for which no pardon or equivalent has been received.

	Yes	No	Comments
52: False or misleading representation 53: deceptive notice of winning a prize			
Corruption of Foreign Public Officials Act 3: Bribing a foreign public official 4: Accounting 5: Offence committed outside Canada **Controlled Drugs and Substance Act** 5: Trafficking in substance 6: Importing and exporting 7: Production of substance	☐ ☐	☐ ☐	
Other Acts 239: False or deceptive statements of the Income Tax Act 327: False or deceptive statements of the Excise Tax Act	☐	☐	

Additional Comment

☐ I, (name)_____, (position)_____, of (company name bidder)_____ _____authorise PWGSC to collect and use the information provided, in additional to any other information that may be required to make a determination of ineligibility and to publicly disseminate the results.

☐ I, (name) _____, (position) _____, of (company name bidder)_____certify that the information provided in this form is, to the best of my knowledge, true and complete. Moreover, I am aware that any erroneous or missing information could result in the cancellation of my bid as well as a determination of ineligibility/suspension.

We appreciate your interest in doing business with The Government of Canada and your understanding on the additional steps that we need to take to protect the integrity of PWGSC's procurement process.

(Form 7)
LIST OF NAMES FORM

In accordance with Part 5, Article 5.2 (a) - Integrity Provision – List of Names, please complete the Form below.

Complete Legal Name of Company	
Company's address	
Company's Procurement Business Number (PBN)	
Solicitation number	
Board of Directors (Use Format – first name last name) **Or put the list as an attachment**	
1. Director	
2. Director	
3. Director	
4. Director	
5. Director	
6. Director	
7. Director	
8. Director	
9. Director	
10. Director	
Other members	
Comments	

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B8815-170230
Security Classification / Classification de sécurité Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Immigration, Refugees and Citizenship	2. Branch or Directorate / Direction générale ou Direction: Communications
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
4. Brief Description of Work / Brève description du travail: Hosted Online Survey	

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No Non	☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No Non	☐ Yes Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non	☑ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No Non	☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☑ No Non	☐ Yes Oui

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

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

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B8815-170230
Security Classification / Classification de sécurité Unclassified

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — [✓] No / Non [ ] Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — [✓] No / Non [ ] Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

[✓] RELIABILITY STATUS / COTE DE FIABILITÉ	[ ] CONFIDENTIAL / CONFIDENTIEL	[ ] SECRET / SECRET	[ ] TOP SECRET / TRÈS SECRET
[ ] TOP SECRET– SIGINT / TRÈS SECRET – SIGINT	[ ] NATO CONFIDENTIAL / NATO CONFIDENTIEL	[ ] NATO SECRET / NATO SECRET	[ ] COSMIC TOP SECRET / COSMIC TRÈS SECRET
[ ] SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — [ ] No / Non [✓] Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted? — [✓] No / Non [ ] Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — [ ] No / Non [✓] Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — [✓] No / Non [ ] Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — [✓] No / Non [ ] Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — [ ] No / Non [✓] Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — [✓] No / Non [ ] Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B8815-170230
Security Classification / Classification de sécurité
Unclassified

PART C - *(continued)* / PARTIE C - *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRES SECRET
Information / Assets / Renseignements / Biens		✓														
Production																
IT Media / Support TI		✓														
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
B8815-170230
Security Classification / Classification de sécurité Unclassified

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Eric Glaude	Assistant Director	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-437-7583		eric.glaude@cic.gc.ca	2017-12-21

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Tracy Vitello	Senior Sec. Analyst	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-437-8907	—	tracy.vitello@cic.gc.ca	21 DEC 2017

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? / Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
BRIAN FULLUM	I.I.S.O.	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-948-3106	613-960-4334	Brian.Fullum@pwgsc.gc.ca	27/08/2018

Government of Canada

Security Control Profile for Cloud-based GC Services

Protected B / Medium Integrity / Medium Availability

VERSION 1.1

28 March 2018

GCDOCS#21145124

Foreword

Cloud computing has the potential to deliver agile and flexible IT services. Under the cloud computing paradigm, the Government of Canada (GC) relinquishes direct control over many aspects of security and privacy, and in doing so, confers a level of trust onto the cloud service provider. At the same time, GC departments and agencies using cloud services remain accountable for the confidentiality, integrity, and availability of the GC information systems and related information hosted by the cloud service provider. GC departments and agencies therefore need to understand cloud security and ensure risks are effectively addressed. To enable the adoption of cloud computing, an integrated risk management approach will be leveraged to establish cloud-based GC services.

The risk management framework used by the GC for managing IT security risks of cloud-based GC services consist of activities to:

- Perform security categorization (in terms of confidentiality, integrity, and availability) of each GC service being deployed on a cloud service;
- Select an appropriate set of security controls based on the GC service's security category;
- Select the right cloud deployment model and cloud service model for the GC service;
- Assess the implementation of the security controls in the supporting cloud service;
- Implement the required security controls in the GC service;
- Assess the implementation of the security controls in the GC service;
- Authorize operations of the resulting cloud-based GC service;
- Continuously monitor the security of the cloud-based GC service during the operation phase; and
- Maintain the authorization state of the cloud-based GC service.

To support these activities, the GC maintains cloud security control profiles suitable for GC programs and services of various sensitivities. Because of the shared nature of cloud computing, each party in a cloud-based GC service is responsible for the implementation, operation, and maintenance of a subset of the security controls in a profile. Cloud service providers use the security controls allocated to them for building and operating conformant cloud services. GC departments and agencies use the security controls allocated to them for procuring suitable cloud services and building, operating, and using GC services on top of conformant cloud services.

The CSE Information Technology Security Guidance (ITSG) 33 [2] on IT security risk management includes recommended security control profiles for information systems. These profiles have been used to develop the GC cloud profile documented herein.

This GC cloud profile is also heavily influenced by the security control profile for moderate impact information systems developed by NIST under the Federal Risk and Authorization Management (FedRAMP) program.

FedRAMP [9] is the US Federal Government risk management program that provides a standardized approach for authorizing and monitoring the security of cloud services. By aligning the GC cloud profiles to the FedRAMP profiles, the GC can maximize both the interoperability of cloud services and the reusability of the authorization evidence produced by cloud service providers.

Executive Summary

Cloud computing has introduced a fundamental shift in the way IT services are delivered and the Government of Canada (GC) has established a strategy [1] that will position itself to leverage this new IT service delivery model. Cloud adoption will ensure that the GC can continue to sustain IT service excellence during a period of increased demand by Canadians for online services and timely access to accurate information.

A key element to the GC's successful adoption of cloud computing is to ensure that an essential set of standardized security controls are properly implemented by cloud service providers (CSPs) to protect their cloud services, and by GC departments and agencies to protect the GC services and related information that are hosted on these cloud services. The level of security must be commensurate with the specific security needs of each GC service. By adhering to a standardized set of security controls, the GC, and more specifically departments and agencies, can identify and assess risks and develop strategies to appropriately mitigate them.

This document identifies the baseline security controls that must be implemented by CSPs and GC departments and agencies in order to appropriately protect cloud-based GC services and related information having a security category of Protected B, medium integrity, and medium availability. It also documents the context in which these security controls are expected to be implemented.

This security control profile was developed by GC lead security agencies based on current IT security risk management guidance from the Communications Security Establishment (CSE) [2] and the US National Institute of Standards and Technology [3].

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Acronyms

CIO	Chief Information Officer
CSE	Communications Security Establishment
FedRAMP	Federal Risk and Authorization Management Program
IM/IT	Information Management/Information Technology
ITSG	Information Technology Security Guidance
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
PBMM	Protected B, Medium Integrity, Medium Availability
RFP	Request for Proposal
SDLC	System Development Lifecycle
SLA	Service Level Agreement
SSC	Shared Services Canada
TBS	Treasury Board of Canada Secretariat

1. Introduction

1.1 Background

The Government of Canada (GC) develops and maintains security control profiles for the implementation of cloud-based GC services in support of the GC cloud adoption strategy [1]. A cloud-based GC service is a GC information system that is deployed over a cloud service. A security control profile is a set of IT security controls that an organization establishes as minimum mandatory requirements for their information systems.

The GC cloud security control profiles satisfy Treasury Board of Canada Secretariat (TBS) baseline security controls applicable to a generic set of departmental security needs, with due consideration for a GC technical context and threat context.

1.2 Scope and applicability

This document describes the security control profile for cloud-based GC services and related information having a security category of Protected B, medium integrity, and medium availability (PBMM). It specifies the security controls that need to be implemented in these information systems, and summarizes the context for which they apply.

The GC cloud PBMM profile is generally applicable to cloud-based services supporting a variety of non-national interest GC programs and services (e.g. programs or services that support sensitive government operations not including international affairs and defence, or federal-provincial affairs). It should only be reused in a similar context and only after performing an appropriate analysis.

1.3 Purpose

This document is to be used as the primary source of guidance for GC departments and agencies and cloud service providers (CSPs) to deploy, authorize, and operate cloud-based GC services.

1.4 Audience

This document is to be used by:

- CSPs to build cloud services suitable for use by the GC;
- GC program and service managers, business owners, IT project managers, and IT and IT security practitioners to procure suitable cloud services and implement GC services over these cloud services; and
- GC and departmental IT security authorities to assess, authorize, and monitor cloud-based GC services.

2. Context and Assumptions

This section summarizes the business contexts for which cloud security controls were selected and tailored.

Confidentiality: *The state of being disclosed only to authorized principals. [PGS* [23]*, adapted]*

Note: In IT security, confidentiality generally applies to information assets.

Integrity: *The state of being accurate, complete, authentic, and intact. [DDSM* [22]*]*

Note: In IT security, integrity generally applies to information assets. Integrity can also apply to business processes, software application logic, and hardware.

Availability: *The state of being accessible and usable in a timely and reliable manner. [PGS* [23]*, adapted]*

Note: In IT security, availability generally applies to information assets, application software, and hardware infrastructure and its components. Availability can also apply to processes.

2.1 Business Context

The GC cloud PBMM profile is suitable for cloud-based services supporting a wide range of GC business activities of medium sensitivity and criticality involving information to a maximum level of PROTECTED *B,* which is particularly sensitive information as described in the TBS Standard on Organization and Administration [4]. Examples of such business activities include, but are not limited to, the delivery of social services, taxation, Receiver General functions, departmental finance and administration, human resources, public service pay and benefits, and providing common and shared services to a broad client base.

Departments that are candidates for using the GC cloud PBMM profile will perform business activities with a maximum security category marking of PROTECTED B / Medium Integrity / Medium Availability, as defined in ITSG-33, Annex 1, Section 6 [2]. Business activities with such a marking have the following general characteristics:

• **Confidentiality** – A compromise of the confidentiality of PROTECTED B information is reasonably expected to cause a medium level of injury to non-national interests

• **Integrity** – A compromise of the integrity of supporting IT assets is reasonably expected to cause a medium level of injury to non-national interests

• **Availability** – A compromise of the availability of supporting IT assets is reasonably expected to cause a medium level of injury to non-national interests

• **Acceptable residual risks**– The business activities require the support of an information system operating with the lowest achievable residual risks for the security objectives of confidentiality, integrity and availability in a threat environment as described in Section 2.3 below.

Table 2-1 characterizes in greater detail suitable business contexts using confidentiality, integrity, and availability objectives. It also includes examples of consequences of compromise, business processes, and related information.

Table 2-1 Characterization of Applicable Business Contexts

Characteristics	Descriptions and Examples
Confidentiality Objective	The business activities involve the processing, transmission, and storage of PROTECTED B information that needs to be adequately protected from unintentional disclosure.
Integrity and Availability Objective	The expected injury from compromise of the integrity and availability of IT assets is assessed as medium. IT assets therefore need to be adequately protected from integrity and availability compromise.
Acceptable Residual Risks	The business activities require the support of an information system operating with the lowest achievable residual risks for the security objectives of confidentiality, integrity and availability.
Examples of Injuries	• Serious civil disorder or unrest • Physical pain, injury, trauma, hardship, or illness to individuals • Psychological distress or trauma to individuals • Financial loss to individuals that affects their quality of life • Financial loss to Canadian companies that reduces their competitiveness • Inability to conduct criminal investigations or other impediments to effective law enforcement • Disruption of government business activities that would seriously inconvenience Canadians
Examples of Business Processes	• Payments of benefits, to Canadians, whose disruption or delay could cause psychological harm to people • Police services whose disruption could cause physical harm to people or lead to civil disorder or unrest • Financial and reporting processes whose disruption could lead to serious financial losses to people or Canadian companies • Processing of large financial transactions and payments • Processes involving health care records
Examples of Information Assets	• Personal medical and financial information • Personal income tax information • Large financial transactions and payments • Information that could be used for criminal purposes (e.g., false identity or impersonation) • Information compiled as part of a criminal investigation • Information about an individual's eligibility for social benefits

Table 2-2 lists the business needs for security that were accounted for in developing the GC cloud PBMM profile. Business needs for security are a fundamental element of the IT security risk management process. Statements of business needs for security are used to influence the selection and

tailoring of security controls, and serve to establish assurance that information systems implement these security controls in a way that fully satisfies legislative and regulatory requirements.

Because of its genericity, the GC cloud PBMM profile may be used to support any GC business activity having a security category of PBMM or lower, which could be regulated by any of the thousands of legislative and regulatory requirements currently in effect in the GC. To limit the scope while maintaining the profile's genericity, the statement of business needs for security is limited to the following instruments:

- The Policy on Information Management [5];
- Directive on Information Management Roles and Responsibilities [6];
- Directive on Recordkeeping [7];
- Access to Information Act [8];
- Privacy Act [9]; and
- Library and Archives of Canada Act [10].

Table 2-2 Statement of Business Needs for Security

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-1	[5], 6.1.4	Authentication Integrity Non-repudiation	Deputy heads must ensure the authenticity of information for as long as it is required to meet operational needs and accountabilities.	Cloud-based GC services must ensure the authenticity and integrity of the information resources that they manage. Note: Where signed records or documents are stored, "information about the digital signature and its validation should be recorded within the metadata" [11].	• AC-3 Access enforcement • AC-5 Separation of duties • AC-6 Least privilege • AU-10 Non-repudiation • SC-8 Transmission confidentiality and integrity • SC-28 Protection of information at rest

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-2	[6], 6.2.2	Authentication Integrity Non-repudiation	Managers must ensure the authenticity and integrity of the information of programs and services for which they are responsible.	See under BNS-1.	See under BNS-1.
BNS-3	[7], 5.1.1	Integrity assurance	The integrity of information resources must be protected.	See under BNS-1.	See under BNS-1.
BNS-4	[8], 13(1)	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Subsection 13(1) (Information obtained in confidence) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	Cloud-based GC services must protect the confidentiality of protected information resources that they manage.	• AC-3 Access enforcement • AC-5 Separation of duties • AC-6 Least privilege • SC-8 Transmission confidentiality and integrity • SC-28 Protection of information at rest
BNS-5	[8], 13(2)	Authorization	To disclosure non-public information exempted from the general right of access under Subsection 13(1) (Information obtained in confidence) of the Access to Information Act, the head of a government institution must first obtain the authorization from the government, organization, or institution from which the information was obtained.	This process could be built into a cloud-based GC service.	• AC-3 Access enforcement • AC-5 Separation of duties • AC-6 Least privilege Note: This process would need to be implemented through an authorization function.

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-6	[8], 16(2)	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Subsection 16(2) (Security) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-7	[8], 16(3)	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Subsection 16(3) (Policing services for provinces and municipalities) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-8	[8], 17	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Section 17 (Safety of individuals) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-9	[8], 19(1)	Privacy (confidentiality of personal information)	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Subsection 19(1) (Personal information) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-10	[8], 19(2)	Authorization	To disclosure non-public information exempted from the general right of access under Subsection 19(1) of Access to Information Act (Personal information), the head of a government institution must first obtain authorization from the person to whom it relates.	See under BNS-5.	See under BNS-5.
BNS-11	[8], 20(1)	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Subsection 20(1) (Third party information) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-12	[8], 21(1)	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Subsection 21(1) (Advice, etc.) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-13	[8], 22	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Section 22 (Testing procedures, tests, and audits) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-14	[8], 23	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Section 23 (Solicitor-client privilege) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-15	[8], 24(1)	Confidentiality	The head of a government institution must protect the confidentiality of information exempted from the general right of access under Section 24(1) (Statutory prohibitions against disclosure) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-16	[8], 68(1)	Confidentiality	The head of a government institution must protect the confidentiality of information excluded from the general right of access under Subsection 68(1) (Canadian Broadcasting Corporation) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.
BNS-17	[8], 68(2)	Confidentiality	The head of a government institution must protect the confidentiality of information excluded from the general right of access under Subsection 68(2) (Atomic Energy of Canada Limited) of the Access to Information Act at a level commensurate with the expected level of injury from compromise.	See under BNS-4.	See under BNS-4.

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-18	[9], 5(1)	Authorization	To collect personal information from any source other than directly from the individual to whom it relates, a government institution must first obtain the authorization from that individual.	See under BNS-5.	See under BNS-5.
BNS-19	[9], 6(2)	Integrity assurance	A government institution must establish and maintain the integrity of personal information.	See under BNS-1.	See under BNS-1.
BNS-20	[9], 7	Authorization	To use personal information for purposes other than those for which it was collected, a government institution must first obtain the authorization from the individual to whom it relates.	See under BNS-5.	See under BNS-5.
BNS-21	[9], 8(1)	Authorization	To disclosure personal information for purposes other than those specified in Section 8, a government institution must first obtain the authorization from the individual to whom the information relates.	See under BNS-5.	See under BNS-5.
BNS-22	[9], 14	Timeliness	Where access to personal information is requested under Subsection 12(1) of the Privacy Act, the head of the government institution to which the request is made must give the individual who made the request access to the information within 30 days after the request is received.	Cloud-based GC services must ensure the availability of information to support this BNS.	• CP-9 Information system backup • CP-10 Information system recovery and reconstitution

ID	Ref.	Topic	Business Need for Security Statement	Interpretation in the Context of Cloud-based GC Services	Supporting Security Controls (most significant)
BNS-23	[10], 10(1)(b)	Timeliness	The publisher of an electronic publication made available in Canada shall provide the contents of that publication to the Librarian and Archivist 7 days after receiving a request from the Librarian and Archivist or as specified in the request.	See under BNS-22.	See under BNS-22.
BNS-24	[10], 12(1)	Authorization	The Librarian and Archivist, or a person duly delegated by the Librarian and Archivist, must authorize the disposal of government and ministerial records.	IM solutions must support authorized disposition of information.	• AC-3 Access enforcement • AC-5 Separation of duties • AC-6 Least privilege
BNS-25	[10], 12(3)	Authorization	The head of a government institution shall authorize access by the Librarian and Archivist to a record under the institution's control to which Subsection 24(1) (Statutory prohibitions against disclosure as set out in Schedule II) of the Access to Information Act applies.	See under BNS-5.	See under BNS-5.
BNS-26	[10], 15.1	Timeliness	A department shall send to the Librarian and Archivist the written report referred to in Subsection 40(2) of the Financial Administration Act within six months after the completion of any data collection done for the purposes of public opinion research carried out under a contract at the request of the department and for the exclusive use of Her Majesty in right of Canada.	See under BNS-22.	See under BNS-22.

2.2 Technical Context

The technical context for the GC cloud PBMM profile is defined by the cloud services and the GC services that are operating over these cloud services.

For cloud services, the GC cloud PBMM profile applies to:

- All existing CSP offerings;
- All cloud deployment models (public cloud, community cloud, private cloud, hybrid cloud) as defined by NIST [12]; and
- All cloud service models (infrastructure as a service, platform as a service, software as a service) as defined by NIST [12].

For GC services, the technical context is dictated largely by the cloud service offerings and there are no limits to what that context may be. The GC cloud PBMM profile neither prescribes nor proscribes any particular technologies and it should generally be suitable for any technical context provided by CSPs in their cloud service offerings.

2.3 Threat Context

The GC cloud PBMM profile has been developed to protect departmental business activities from IT-related threats that are relevant to both the business context and the technical context. In addition to the objective of protecting GC business activities, the profile aims to protect the cloud-based GC services. This approach is necessary as threats may be directed towards IT assets for no other reasons than to compromise technical components and benefit from their resources, irrespective of the type of business activities being supported by these IT assets.

For example, many attackers are not interested in GC information or in disrupting GC business activities; rather, they are interested in compromising cloud and non-cloud information systems in order to perform illegal acts, such as storing illegal data (e.g., images or movies) and covertly sharing that data with other criminals, performing denial of service attacks on commercial websites, extorting money, sending spam, or infecting computer systems with malware.

Threat information has been analyzed from multiple sources, including TBS and departmental threat and incident reports, in addition to analysis performed by CSE. As a result, the GC cloud PBMM profile, when correctly implemented, mitigates to a low residual level the risks from exposure to deliberate threat agents of categories from Td1 to Td4, and accidental threats and natural hazards of categories Ta1 to Ta3, as described in Table 2-3. As threat agent capabilities evolve over time, this profile will be updated to ensure that the selection of security controls is appropriately adjusted to mitigate new capabilities.

While this profile was developed by GC lead security agencies considering generic departmental requirements as a starting point, departments will still be required to ensure that the threat context is

applicable to their environment. Where the threat context differs, it is possible that further tailoring will be necessary, or that the department will have to accept higher levels of residual risk. If the differences are significant, a different security control profile may need to be selected, if available. Further guidance can be obtained from departmental IT security authorities if needed.

Table 2-3 Summary of Mandatory Threats to be mitigated (by Threat Category)

Deliberate Threats			Accidental Threats		
Category	**Typical Threat Actors**	**Selected**	**Category**	**Typical Threat Events**	**Selected**
Td1	Non-malicious adversary	Yes	Ta1	• Minor accidental events (e.g., trip over a power cord, enter wrong information)	Yes
Td2	Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening, *script kiddie*)	Yes	Ta2	• Moderate accidental events (e.g., render server inoperable, database corruption) • Minor hardware or software failures (e.g., hard disk failure) • Minor natural hazards (e.g., localized flooding, earthquake compromising part of a facility)	Yes
Td3	Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers)	Yes	Ta3	• Serious inadvertent or accidental events (e.g. fire in a facility, large scale database corruption) • Moderate mechanical failures (e.g., long term facility power failure) • Moderate natural hazards (e.g., localized flooding or earthquake compromising a facility)	Yes
Td4	Adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations)	Yes	Ta4	• Serious mechanical failures (e.g., long term, city-wide power failure) • Serious natural hazards (e.g., earthquake with city-wide devastation) • Serious inadvertent or accidental events	No
Td5	Adversary with moderate resources who is willing to take significant risk (e.g., organized crime, international terrorists)	No	Ta5	• Very serious mechanical failures (e.g., long term, regional power failure) • Very serious natural hazard (e.g., earthquake with regional or national devastation) • Very serious inadvertent or accidental events	No
Td6	Adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation)	No			

Deliberate Threats			Accidental Threats		
Category	**Typical Threat Actors**	**Selected**	**Category**	**Typical Threat Events**	**Selected**
Td7	Adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis)	No			

3. IT Security Approaches

3.1 Alignment with other Cloud Security Control Profiles

It is part of the GC cloud adoption strategy [1] to align GC cloud profiles with those of the Federal Risk and Authorization Management Program (FedRAMP) and other cloud-related initiatives, notably, the Cloud Security Alliance (CSA) [13], the US Defense Information System Agency (DISA) [14], and the International Organization for Standardization (ISO) [15]. This strategic alignment will help ensure interoperability between cloud service offerings, and the reusability of the IT security evidence used by other programs to certify or authorize cloud services.

3.2 Holistic Approach to IT Security

Unlike other cloud security control profiles, the GC cloud PBMM profile covers not just the CSP cloud service infrastructure but all of the CSP and GC infrastructure components that are used to both provide and consume cloud-based GC services. This holistic approach to IT security provides a stronger foundation to identify and mitigate risks to cloud-based GC services and related information from both a service or information hosting perspective and a service consumption or information use perspective.

As illustrated in Figure 3-1[1], the coverage of the GC cloud PBMM profile includes the CSP's cloud services infrastructure (consisting of people, processes, and technology), the GC service or information that is hosted on CSP's cloud services, the GC user devices and networks that are used to consume the cloud-based GC service or access GC information, and any other infrastructure components where related GC information may reside.

[1] Figure based on NIST SP 500-292 Cloud Computing Reference Architecture and NIST SP 500-299 Cloud Computing Security Reference Architecture

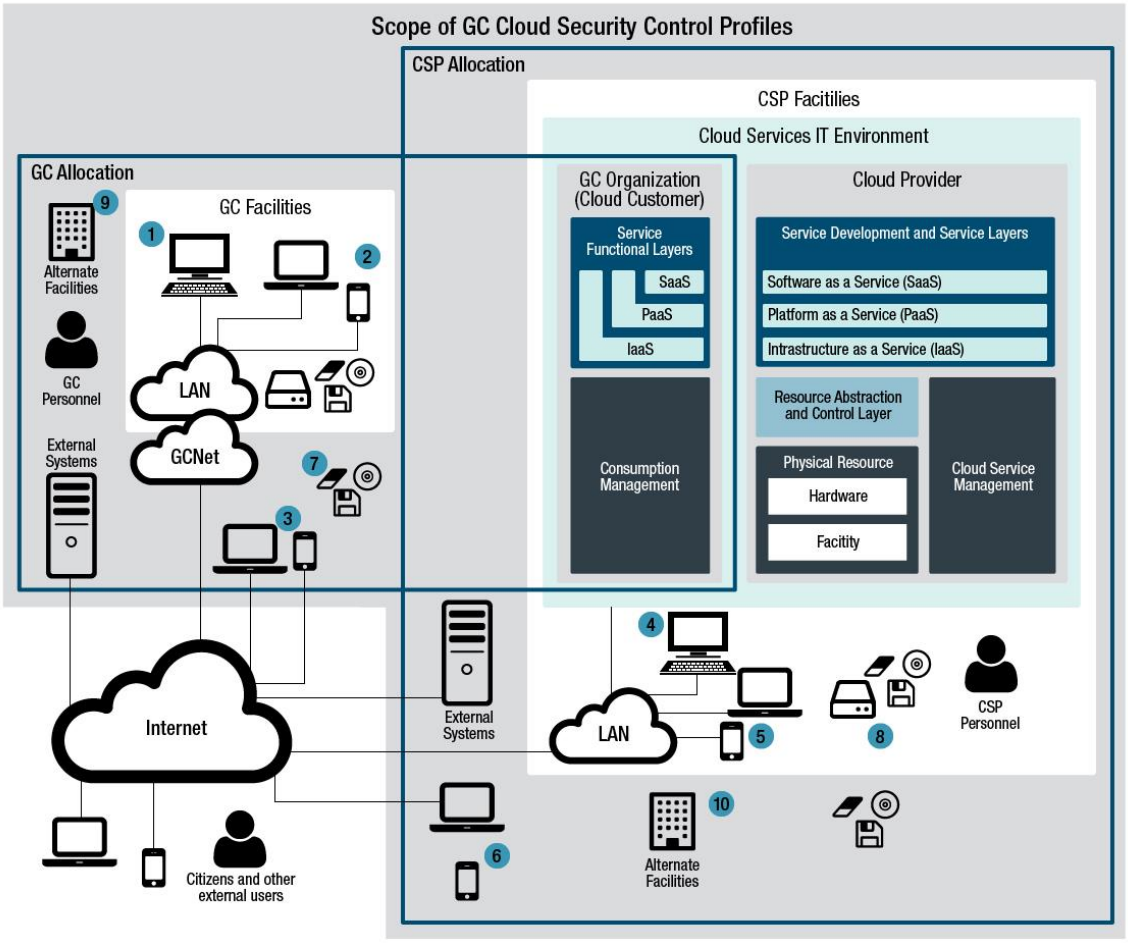

Figure 3-1 Scope of GC Cloud PBMM Profile

The scope of the GC cloud PBMM profile can be demonstrated using the following use cases:

1) A GC user accesses a cloud-based GC service from a GC local network.
2) A GC user accesses a cloud-based GC service from a GC local wireless network.
3) A GC user accesses a cloud-based GC service from the internet.
4) A CSP user accesses the cloud service environment from the CSP's local network.
5) A CSP user accesses the cloud service environment from the CSP's local wireless network.
6) A CSP user accesses the cloud service environment from the internet.
7) A GC user stores cloud-hosted information on a portable storage media.
8) A CSP user stores GC or CSP information on a portable storage media.
9) A GC system administrator creates a backup of cloud-hosted information and sends the backup media at an alternative facility.
10) The CSP uses an alternate facility to support their cloud service contingency plan.

In this holistic approach to cloud security, the majority of the security controls in the GC cloud PBMM profile needs to be implemented by both the CSP and GC departments and agencies, while some security controls need to be implement only by one or the other. The presence of these party-specific security controls is a direct result of the GC cloud adoption strategy (discussed in Section 3.1). It reflects the delta between cloud-based security control profiles and the generic ITSG-33 PBMM profile that GC departments and agencies are recommended to implement (in current GC IT security risk management guidance) for all information systems supporting their GC programs and services.

3.3 IT Security Engineering Principles

In addition to the business, technical, and threat contexts documented in previous sections, the selection of security controls for the GC cloud PBMM profile was also influenced by the choice of security engineering best-practices applied to the implementation of dependable information systems. This profile is meant to address the IT security needs of a broad range of business activities, from day-to-day office work to citizen-facing service delivery applications to common and shared service infrastructure support. The protection of business activities call for security approaches where, at a minimum, the following main security engineering best-practices are applied:

- *Defence-in-depth:* technical, operational (including personnel and physical), and management security controls are used in a mutually supportive manner to mitigate risks (e.g., technical access controls used to protect sensitive databases, and additional physical security to prevent unauthorized personnel to physically access the database servers).
- *Least-privilege*: users are provided only the minimum access necessary to perform their duties (e.g., day-to-day tasks are performed using limited user accounts only, not administrative accounts).
- *Prevent-detect-analyze-respond-recover (PDARR)*: prevents attacks from being successful to the maximum extent feasible and then ensures that successful attacks can be detected and contained, IT assets can be restored to a secure and authentic state, and lessons learned are documented and used to improve the security posture of information systems.
- *Layered defence:* ensures that the various layers of an information system such as applications, databases, platforms, middleware, and communications are adequately protected. This approach reduces the risk that a weakness in one part of the information system could be exploited to circumvent safeguards in other parts (e.g., SQL injection application-layer attacks bypassing network-layer boundary protection).

The broad range of applicability of this profile does not lend itself easily to the use of a set of IT security approaches where strict boundary protection and strong physical and personnel security are used as the main protection measures (this approach could potentially afford the use of weaker internal security controls). In contrast, this profile suggests a balanced set of security controls to reduce the risks of compromised internal elements of an information system being used to easily compromise additional

elements. This profile also suggests security controls to detect, respond, and recover gracefully from security incidents. Many of these controls are operational controls that a mature CSP should have in place, not only for security reasons, but also for the efficient and cost-effective day-to-day operations and management of information systems.

Note: While selecting security controls is somewhat subjective, considerable effort was made to include security controls that mitigate real threats, and that can be implemented using readily available COTS products. As well, the selection of security controls was aligned to existing cloud security best practices and international cloud security certifications. Security controls that specify a specialized or advanced capability not required for all information systems were excluded from this security profile. Furthermore, every effort was made to achieve the appropriate balance between usability and security.

3.4 Multi-tenant Separation

There are threats specific to cloud computing that may not necessarily be mitigated to a sufficient degree by conforming to a standard set of security controls developed for non-cloud IT environments. In the absence of additional security controls to mitigate these cloud-specific threats, it is reasonable to expect a conforming cloud service to be operating at higher levels of residual risk than what would normally be expected in a more-traditional IT environment.

The most-significant increase in risk comes from the presence within cloud environments of multiple tenants, which may be operating under very different security requirements. A tenant operating under a less-stringent set of security controls could expose another tenant to unacceptable levels of risk because their respective cloud-based services are operating within a common logical environment over a common physical platform. One way to reduce this exposure is to separate the tenants whereby tenants with similar security requirements are grouped together and each group is provided with separate logical environments over a common physical platform, or completely separate physical environments. The physical separation reduces exposure more than logical separation. However, the downside of physical separation is a decrease in the hardware consolidation ratio, and a corresponding increase in costs to CSPs and, ultimately, to their consumers.

CSE provides network security zoning recommendations in ITSG-22 [16] and ITSG-38 [17], that, if implemented correctly in a cloud environment, would result in relatively strong multi-tenant

separation[2]. GC departments and agencies will need to determine if and how authorized CSPs have implemented multi-tenant separation and must ensure that related threats and risks are taken into account when provisioning cloud services for their cloud-based GC service implementation initiatives.

3.5 Security Control Tailoring

The GC cloud PBMM profile specifies a baseline of security controls suitable to protect business processes and information as described in Section 2.1. The profile aims to ensure the appropriate mitigation of threats that could compromise through cloud-based GC services the confidentiality, integrity, and availability of IT assets supporting GC programs, services, and business activities.

Further tailoring of this profile for specific departmental security needs may be required. However, GC organizations may need to limit tailoring to security controls that are within their scope of responsibility, as their ability to influence change in public cloud service offerings will likely be limited. This may apply to a lesser degree in private cloud service offerings, where the ability to negotiate changes to security controls is greater. This analysis is critical as it will define which deployment model can best meet a department's requirement. If deemed necessary, further tailoring of this profile to satisfy specific departmental security needs will have to take into account the complex and subtle relationships between cloud consumers and CSPs as well as their scope of responsibility within the cloud service infrastructure.

To assist with tailoring and implementation, the GC cloud PBMM profile includes a suggested allocation of security controls and enhancements to the consumer and provider organizations and the cloud computing architecture layers defined in the NIST cloud computing reference architecture [18].

[2] Like other cloud security control profiles (with the exception of ISO/IEC 27017) [8], the GC cloud PBMM profile does not directly prescribe multi-tenant separation in its security controls. There are some security controls that call for the separation of information flow by type (AC-4) and process isolation (SC-39), but these mechanisms alone do not constitute multi-tenant separation. Under security control SC-7, the profile calls for the establishment of external and internal boundary protection that could result in a significant degree of separation of tenant resources; however, there is no guarantee as the implementation is left to the CSP who could conform to this security control without achieving any significant degree of separation.

3.6 Procurement Considerations

Cloud service offerings are being acquired following the standard GC procurement process. This means that CSPs are subject to the Public Services and Procurement Canada (PSPC) Industrial Security Program. Through this program, the GC will include an appropriate set of security clauses in request for proposals (RFPs) for inclusion in cloud services contracts, while CSPs establish a strong personnel and physical security foundation for correctly implementing the IT security controls in the GC cloud PBMM profile.

4. GC Cloud PBMM Security Control Profile

Appendix A lists the security controls and control enhancements that constitute the GC cloud PBMM profile. This list is also maintained in other forms that are more suitable for use by IT and IT security practitioners as input to requirements engineering and other system development lifecycle (SDLC) activities.

While the entire GC cloud PBMM profile applies to a cloud-based GC service, neither the CSP's nor the GC's scope of responsibility extends to all of the security controls in the profile. This is illustrated in Figure 3-1. On the one hand, the profile includes GC-specific security controls that the CSP is not expected to implement. On the other hand, the profile includes cloud-specific security controls that GC organizations are not expected to implement. This variation in security control responsibility is a direct result of the GC cloud strategy taking a holistic approach to IT security (as outlined in Section 3.2), conforming to CSE's recommended security controls, and maintaining an alignment with other cloud security initiatives for reasons of compatibility and reusability. The allocation of security control responsibility is included in Appendix A.

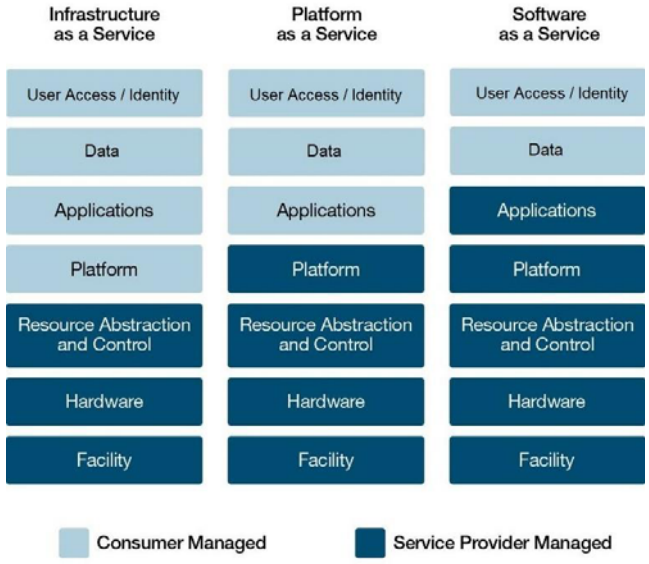

Figure 4-1 Scope of Responsibility

From the perspective of the CSP's infrastructure (delimited in Figure 3-1 by the CSP facilities component), the scope of responsibility also varies depending on the cloud service model. Figure 4-1 is a simplified view of the architectural layers to support the depiction of the scope of responsibility as it applies to the service models, using the NIST cloud reference architecture [18] and the cloud computing layers in NIST 500-299 [19] as the basis of the illustrations. An organization view was added to the cloud computing layers for security controls that are implemented by people, for example the development of

policies and procedures, the execution of access control procedures, personnel security, security assessment and authorization, and risk management.

Under IaaS, the consumer has the capability to provision fundamental computing resources such as operating systems, storage, and networking, as well as the application software operating over these resources [18]. Consequently, the consumer may be responsible for some of the security controls of the virtualization infrastructure layer and all of the security controls of the consumer organization, platform, and application layers. The consumer has no responsibility for the security controls of the hardware and facility layers.

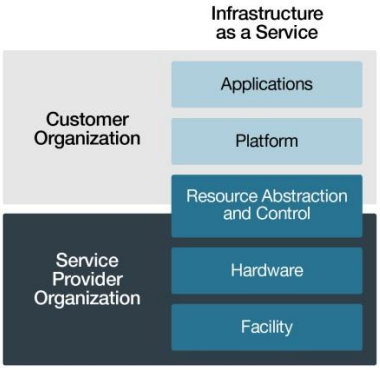

Figure 4-2 Scope of Responsibility for IaaS

Under PaaS,the consumer has the capability to implement commercial software products over and custom business applications over CSP-provided operating systems, servers, and networks , application frameworks, and other program libraries and tools [19]. As a result, the consumer may be responsible for some of the security controls of the platform layer and all the security controls of the consumer organization and application layers.

Figure 4-3 Scope of Responsibility for PaaS

Under SaaS,the consumer has the capability to use CSP-provided software products and applications. In some cases, the consumer may also have the capability to configure certain aspects of a software product or application, for example, manage user accounts, create folder structures, or select and deselect optional functions. Consequently, the consumer may be responsible for some of the security controls of the application layer.

Figure 4-4 Scope of Responsibility for SaaS

The allocation of the GC cloud PBMM profile to the the cloud computing archectural layers is included in Appendix A. Table 4-1 provides a summary of the allocation mapped to the following security control families:

AC - Access control
AT - Awareness and training
AU - Audit & accountability
CA - Security assessment and authorization
CM - Configuration management
CP - Contingency planning
IA - Identification and authentication
IR - Incident response
MA - Maintenance
MP - Media protection
PE - Physical and environmental
PL - Planning
PM - Program management
PS - Personnel security
RA - Risk assessment
SA - System and services acquisition
SC - System and communications protection
SI - System and information integrity

Table 4-1 Summary of Security Control Responsibility

	Cloud Service Model	Architectural Layers	Security Control Families
Consumer	SaaS	Application	AC, AU, IA, SC, SI
	PaaS	Platform	AC, AU, CM, CP, IA, MA, SC, SI
	IaaS	Virtualization Infrastructure	AC, AU, CM, CP, IA, MA, SC, SI
	All	Facility & Hardware	Not applicable
	All	Organization	AC, AT, AU, CA, CM, CP, IA, IR, MA, PL, PS, RA, SA, SC, SI
Cloud Service Provider	SaaS	Application	AC, AU, IA, SC, SI
	PaaS	Platform	AC, AU, CM, CP, IA, MA, SC, SI
	IaaS	Virtualization Infrastructure	AC, AU, CM, CP, IA, MA, SC, SI
	All	Facility & Physical	PE
	All	Organization	AC, AT, AU, CA, CM, CP, IA, IR, MA, MP, PE, PL, PM, PS, RA, SA, SC, SI

5. References

[1] Treasury Board of Canada Secretariat (TBS), "GC Cloud Adoption Strategy," DRAFT, December 2015.

[2] Communications Security Establishment (CSE), "[ITSG-33] IT Security Risk Management: A Lifecycle Approach," November 2012.

[3] National Institute of Standards and Technology (NIST), "NIST Special Publications, SP800s - Computer Security," [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html#SP 800.

[4] Treasury Board of Canada Secretariat, "Security Organization and Administration Standard," June 1995.

[5] Treasury Board of Canada Secretariat, "Policy on Information Management," [Online]. Available: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742.

[6] Treasury Board of Canada Secretariat, "Directive on Information Management Roles and Responsibilities," [Online]. Available: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12754.

[7] Treasury Board of Canada Secretariat, "Directive on Recordkeeping," [Online]. Available: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16552.

[8] Department of Justice Canada, "Access to Information Act," [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/A-1/index.html.

[9] Department of Justice Canada, "Privacy Act," [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html.

[10] Department of Justice Canada, "Library and Archives of Canada Act," [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/L-7.7/index.html .

[11] International Council on Archives, "Principles and Functional Requirements for Records in Electronic Office Environments," [Online]. Available: http://www.adri.gov.au/resources/documents/ICA-M2-ERMS.pdf.

[12] National Institute of Standards and Technology (NIST), "[SP800-145] The NIST Definition of Cloud Computing," September 2011.

[13] Cloud Security Alliance (CSA), "Cloud Controls Matrix (CCM)," [Online]. Available: https://cloudsecurityalliance.org/group/cloud-controls-matrix/.

[14] Defense Information Systems Agency (DISA), "Department of Defense Cloud Computing Security Requirements Guide," March 18, 2016.

[15] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), "[ISO/IEC 27017] Inforamtion technology - Security techniques - Code of practice for information technology security controls based on ISO/IEC 27002 for cloud services," 2015-12-15.

[16] Communications Security Establishment (CSE), "[ITSG-22] Baseline Security Requirements for Network Security Zones in the Government of Canada," June 2007.

[17] Communications Security Establishment (CSE), "[ITSG-38] Network Security Zoning: Design Considerations for Placement of Services within Zones," May 2009.

[18] National Institute of Standards and Technology, "NIST Cloud Computing Reference Architecture (SP 500-292)," September 2011.

[19] National Institute for Standards and Technology, "NIST Cloud Computing Security Reference Architecture [SP 500-299]," Draft, 2013.

[20] U.S. General Services Administration (GSA), "Federal Risk and Authorization Management Progarm (FedRAMP)," [Online]. Available: https://www.fedramp.gov/.

[21] American Institute of Certified Public Accountants (AICPA), "Service Organization Controls (SOC)," [Online]. Available: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html.

[22] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements," 2013.

[23] Treasury Board of Canada Secretariat (TBS), "Directive on Departmental Security Management," July 2009.

[24] Treasury Board of Canada Secretariat (TBS), "Policy on Government Security," April 1, 2012.

Appendix A –Security Control Profile

The security controls and enhancements that constitute the GC cloud PBMM profile are listed in the table below. The table also shows the allocation of security controls to the GC and CSPs, the cloud components to which they apply as per Figure 3-1, and cross referenced to other related profiles and standards.

Note that the mapping table provided in this appendix provide organizations with a general indication of security control coverage in comparison to the following informative references:

- Federal Risk and Authorization Management Program (FedRAMP) Moderate [20]
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) [13]
- AICPA Service Organization Controls (SOC) [21]
- ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements [22]

The following values are included in the table:

- X indicates that the control was selected or is applicable
- Not selected indicates that the control was not selected for inclusion in the profile
- Not allocated indicates that the control is selected, but not the responsibility for either the GC or the CSP to implement
- Not applicable indicates that the control is not included in the standard/profile (e.g. PM control family not included in ITSG-33 Annex 3 Controls Catalog)

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
			469	433	335								433	325			
AC-1	Access Control Policy and Procedures	(A) Personnel or roles = [personnel or roles with access control responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AIS-04 AAC-03 DSI-04 GRM-06 GRM-08 GRM-09 GRM-11 IAM-02 IAM-05 IAM-07 IAM-12 IVS-12	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.9.1.1 A.12.1.1 A.18.1.1 A.18.2.2
AC-2	Account Management	(A) Information system account types = To be defined as part of the tailoring process (E) Personnel or roles = [responsible managers] (F) Procedures or conditions = [information system account management procedures] (J) Frequency = [at least annually]	X	X	X	X	X						X	X	IAM-05 IAM-10 IAM-11 IAM-12	CC5.2 CC6.1	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.5 A.9.2.6
AC-2(1)	Account Management | Automated System Account Management	Not applicable	X	X	X	X	X						X	X	IAM-05 IAM-10 IAM-11	CC5.2	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts	Selection: removes; disables = [disables] Time period = [no more than 30 days for both temporary and emergency accounts]	X	X	X				X	X	X	X	X	X	IAM-05 IAM-10 IAM-11	CC5.2	
AC-2(3)	Account Management | Disable Inactive Accounts	Time period = [90 days]	X	X	X				X	X	X	X	X	X	IAM-05 IAM-10 IAM-11	CC5.2	
AC-2(4)	Account Management | Automated Audit Actions	Personnel or roles = [as defined under AC-2(A)]	X	X	X				X	X	X	X	X	X	IAM-05 IAM-10 IAM-11	CC5.2	
AC-2(5)	Account Management | Inactivity Logout	Time period or description = [leaving at the end of their workday]	X	X	X	X	X						X	X		CC5.3	
AC-2(7)	Account Management | Role-Based Schemes	(c) Actions = [remove privileged role assignments]	X	X	X	X	X						X	X	IAM-05 IAM-10 IAM-11	CC5.4	
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts	Conditions = To be defined as part of the tailoring process	X	Not allocated	X	X							Not Selected	X		CC5.2	
AC-2(10)	Account Management | Shared / Group Account Credential Termination	Not applicable	X	Not allocated	X				X	X	X	X	Not Selected	X		CC5.2	
AC-3	Access Enforcement	Not applicable	X	X	X				X	X	X	X	X	X	IAM-09 IAM-12	CC5.1	A.6.2.2 A.9.1.2 A.9.4.1 A.9.4.4 A.9.4.5 A.13.1.1 A.14.1.2 A.14.1.3 A.18.1.3
AC-3(4)	Access Enforcement | Discretionary Access Control	DAC policies = To be defined as part of the tailoring process	X	X	Not allocated				X	X	X	X	X	Not Selected		CC5.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-3(7)	Access Enforcement | Role-Based Access Control	Roles and users = [as specified under AC-2(A)]	X	X	Not allocated				X	X	X	X	X	Not Selected			
AC-3(9)	Access Enforcement | Controlled Release	(a) System or component = To be defined as part of the tailoring process (a) Security safeguards = To be defined as part of the tailoring process (b) Security safeguards = To be defined as part of the tailoring process	X	X	Not allocated					X	X	X	X	Not Selected			
AC-3(10)	Access Enforcement | Audited Override of Access Control Mechanisms	Conditions = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
AC-4	Information Flow Enforcement	(A) Information flow control policies = [deny all, approve by exception information flow policies]	X	X	X				X	X	X		X	X	AIS-04 DSI-01 IVS-09	CC5.1	A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3
AC-4(21)	Information Flow Enforcement | Physical / Logical Separation of Information Flows	Mechanisms and techniques = [session encryption and in accordance with ITSG-22] Required separations = [separation of all sessions]	X	Not allocated	X				X	X	X		Not Selected	X		CC5.1	
AC-5	Separation of Duties	(A)(a) Duties = To be defined as part of the tailoring process	X	X	X	X	X						X	X	IAM-05 IAM-09	CC5.1	A.6.1.2
AC-6	Least Privilege	Not applicable	X	X	X	X	X						X	X	IAM-05 IAM-09 IAM-13	CC5.4	A.6.1.2
AC-6(1)	Least Privilege | Authorize Access to Security Functions	Functions and information = [all security functions not publicly accessible and all security-relevant information not publicly available]	X	X	X	X	X						X	X	IAM-05 IAM-09 IAM-13	CC5.4	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-6(2)	Least Privilege | Non-Privileged Access for Non-Security Functions	Functions or information = [any security function]	X	X	X	X	X						X	X	IAM-05 IAM-09 IAM-13	CC5.1	
AC-6(5)	Least Privilege | Privileged Accounts	Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	X		CC5.4	
AC-6(9)	Least Privilege | Auditing Use of Privileged Functions	Not applicable	X	X	X				X	X	X	X	X	X		CC6.1	
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	Not applicable	X	X	X				X	X	X	X	X	X		CC5.1	
AC-7	Unsuccessful Logon Attempts	(A) Number = [not more than three] (A) Time period = [15 minutes] (B) Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm] = [locks the account/node for a [Assignment: organization-defined time period]] (B) Time period (if selected) = 30 minutes (B) Delay algorithm (if selected) = Not selected	X	X	X				X	X	X	X	X	X	IAM-02	CC5.3	A.6.1.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-8	System Use Notification	(A) Message or banner = To be defined as part of the tailoring process (C)(a) Conditions = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	X	HRS-08	CC2.3	A.6.1.2
AC-9	Previous Logon (Access) Notification	Not applicable	X	X	Not allocated					X	X	X	X	Not Selected			A.6.1.2
AC-9(3)	Previous Logon (Access) Notification | Notification of Account Changes	Changes = To be defined as part of the tailoring process Time period = To be defined as part of the tailoring process	X	X	Not allocated					X	X	X	X	Not Selected			
AC-10	Concurrent Session Control	(A) Account and/or account type = [for all accounts unless justified for operation requirements] (A) Number = [3 sessions for privileged access and 2 sessions for non-privileged access]	X	Not allocated	X				X	X	X	X	Not Selected	X	IAM-02	CC5.3	None
AC-11	Session Lock	(A) Time period = [15 minutes]	X	X	X				X	X	X	X	X	X	HRS-11 IAM-12	CC5.3	A.11.2.8 A.11.2.9
AC-11(1)	Session Lock | Pattern-Hiding Displays	Not applicable	X	X	X				X	X	X	X	X	X	IAM-12	CC5.3	
AC-12	Session Termination	(A) Conditions or trigger events = [upon request by user and after a maximum of 24 hours of inactivity] *Note: For CSP, this applies to CSP privileged users.*	X	Not allocated	X				X	X	X	X	Not Selected	X		CC5.3	None
AC-14	Permitted Actions without Identification or Authentication	(A) User actions = To be defined as part of the tailoring process	X	X	X	X	X						X	X	IAM-02	CC5.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-16	Security Attributes	(A) Types of security attributes = To be defined as part of the tailoring process (A) Security attribute values = To be defined as part of the tailoring process (C) Security attributes = To be defined as part of the tailoring process (C) Information systems = To be defined as part of the tailoring process (D) Values or ranges = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected	DSI-04	CC5.1	None
AC-16(2)	Security Attributes | Attribute Value Changes by Authorized Individuals	Not applicable	X	X	Not allocated					X	X	X	X	Not Selected			
AC-16(4)	Security Attributes | Association of Attributes by Authorized Individuals	Security attributes = To be defined as part of the tailoring process Subjects and objects = To be defined as part of the tailoring process	X	X	Not allocated					X	X	X	X	Not Selected			
AC-16(5)	Security Attributes | Attribute Displays for Output Devices	Instructions = To be defined as part of the tailoring process Naming convention = To be defined as part of the tailoring process	X	X	Not allocated					X	X	X	X	Not Selected			
AC-17	Remote Access	***NOTE: Item (AA) is not applicable to CSPs.***	X	X	X	X	X						X	X	DCS-04 HRS-05	CC5.6	A.6.2.1 A.6.2.2 A.13.1.1 A.13.2.1 A.14.1.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-17(1)	Remote Access | Automated Monitoring / Control	Not applicable	X	X	X				X	X	X	X	X	X	DCS-04 HRS-05	CC5.6	
AC-17(2)	Remote Access | Protection of Confidentiality / Integrity using Encryption	Not applicable	X	X	X				X	X	X	X	X	X	DCS-04 HRS-05	CC5.6	
AC-17(3)	Remote Access | Managed Access Control Points	Number = [approved]	X	X	X				X	X			X	X	DCS-04 HRS-05	CC5.6	
AC-17(4)	Remote Access | Privileged Commands / Access	(a) Needs = [justified operational requirements]	X	X	X	X	X						X	X	DCS-04 HRS-05	CC5.6	
AC-17(6)	Remote Access | Protection of Information	Not applicable	X	X	X	X	X						X	Not Selected		CC2.3	
AC-17(100)	Remote Access | Remote Access to Privileged Accounts using Dedicated Management Console	Not applicable	X	X	Not allocated					X	X	X	X	Not Selected			
AC-18	Wireless Access	Not applicable	X	X	X	X							X	X	EKM-03 HRS-05 IVS-12	CC5.6	A.6.2.1 A.13.1.1 A.13.2.1
AC-18(1)	Wireless Access | Authentication and Encryption	Section (one or more): users; devices = To be defined as part of the tailoring process	X	X	X				X				X	X	EKM-03 HRS-05 IVS-12	CC5.6	
AC-18(3)	Wireless Access | Disable Wireless Networking	Not applicable	X	X	X	X							X	Not Selected		CC7.4	
AC-18(4)	Wireless Access | Restrict Configurations by Users	Not applicable	X	X	Not allocated		X						X	Not Selected			
AC-19	Access Control for Mobile Devices	Not applicable	X	X	X	X	X						X	X	HRS-05	CC5.6	A.6.2.1 A.11.2.6 A.13.2.1
AC-20	Use of External Information Systems	Not applicable	X	X	X	X	X						X	X	HRS-08	CC2.3	A.11.2.6 A.13.1.1 A.13.2.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AC-20(1)	Use of External Information Systems | Limits of Authorized Use	Not applicable	X	X	X	X	X						X	X	HRS-08	CC5.6	
AC-20(2)	Use of External Information Systems | Portable Storage Devices	Selection: restricts; prohibits = [restricts unless approval obtained for operational reasons]	X	X	X	X	X						X	X	HRS-08	CC5.6	
AC-20(3)	Use of External Information Systems | Non-Organizationally Owned Systems / Components / Devices	Selection: restricts; prohibits = [restricts use of external information systems by personnel with privileged access]	X	X	Not allocated		X						X	Not Selected			
AC-20(4)	Use of External Information Systems | Network Accessible Storage Devices	Devices = [restricts unless approval obtained for operational reasons]	X	X	Not allocated		X						X	Not Selected			
AC-21	Information Sharing	(A) Circumstances = To be defined as part of the tailoring process (B) Automated or manual = To be defined as part of the tailoring process	X	X	X	X	X						X	X		CC5.4	None
AC-21(100)	Information Sharing | Safeguarding of Sensitive Information	Not applicable	X	X	Not allocated		X						X	Not Selected			
AC-22	Publicly Accessible Content	(D) Frequency = [at least quarterly]	X	X	X	X	X						X	X	DSI-03	CC5.4	None
AT-1	Security Awareness and Training Policy and Procedures	(A) Personnel or roles = [personnel or roles with security awareness and training responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 GRM-06 GRM-08 GRM-09 GRM-11 HRS-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
AT-2	Security Awareness Training	(A)(c) Frequency = [at least annually]	X	X	X	X	X						X	X	GRM-03 HRS-09 HRS-10	CC2.3	A.7.2.2.2 A.12.2.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AT-2(2)	Security Awareness Training | Insider Threat	Not applicable	X	X	X	X	X						X	X		CC1.3 CC2.5	
AT-3	Role-Based Security Training	(A)(c) Frequency = [at least annually]	X	X	X	X	X						X	X	GRM-03 HRS-09 HRS-10	CC2.3	A.7.2.2*
AT-3(4)	Role-Based Security Training | Suspicious Communications and Anomalous System Behavior	Indicators of malicious code = [current indicators of malicious code]	X	X	X	X	X						X	Not Selected		CC1.3	
AT-4	Security Training Records	(B) Time period = [at least one year]	X	X	X	X	X						X	X	GRM-03 HRS-09 HRS-10	CC2.3	None
AU-1	Audit and Accountability Policy and Procedures	(A) Personnel or roles = [personnel or roles with audit responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 GRM-06 GRM-08 GRM-09 GRM-11 IAM-05 IAM-07 IVS-01 IVS-03	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-2	Audit Events	(A) Auditable events = [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes] (D) Auditable events (or subject thereof) with frequency of or situation for auditing = To be defined as part of the tailoring process	X	X	X	X	X						X	X	IAM-05 IAM-12 IVS-01	CC6.1	None
AU-2(3)	Audit Events | Reviews and Updates	Frequency = [annually or whenever there is a change in the threat environment]	X	X	X	X	X						X	X	IAM-12 IVS-01	CC6.1	
AU-3	Content of Audit Records	Not applicable	X	X	X				X	X	X	X	X	X	IVS-01	CC6.1	A.12.4.1*
AU-3(1)	Content of Audit Records | Additional Audit Information	Additional/More information = [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon]	X	X	X				X	X	X	X	X	X	IVS-01	CC6.1	
AU-4	Audit Storage Capacity	(A) Storage requirements = [capacity that is sufficient to support the requirement under AU-11]	X	X	X	X	X						X	X	IVS-01	CC6.1	A.12.1.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-4(1)	Audit Storage Capacity | Transfer to Alternate Storage	Frequency = [as audit records are generated or as soon as operationally feasible]	X	X	X				X	X	X	X	X	Not Selected		CC6.1	
AU-5	Response to Audit Processing Failures	(A) Personnel or roles = To be defined as part of the tailoring process (B) Additional actions = [overwrite oldest audit records]	X	X	X				X	X	X	X	X	X	IVS-01	CC6.1	None
AU-5(1)	Response to Audit Processing Failures | Audit Storage Capacity	Personnel, roles, and/or locations = To be defined as part of the tailoring process Time period = To be defined as part of the tailoring process Percentage = [75%]	X	X	Not allocated					X	X	X	X	Not Selected			
AU-6	Audit Review, Analysis, and Reporting	(A) Frequency = [at least weekly] (A) Inappropriate or unusual activity = [indicators of compromise identified in SI-4(5)] (B) Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	X	IAM-05 IAM-10 IVS-01 SEF-04	CC6.1	A.12.4.1 A.16.1.2 A.16.1.4
AU-6(1)	Audit Review, Analysis, and Reporting | Process Integration	Not applicable	X	X	X	X	X						X	X	IAM-05 IAM-10 IVS-01 SEF-04	CC6.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-6(3)	Audit Review, Analysis, and Reporting | Correlate Audit Repositories	Not applicable	X	X	X	X	X						X	X	IAM-05 IAM-10 IVS-01 SEF-04	CC6.1	
AU-6(4)	Audit Review, Analysis, and Reporting | Central Review and Analysis	Additional information: The information system provides the capability to centrally review and analyze audit records from multiple components [within each tenant's system boundary and the CSP's own system boundary.]	X	X	X				X	X	X	X	X	Not Selected		CC6.1	
AU-6(7)	Audit Review, Analysis, and Reporting | Permitted Actions	Selection (one or more): information system process; role; user = [information system process; role]	X	X	Not allocated		X						X	Not Selected			
AU-7	Audit Reduction and Report Generation	Not applicable	X	X	X				X	X	X	X	X	X	IVS-01 SEF-04	CC6.1	None
AU-7(1)	Audit Reduction and Report Generation | Automatic Processing	Audit fields = [all audit fields specified in AU-3 and AU-3(1)]	X	X	X				X	X	X	X	X	X	IVS-01 SEF-04	CC6.1	
AU-7(2)	Audit Reduction and Report Generation | Automatic Sort and Search	Audit fields = [all audit fields specified in AU-3 and AU-3(1)]	X	X	Not allocated					X	X	X	X	Not Selected			
AU-8	Time Stamps	(B) Granularity = [1 second precision]	X	X	X				X	X	X	X	X	X	IVS-03	CC6.1	A.12.4.4
AU-8(1)	Time Stamps | Synchronization with Authoritative Time Source	(a) Frequency = [at least daily] (a) Authoritative time source= [http://www.nrc-cnrc.gc.ca/eng/services/time/network_time.html] (b) Time difference = [1 millisecond]	X	X	X				X	X	X		X	X	IVS-03	CC6.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-9	Protection of Audit Information	Not applicable	X	X	X				X	X	X	X	X	X	IAM-01 IVS-01 SEF-04	CC6.1	A.12.4.2 A.12.4.3 A.18.1.3
AU-9(2)	Protection of Audit Information | Audit Backup on Separate Physical Systems / Components	Frequency = [at least weekly]	X	X	X				X	X	X	X	X	X	IAM-01 SEF-04	CC6.1	
AU-9(4)	Protection of Audit Information | Access by Subset of Privileged Users	Subset of privileged users = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
AU-9(6)	Protection of Audit Information | Read-Only Access	Subset of privileged users = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
AU-11	Audit Record Retention	CSP: (A) Time period = [at least 90 days] GC: (A) Time period = [events and logs at least 3 months online and at least 6 months in storage; events and logs associated with a security incident for at least 2 years]	X	X	X	X	X						X	X	IAM-12 IVS-01 SEF-04	CC6.1	A.12.4.1 A.16.1.7
AU-12	Audit Generation	(A) Components = [all information system and network components where audit capability is deployed/available] (B) Personnel or roles = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	X	IVS-01	CC6.1	A.12.4.1 A.12.4.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-12(1)	Audit Generation | System-Wide / Time-Correlated Audit Trail	Components = [all information system components which have audit capability or where audit capability is feasible] Level of tolerance = [1 second between time stamps of individual records in the audit trail]	X	X	Not allocated				X	X	X	X	X	Not Selected		CC6.1	
AU-12(2)	Audit Generation | Standardized Formats	Not applicable	X	X	Not allocated					X	X	X	X	Not Selected			
CA-1	Security Assessment and Authorization Policies and Procedures	(A) Personnel or roles = [personnel or roles with security assessment responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AIS-02 AAC-02 AAC-03 CCC-01 CCC-05 GRM-03 GRM-06 GRM-08 GRM-09 GRM-11 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CA-2	Security Assessments	(B) Frequency = [at least annually] (D) Individuals or roles = To be defined as part of the tailoring process but to include [GC governance body]	X	X	X	X	X						X	X	AIS-02 AAC-01 AAC-02 DSI-06	CC4.1	A.14.2.8 A.18.2.2 A.18.2.3
CA-2(1)	Security Assessments | Independent Assessors	Level of independence = [an external independent organization]	X	Not allocated	X	X							Not Selected	X	AIS-02 AAC-01 AAC-02 DSI-06	CC4.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CA-2(2)	Security Assessments | Specialized Assessments	Frequency = [at least annually] Selection = [announced] Selection = [penetration testing and vulnerability scanning, which is to include credentialed tests and scans]	X	X	X	X	X						X	X		CC4.1	
CA-2(3)	Security Assessments | External Organizations	Information system = [CSP's information system within the scope of the cloud services provided, excluding tenant components] External organization = [an external independent organization] Requirements = [all applicable requirements]	X	Not allocated	X	X							Not Selected	X		CC4.1	
CA-3	System Interconnections	(C) Frequency = [annually]	X	X	X	X	X						X	X	GRM-02 STA-03 STA-05 STA-09	CC7.1	A.13.1.2 A.13.2.1 A.13.2.2
CA-3(3)	System Interconnections | Classified Non-National Security System Connections	Connection of = [any internal network or system] Boundary protection device = [GC-approved security controls]	X	X	X	X	X						X	X		CC7.1	
CA-5	Plan of Action and Milestones	(B) Frequency = [at least monthly]	X	X	X	X	X						X	X	AIS-02 GRM-03	CC4.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CA-6	Security Authorization	(C) Frequency = [at least every three years or when a significant change occurs]	X	X	X	X	X						X	X	AIS-02 AAC-02 CCC-05 GRM-03 GRM-11	CC7.4	None
CA-7	Continuous Monitoring	(A) Metrics = To be defined as part of the tailoring process but to include [GC-approved metrics] (B) Frequencies for monitoring = To be defined as part of the tailoring process but to include [GC-approved frequencies] (B) Frequencies for assessments = To be defined as part of the tailoring process but to include [GC-approved frequencies] (G) Personnel or roles = To be defined as part of the tailoring process but to include [GC governance body] (G) Frequency = To be defined as part of the tailoring process but to include [GC-approved frequencies]	X	X	X	X	X						X	X	AAC-01 CCC-05 GRM-03 GRM-11	CC4.1	None
CA-7(1)	Continuous Monitoring | Independent Assessment	Level of independence = [full independence from the organizational unit responsible for day to day security operations]	X	Not allocated	X	X							Not Selected	X		CC4.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CA-8	Penetration Testing	(A) Frequency = [at least annually] (A) Information systems or components = To be defined as part of the tailoring process	X	Not allocated	X	X							Not Selected	X		CC4.1	None
CA-8(1)	Penetration Testing | Independent Penetration Testing Agent for Team	Not applicable	X	Not allocated	X	X							Not Selected	X		CC4.1	
CA-9	Internal System Connections	(A) Components or classes of components = To be defined as part of the tailoring process	X	X	X	X	X						X	X		CC7.1	None
CA-9(1)	Internal System Connections | Security Compliance Checks	Not applicable	X	X	Not allocated		X						X	Not Selected			
CM-1	Configuration Management Policy and Procedures	(A) Personnel or roles = [personnel or roles with configuration management responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 CCC-01 CCC-03 CCC-04 GRM-05 GRM-06 GRM-08 GRM-09 GRM-11 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CM-2	Baseline Configuration	Not applicable	X	X	X	X	X						X	X	BCR-10 CCC-03 CCC-04 CCC-05 GRM-01	CC7.4	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-2(1)	Baseline Configuration | Reviews and Updates	(a) Frequency = [at least annually] (b) Circumstances = [significant changes as defined in NIST SP 800-37 rev1, Appendix F or when directed by the GC governance body]	X	X	X	X	X						X	X	BCR-10 CCC-03 CCC-04 CCC-05 GRM-01	CC7.2 CC7.3 CC7.4	
CM-2(2)	Baseline Configuration | Automation Support for Accuracy / Currency	Not applicable	X	X	X	X	X		X	X	X		X	X		CC7.4	
CM-2(3)	Baseline Configuration | Retention of Previous Configurations	Previous versions = [most recent previous version]	X	Not allocated	X	X							Not Selected	X	BCR-10 CCC-03 CCC-04 CCC-05 GRM-01	CC7.4	
CM-2(6)	Baseline Configuration | Development and Test Environments	Not applicable	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-3	Configuration Change Control	(E) Time period = [at least 90 days] (G) Configuration change control element = [Central communication process that include [GC governance body]] (G) Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions] = To be defined as part of the tailoring process (G) Frequency (if selected) = To be defined as part of the tailoring process (G) Configuration change conditions (if selected) = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-10 CCC-04 CCC-05 TVM-02	CC7.4	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4
CM-3(2)	Configuration Change Control | Test / Validate / Document Changes	Not applicable	X	X	Not allocated		X						X	Not Selected	BCR-10 CCC-04 CCC-05 TVM-02		
CM-3(3)	Configuration Change Control | Automated Change Implementation	Not applicable	X	X	Not allocated		X						X	Not Selected			
CM-3(4)	Configuration Change Control | Security Representative	Configuration change control element = To be defined as part of the tailoring process	X	X	X	X	X						X	Not Selected		CC7.1	
CM-3(6)	Configuration Change Control | Cryptography Management	Security safeguards = [any cryptographic-based safeguards]	X	X	X	X	X						X	Not Selected		CC7.4	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-4	Security Impact Analysis	Not applicable	X	X	X	X	X						X	X	BCR-10 TVM-02	CC7.1	A.14.2.3
CM-4(1)	Security Impact Analysis | Separate Test Environments	Not applicable	X	X	X	X	X						X	Not Selected		CC7.1 CC7.4	
CM-4(2)	Security Impact Analysis | Verification of Security Functions	Not applicable	X	X	Not allocated		X						X	Not Selected			
CM-5	Access Restrictions for Change	Not applicable	X	X	X	X	X						X	X	BCR-10 CCC-04 CCC-05 IAM-06	CC7.4	A.9.2.3 A.9.4.5 A.12.1.2 A.12.1.4 A.12.5.1
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement / Auditing	Not applicable	X	X	X				X	X	X		X	X	CCC-04 CCC-05 IAM-06	CC7.4	
CM-5(2)	Access Restrictions for Change | Review System Changes	Frequency = [at least every 12 months] Circumstances = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CM-5(5)	Access Restrictions for Change | Limit Production / Operational Privileges	(b) Frequency = [at least quarterly]	X	X	X	X	X						X	X	CCC-04 CCC-05 IAM-06	CC7.4	
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	Not applicable	X	X	X	X	X						X	Not Selected		CC7.4	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-6	Configuration Settings	(A) Checklists = [checklists from one or more of the following Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA)] (C) System components = [any information system component] (C) Operational requirements = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-10 CCC-05 IVS-12	CC5.1 CC7.4	None
CM-6(1)	Configuration Settings | Automated Central Management / Application / Verification	System components = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-10 CCC-05 IVS-12	CC7.4	
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes	Security safeguards = To be defined as part of the tailoring process Configuration settings = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CM-7	Least Functionality	(B) Assignment = To be defined as part of the tailoring process and that follows one or more standards from Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), or Defense Information Systems Agency (DISA)	X	X	X	X	X						X	X	CCC-04 IAM-03 IAM-13 IVS-06	CC5.1 CC7.1	A.12.5.1*
CM-7(1)	Least Functionality | Periodic Review	Frequency = [at least annually] Assignment = To be defined as part of the tailoring process	X	X	X	X	X						X	X	CCC-04 IAM-03 IAM-13 IVS-06	CC7.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-7(3)	Least Functionality | Registration Compliance	Registration requirements = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CM-7(5)	Least Functionality | Authorized Software / Whitelisting	(a) Software programs = [authorized software programs in baseline configuration and information system component inventory] (c) Frequency = [at least annually or when there is a change]	X	X	X	X	X						X	X		CC5.1	
CM-8	Information System Component Inventory	(D) Information = [unique asset identifier, NetBIOS name, baseline configuration name, OS Name, OS Version, system owner information] (E) Frequency = [at least monthly]	X	X	X	X	X						X	X	CCC-04 DCS-05	CC5.1	A.8.1.1 A.8.1.2
CM-8(1)	Information System Component Inventory | Updates During Installations / Removals	Not applicable	X	X	X	X	X						X	X	CCC-04 DCS-05	CC7.4	
CM-8(2)	Information System Component Inventory | Automated Maintenance	Not applicable	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-8(3)	Information System Component Inventory | Automated Unauthorized Component Detection	(a) Frequency = [continuously with a maximum 5-minute delay in detection] (b) Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles] = To be defined as part of the tailoring process (b) Personnel or roles (if selected) = To be defined as part of the tailoring process	X	X	X	X	X						X	X	CCC-04 DCS-05	CC6.1 CC6.2	
CM-8(4)	Information System Component Inventory | Accountability Information	Selection (one or more): name; position; role = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CM-8(5)	Information System Component Inventory | No Duplicate Accounting of Components	Not applicable	X	X	X	X	X						X	X	CCC-04 DCS-05	CC7.4	
CM-8(6)	Information System Component Inventory | Assessed Configurations / Approved Deviations	Not applicable	X	X	Not allocated		X						X	Not Selected			
CM-9	Configuration Management Plan	Not applicable	X	X	X	X	X						X	X	BCR-10 CCC-01 CCC-04 CCC-05	CC7.4	A.6.1.1*
CM-10	Software Usage Restrictions	Not applicable	X	X	X	X	X						X	X		CC3.1	A.18.1.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-11	User-Installed Software	(A) Policies = To be defined as part of the tailoring process (B) Methods = To be defined as part of the tailoring process (C) Frequency = [continuously (via CM-7(5))]	X	X	X	X	X						X	X		CC5.8	A.12.5.1 A.12.6.2
CM-11(1)	User-Installed Software | Alerts for Unauthorized Installations	Personnel, roles = To be defined as part of the tailoring process	X	X	Not allocated					X	X		X	Not Selected			
CM-11(2)	User-Installed Software | Prohibit Installation without Privileged Status	Not applicable	X	X	Not allocated					X	X		X	Not Selected			
CP-1	Contingency Planning Policy and Procedures	(A) Personnel or roles = [personnel or roles with contingency planning responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 BCR-01 BCR-09 GRM-08 GRM-09 IAM-07	CC3.1 CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CP-2	Contingency Plan	(A)(f) Personnel or roles = To be defined as part of the tailoring process (B) Key contingency personnel = To be defined as part of the tailoring process (D) Frequency = [at least annually] (F) Key contingency personnel = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-01 BCR-02 BCR-09 BCR-11	CC3.1 CC3.3	A.6.1.1 A.17.1.1 A.17.2.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CP-2(1)	Contingency Plan | Coordinate with Related Plans	Not applicable	X	X	X	X	X						X	X	BCR-01 BCR-02 BCR-11	CC3.1	
CP-2(2)	Contingency Plan | Capacity Planning	Not applicable	X	X	X	X	X						X	X	BCR-01 BCR-02 BCR-11	A1.1	
CP-2(3)	Contingency Plan | Resume Essential Missions / Business Functions	Time period = [within 24 hours]	X	X	X	X	X						X	X		CC3.1	
CP-2(4)	Contingency Plan | Resume All Missions / Business Functions	Time period = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CP-2(5)	Contingency Plan | Continue Essential Missions / Business Functions	Not applicable	X	X	Not allocated		X						X	Not Selected			
CP-2(6)	Contingency Plan | Alternate Processing / Storage Site	Not applicable	X	X	Not allocated		X						X	Not Selected			
CP-2(8)	Contingency Plan | Identify Critical Assets	Not applicable	X	X	X	X	X						X	X		CC3.1	
CP-3	Contingency Training	(A) Time period = [10 days] (C) Frequency = [at least annually]	X	X	X	X	X						X	X	BCR-01 BCR-02	CC1.3	A.7.2.2*
CP-3(1)	Contingency Training | Simulated Events	Not applicable	X	X	Not allocated		X						X	Not Selected			
CP-4	Contingency Plan Testing	(A) Frequency = [at least annually] (A) Tests = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-01 BCR-02	A1.3	A.17.1.3
CP-4(1)	Contingency Plan Testing | Coordinate with Related Plans	Not applicable	X	X	X	X	X						X	X	BCR-01 BCR-02	A1.3	
CP-4(2)	Contingency Plan Testing | Alternate Processing Site	Not applicable	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CP-6	Alternate Storage Site	Not applicable	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	A.11.1.4 A.17.1.2 A.17.2.1
CP-6(1)	Alternate Storage Site | Separation from Primary Site	Not applicable	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	
CP-6(2)	Alternate Storage Site | Recovery Times / Point Objectives	Not applicable	X	X	Not allocated								X	Not Selected			
CP-6(3)	Alternate Storage Site | Accessibility	Not applicable	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	
CP-7	Alternative Processing Site	(A) Information system operations = To be defined as part of the tailoring process (A) System operations = To be defined as part of the tailoring process (A) RTO/RPO = To be defined as part of the tailoring process but to include [the recovery time and recovery point objectives specified in the service agreement with the GC]	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	A.11.1.4 A.17.1.2 A.17.2.1
CP-7(1)	Alternative Processing Site | Separation from Primary Site	Not applicable	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	
CP-7(2)	Alternative Processing Site | Accessibility	Not applicable	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CP-7(3)	Alternative Processing Site | Priority of Service	Not applicable	X	X	X	X							X	X	BCR-01 BCR-11 STA-03	A1.2	
CP-7(4)	Alternative Processing Site | Preparation for Use	Not applicable	X	X	Not allocated								X	Not Selected			
CP-7(6)	Alternative Processing Site | Inability to Return to Primary Site	Not applicable	X	X	Not allocated								X	Not Selected			
CP-8	Telecommunications Services	(A) System operations = [all information system operations covered by the contingency plan (CP-2)] (A) Time period = [the recovery time objectives specified in the service agreement]	X	X	X	X							X	X	BCR-01 BCR-08 BCR-11 STA-03	A1.2	A.11.2.2 A.17.1.2
CP-8(1)	Telecommunications Services | Priority of Service Provisions	Not applicable	X	X	X	X							X	X	BCR-01 BCR-08 BCR-11 STA-03	A1.2	
CP-8(2)	Telecommunications Services | Single Points of Failure	Not applicable	X	X	X	X							X	X	BCR-01 BCR-08 BCR-11 STA-03	A1.2	
CP-8(3)	Telecommunications Services | Separation of Primary / Alternate Providers	Not applicable	X	X	Not allocated								X	Not Selected			
CP-8(5)	Telecommunications Services | Alternate Telecommunication Service Testing	Frequency = [at least annually]	X	X	Not allocated								X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CP-9	Information System Backup	(A) Frequency = [daily incremental; weekly full] (B) Frequency = [daily incremental; weekly full] (C) Frequency = [daily incremental; weekly full]	X	X	X	X							X	X	BCR-01 BCR-04 BCR-11	A1.2 CC5.6	A.12.3.1 A.17.1.2 A.18.1.3
CP-9(1)	Information System Backup | Testing for Reliability / Integrity	Frequency = [at least annually]	X	X	X	X							X	X	BCR-01 BCR-04 BCR-11	A1.3	
CP-9(2)	Information System Backup | Test Restoration using Sampling	Not applicable	X	X	Not allocated		X						X	Not Selected			
CP-9(3)	Information System Backup | Separate Storage for Critical Information	Critical system software and other security-related information = [all operating system and critical software code]	X	X	X	X							X	X	BCR-01 BCR-04 BCR-11	A1.2	
CP-9(5)	Information System Backup | Transfer to Alternate Storage Site	Time period and transfer rate = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			
CP-9(7)	Information System Backup | Dual Authorization	Backup information = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CP-10	Information System Recovery and Reconstitution	Not applicable	X	X	X	X							X	X	BCR-01 BCR-04	CC3.1	A.17.1.2
CP-10(2)	Information System Recovery and Reconstitution | Transaction Recovery	Not applicable	X	X	X					X	X		X	X	BCR-01 BCR-04	A1.2	
CP-10(4)	Information System Recovery and Reconstitution | Restore within Time Period	Time periods = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
CP-10(6)	Information System Recovery and Reconstitution | Component Protection	Not applicable	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CP-11	Alternate Communications Protocols	(A) Alternative communications protocols = To be defined as part of the tailoring process	X	X	Not allocated					X			X	Not Selected			A.17.1.2*
CP-13	Alternative Security Mechanisms	(A) Alternative or supplemental security mechanisms = To be defined as part of the tailoring process (A) Security functions = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			A.17.1.2*
IA-1	Identification and Authentication Policy and Procedures	(A) Personnel or roles = [personnel or roles with identification and authentication responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 GRM-06 GRM-08 GRM-09 IAM-02 IAM-07 IAM-12	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
IA-2	Identification and Authentication (Organizational Users)	Not applicable	X	X	X				X	X	X	X	X	X	IAM-09 IAM-12	CC5.3	A.9.2.1
IA-2(1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	Not applicable	X	X	X				X	X	X	X	Not Selected	X	IAM-09 IAM-12	CC5.3	
IA-2(3)	Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts	Not applicable	X	X	X				X	X	X	X	Not Selected	X	IAM-09 IAM-12	CC5.3	
IA-2(6)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Separate Device	Strength of mechanism requirements = [the requirements in CSE's ITSP.30.031]	X	X	X				X	X	X	X	Not Selected				
IA-2(8)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant	Not applicable	X	X	X				X	X	X	X	X	X	IAM-09 IAM-12	CC5.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IA-2(9)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant	Not applicable	X	X	X				X	X	X	X	X	Not Selected		CC5.3	
IA-2(10)	Identification and Authentication (Organizational Users) | Single Sign-On	List of accounts and services = To be defined as part of the tailoring process	X	X	Not allocated					X	X		X	Not Selected			
IA-2(11)	Identification and Authentication (Organizational Users) | Remote Access - Separate Device	Strength of mechanism requirements = [the requirements in CSE's ITSP.30.031]	X	X	X				X	X	X	X	X	X		CC5.3	
IA-3	Device Identification and Authentication	(A) Specific and/or types of devices = To be defined as part of the tailoring process (A) Selection (one or more): local; remote; network = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	X	DCS-03	CC5.1	None
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	Devices and/or types of devices = [portable devices] Selection (one or more): local; remote; network = [network]	X	X	X				X	X	X	X	X	Not Selected		CC5.1	
IA-3(3)	Device Identification and Authentication | Dynamic Address Allocation	(a) Duration = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
IA-4	Identifier Management	(A) Personnel or roles = To be defined as part of the tailoring process (D) Time period = [at least two years] (E) Time period = [90 days for user identifiers]	X	X	X	X	X						X	X	DCS-03 IAM-07 IAM-09	CC5.1 CC5.2	A.9.2.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IA-4(1)	Identifier Management | Prohibit Account Identifiers as Public Identifiers	Not applicable	X	X	Not allocated		X						X	Not Selected			
IA-4(2)	Identifier Management | Supervisor Authorization	Not applicable	X	X	Not allocated		X						X	Not Selected			
IA-4(3)	Identifier Management | Multiple Forms of Certification	Not applicable	X	X	Not allocated		X						X	Not Selected			
IA-4(4)	Identifier Management | Identify User Status	Characteristic identifying individual status = [employee, contractor, foreign nationals]	X	X	X	X	X						X	X	DCS-03 IAM-09	CC5.2	
IA-4(7)	Identifier Management | In Person Registration	Not applicable	X	X	Not allocated		X						X	Not Selected			
IA-5	Authenticator Management	(G) Time period = [at least every 180 days]	X	X	X	X	X						X	X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1 CC5.2 CC5.3	A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.3
IA-5(1)	Authenticator Management | Password-Based Authentication	*If IA-2(3) is selected, then the following parameters apply:* (a) Password requirements = [case sensitive, minimum of eight characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters] (b) Number of change characters = [at least one] (d) Lifetime restrictions = [one day minimum, sixty day maximum] (e) Password re-use = [24 generations] *If IA-2(3) is NOT selected, then the following parameters apply:*	X	X	X				X	X	X	X	X	X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1 CC5.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
		(a) Password requirements = [case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters] (b) Number of change characters = [at least one] (d) Lifetime restrictions = [one day minimum, sixty day maximum (e) Password re-use = [24 generations]															
IA-5(2)	Authenticator Management | PKI-Based Authentication	Not applicable	X	X	X				X	X	X	X	X	X	GRM-09 IAM-07 IAM-07 IAM-09 IAM-12	CC5.1 CC5.3	
IA-5(3)	Authenticator Management | In-Person or Trusted Third-Party Registration	Types of and/or specific authenticators = [a hardware/biometric multi-factor authenticator] Selection: in person; by a trusted third party = [in person] Registration authority = To be defined as part of the tailoring process Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.2	
IA-5(4)	Authenticator Management | Automated Support for Password Strength Determination	Requirements = [password length, complexity, rotation and lifetime restrictions established by IA-5(1)]	X	Not allocated	X	X							Not Selected	X		CC6.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IA-5(6)	Authenticator Management | Protection of Authenticators	Not applicable	X	X	X	X	X						X	X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1	
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	Not applicable	X	X	X	X	X						X	X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1 CC7.1	
IA-5(8)	Authenticator Management | Multiple Information System Accounts	Security safeguards = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
IA-5(9)	Authenticator Management | Cross-Organizational Credential Management	External organizations = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
IA-5(11)	Authenticator Management | Hardware Token-Based Authentication	Token quality requirements = [As per CSE User Authentication Guidance for IT Systems (ITSP.30.031 V2), or subsequent versions]	X	X	X				X	X	X	X	Not Selected	X		CC5.3	
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	Time period = To be defined as part of the tailoring process	X	X	Not allocated				X	X	X	X	X	Not Selected		CC5.3	
IA-5(14)	Authenticator Management | Managing Content of PKI Trust Stores	Not applicable	X	X	Not allocated		X						X	Not Selected			
IA-6	Authenticator Feedback	Not applicable	X	X	X				X	X	X	X	X	X	IAM-12	CC5.3	A.9.4.2
IA-7	Cryptographic Module Authentication	Not applicable	X	X	X				X	X	X		X	X	AAC-03 EKM-03	CC5.1	A.18.1.5
IA-8	Identification and Authentication (Non-Organizational Users)	Not applicable	X	X	X				X	X	X	X	X	X	IAM-07 IAM-09 IAM-12	CC5.3	A.9.2.1
IA-8(100)	Identification and Authentication (Non-Organizational Users) | Identity and Credential Assurance Levels	Not applicable	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IR-1	Incident Response Policy and Procedures	(A) Personnel or roles = [personnel or roles with incident management responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 GRM-06 GRM-08 GRM-09 IAM-07 SEF-02	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
IR-2	Incident Response Training	(A) Time period = [within 30 days] (C) Frequency = [at least annually]	X	X	X	X	X						X	X	SEF-02 SEF-03	CC1.3	A.7.2.2*
IR-2(1)	Incident Response Training | Simulated Events	Not applicable	X	X	Not allocated		X						X	Not Selected			
IR-3	Incident Response Testing	(A) Frequency = [at least annually] (A) Tests = [tests and exercises defined in NIST SP 800-61 or GC equivalent]	X	X	X	X	X						X	X	SEF-02	CC6.2	None
IR-3(2)	Incident Response Testing | Coordination with Related Plans	Not applicable	X	X	X	X	X						X	X		CC6.2	
IR-4	Incident Handling	Not applicable	X	X	X	X	X						X	X	SEF-02 SEF-05	CC6.2	A.16.1.4 A.16.1.5 A.16.1.6
IR-4(3)	Incident Handling | Continuity of Operations	Classes of incidents = To be defined as part of the tailoring process Actions = To be defined as part of the tailoring process	X	X	X	X	X						X	Not Selected		CC6.2	
IR-4(4)	Incident Handling | Information Correlation	Not applicable	X	X	X	X	X						X	Not Selected		CC6.2	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IR-4(8)	Incident Handling | Correlation with External Organizations	External organizations = [At a minimum, the CSP must coordinate with GC Computer Incident Response Team (GC CIRT), in alignment with GC Cyber Event Management Plan (https://www.tbs-sct.gc.ca/hgw-cgf/oversight-surveillance/atip-aiprp/sim-gsi/msi-gis/csemp-pgec-eng.asp)] Incident information = [as required by GC CIRT]	X	X	X	X	X						X	Not Selected		CC6.2	
IR-4(9)	Incident Handling | Dynamic Response Capability	Dynamic response capabilities = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
IR-5	Incident Monitoring	Not applicable	X	X	X	X	X						X	X	SEF-02 SEF-04 SEF-05	CC6.2	None
IR-6	Incident Reporting	(A) Time period = [the time periods specified in the GC CSEMP] (B) Authorities = [organizations specified in the GC CSEMP]	X	X	X	X	X						X	X	SEF-01 SEF-03	CC6.1	A.6.1.3 A.16.1.2
IR-6(1)	Incident Reporting | Automated Reporting	Not applicable	X	Not allocated	X	X							Not Selected	X	SEF-01 SEF-03	CC6.2	
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents	Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	Not Selected		CC6.2	
IR-7	Incident Response Assistance	Not applicable	X	X	X	X	X						X	X	SEF-02 SEF-03 SEF-04	CC6.1	None
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information / Support	Not applicable	X	Not allocated	X	X							Not Selected	X	SEF-02 SEF-03 SEF-04	CC6.2	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IR-7(2)	Incident Response Assistance | Coordination with External Providers	Not applicable	X	Not allocated	X	X							Not Selected	X	SEF-02 SEF-03 SEF-04	CC6.2	
IR-8	Incident Response Plan	(A)(h) Personnel or roles = To be defined as part of the tailoring process (B) Assignment = To be defined as part of the tailoring process (C) Frequency = [at least annually] (E) Assignment = To be defined as part of the tailoring process	X	X	X	X	X						X	X	SEF-02 SEF-04 SEF-05	CC6.2	A.16.1.1
IR-9	Information Spillage Response	(B) Personnel or roles = [Incident Response personnel as documented within the Incident Management Plan] (F) Actions = [actions documented within the Incident Management Plan]	X	X	X	X	X						X	X		CC6.2	None
IR-9(1)	Information Spillage Response | Responsible Personnel	Personnel or roles = Personnel or roles = [Incident Response personnel as documented within the Incident Management Plan]	X	X	X	X	X						X	X		CC6.2	
IR-9(2)	Information Spillage Response | Training	Frequency = [in accordance with the frequency specified under AT-3]	X	X	X	X	X						X	X		CC1.3	
IR-9(3)	Information Spillage Response | Post-Spill Operations	Procedures = To be defined as part of the tailoring process	X	X	X	X	X						X	X		A1.2	
IR-9(4)	Information Spillage Response | Exposure to Unauthorized Personnel	Security safeguards = To be defined as part of the tailoring process	X	X	X	X	X						X	X		CC2.3	
IR-10	Integrated Information Security Analysis Team	Not applicable	X	X	Not allocated		X						X	Not Selected			None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
MA-1	System Maintenance Policy and Procedures	(A) Personnel or roles = [personnel or roles with system maintenance responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 DCS-04 DCS-08 GRM-06 GRM-08 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
MA-2	Controlled Maintenance	(C) Personnel or roles = To be defined as part of the tailoring process (F) Maintenance-related information = [date and time of maintenance, name of the individual performing the maintenance; name of escort (if applicable), description of the maintenance performed; equipment removed or replaced (including identification numbers, if applicable)]	X	X	X	X	X						X	X	BCR-07 DCS-08	CC5.6 CC7.1	A.11.2.4* A.11.2.5*
MA-3	Maintenance Tools	Not applicable	X	X	X	X	X						X	X	BCR-07 IAM-03	CC7.1	None
MA-3(1)	Maintenance Tools | Inspect Tools	Not applicable	X	Not allocated	X	X							Not Selected	X	BCR-07 IAM-03	CC5.6	
MA-3(2)	Maintenance Tools | Inspect Media	Not applicable	X	X	X	X	X						X	X	BCR-07 IAM-03	CC5.8	
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	(d) Personnel or roles = [the information owner]	X	Not allocated	X	X							Not Selected	X	BCR-07 IAM-03	CC5.6	
MA-4	Nonlocal Maintenance	Not applicable	X	X	X	X	X						X	X	BCR-07 BCR-10 IAM-03	CC5.1 CC5.3 CC6.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
MA-4(1)	Nonlocal Maintenance | Auditing and Review	(a) Audit events = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected	BCR-07 BCR-10 IAM-03		
MA-4(2)	Nonlocal Maintenance | Document Nonlocal Maintenance	Not applicable	X	X	X	X	X						X	X	BCR-07 BCR-10 IAM-03	CC7.4	
MA-4(3)	Nonlocal Maintenance | Comparable Security / Sanitization	Not applicable	X	X	Not allocated		X						X	Not Selected		CC7.4	
MA-4(4)	Nonlocal Maintenance | Authentication / Separation of Maintenance Sessions	(a) Authenticators = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
MA-4(5)	Nonlocal Maintenance | Approvals and Notifications	(a) Personnel or roles = To be defined as part of the tailoring process (b) Personnel or roles = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
MA-4(6)	Nonlocal Maintenance | Cryptographic Protection	Not applicable	X	X	X				X	X	X		X	Not Selected		CC7.4	
MA-5	Maintenance Personnel	Not applicable	X	X	X	X	X						X	X	BCR-07 IAM-03 IAM-09	CC1.4 CC5.6	None
MA-5(1)	Maintenance Personnel | Individuals without Appropriate Access	Not applicable	X	X	X	X	X						X	X		CC7.4	
MA-5(5)	Maintenance Personnel | Non System-Related Maintenance	Not applicable	X	X	Not allocated								X	Not Selected			
MA-6	Timely Maintenance	(A) System components = [all system components requiring vendor support and/or spare parts] (A) Time period = [as needed to support availability commitments]	X	X	X	X	X						X	X	BCR-07	A1.2	A.11.2.4

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
MP-1	Media Protection Policy and Procedures	(A) Personnel or roles = [personnel or roles with media protection responsibilities] (B)(a) Frequency = [at least annually] (B)(b) Frequency = [at least annually]	X	X	X	X							X	X	AAC-03 DSI-04 GRM-06 GRM-08 GRM-09 HRS-11 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
MP-2	Media Access	(A) Types of media = [IT media (digital and non-digital)] (A) Personnel or roles = [authorized administrators]	X	X	X	X							X	X	HRS-05 HRS-11	CC5.5	A.8.2.3 A.8.3.1 A.11.2.9
MP-3	Media Marking	(B) Types of system media = [no removable media types] (B) Controlled areas = [controlled areas that meet the requirements of the GC Industrial Security Program]	X	X	X	X							X	X	DSI-04 HRS-11	CC5.7	A.8.2.2
MP-4	Media Storage	(A) Types of media = [all types of digital and non-digital media with sensitive information] (A) Controlled areas = [controlled areas that meet the requirements of the GC Industrial Security Program]	X	X	X	X							X	X	HRS-05 HRS-11	CC5.5	A.8.2.3 A.8.3.1 A.11.2.9
MP-5	Media Transport	(A) Types of media = [all media with sensitive information] (A) Security safeguards = To be defined as part of the tailoring process	X	X	X	X							X	X	SEF-04 STA-05	CC5.7	A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.5 A.11.2.6

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
MP-5(4)	Media Transport | Cryptographic Protection	Not applicable	X	X	X	X							X	X	SEF-04 STA-05	CC5.7	
MP-6	Media Sanitization	(A) System media = To be defined as part of the tailoring process (A) Sanitization = To be defined as part of the tailoring process	X	X	X	X							X	X	DSI-07 HRS-05	CC5.5	A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7
MP-6(1)	Media Sanitization | Review / Approve / Track / Document / Verify	Not applicable	X	X	X								X	Not Selected			
MP-6(2)	Media Sanitization | Equipment Testing	Frequency = [at least annually]	X	X	X	X							X	X		CC5.5	
MP-6(3)	Media Sanitization | Non-destructive Techniques	Circumstances = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			
MP-6(8)	Media Sanitization | Remote Purging / Wiping of Information	Information systems, components, or devices = To be defined as part of the tailoring process Conditions = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			
MP-8	Media Downgrading	(A) Downgrading process = To be defined as part of the tailoring process (A) Strength and integrity = To be defined as part of the tailoring process (C) System media = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			None
MP-8(1)	Media Downgrading | Documentation of Process	Not applicable	X	X	Not allocated								X	Not Selected			
MP-8(3)	Media Downgrading | Controlled Unclassified Information	Protected information = [Protected A and Protected B information]	X	X	Not allocated								X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-1	Physical and Environmental Protection Policy and Procedures	(A) Personnel or roles = [personnel or roles with physical and environmental protection responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X							X	X	AAC-03 BCR-03 BCR-05 BCR-06 BCR-08 DSI-07 DCS-04 GRM-06 GRM-08 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PE-2	Physical Access Authorizations	(C) Frequency = [monthly]	X	X	X	X							X	X	DCS-02 DCS-06 DCS-09 IVS-01	CC5.5	A.11.1.2*
PE-2(1)	Physical Access Authorizations | Access by Position / Role	Not applicable	X	X	X								X	Not Selected			
PE-2(100)	Physical Access Authorizations | Identification Card	Not applicable	X	X	Not allocated								X	Not Selected			
PE-3	Physical Access Control	(A) Entry/exit points = [all physical access points to the facility] (A)(b) Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards] = [controlled areas that meet the requirements of the GC Industrial Security Program] (A)(b) Physical access control systems/devices (if selected) = To be	X	X	X			X					X	X	DCS-02 DCS-06 DCS-09 IVS-01	CC5.5	A.11.1.1 A.11.1.2 A.11.1.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
		defined as part of the tailoring process (B) Entry/exit points = [all physical access points to the facility] (C) Security safeguards = To be defined as part of the tailoring process (D) Circumstances for escorts and monitoring = [at all times while in the data center] (F) Physical access devices = To be defined as part of the tailoring process (F) Frequency = [annually] (G) Frequency = [only when keys are lost, combinations are compromised or individuals are transferred or terminated]															
PE-3(1)	Physical Access Control | Information System Access	Physical spaces = To be defined as part of the tailoring process	X	X	X			X					X	Not Selected		CC5.5	
PE-3(3)	Physical Access Control | Continuous Guards / Alarms / Monitoring	Not applicable	X	X	X								X	Not Selected			
PE-3(4)	Physical Access Control | Lockable Casings	System components = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-4	Access Control for Transmission Medium	(A) Lines = [all distribution and transmission lines] (A) Security safeguards = [in accordance with, or uses an adequate risk-based approach aligned with the practices with TBS and RCMP physical security standards]	X	X	X			X					X	X	BCR-03 DCS-06 IVS-12	CC5.5	A.11.1.2 A.11.2.3
PE-5	Access Control for Output Devices	Not applicable	X	X	X			X					X	X	BCR-06 DCS-06	CC5.5	A.11.1.2 A.11.1.3
PE-6	Monitoring Physical Access	(B) Frequency = [at least monthly] (B) Events = To be defined as part of the tailoring process	X	X	X			X					X	X	DCS-02 DCS-06 DCS-09	CC5.5	None
PE-6(1)	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment	Not applicable	X	X	X			X					X	X	DCS-02 DCS-06 DCS-09	CC5.5	
PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Information Systems	Physical spaces = [identified under PE-3(1)]	X	X	X								X	Not Selected			
PE-8	Visitor Access Records	(A) Time period = [a minimum of 1 year] (B) Frequency = [at least monthly]	X	X	X			X					X	X	DCS-02	CC5.5	None
PE-9	Power Equipment and Cabling	Not applicable	X	X	X			X					X	X	BCR-08	A1.2	A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3
PE-10	Emergency Shutoff	(B) Location by system or components = To be defined as part of the tailoring process	X	X	X			X					X	X	BCR-08	A1.2	A.11.2.2*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-11	Emergency Power	(A) Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power = [transition of the information system to long-term alternate power]	X	X	X			X					X	X	BCR-08	A1.2	A.11.2.2*
PE-12	Emergency Lighting	Not applicable	X	X	X			X					X	X	BCR-08	A1.2	A.11.2.2*
PE-12(1)	Emergency Lighting | Essential Missions / Business Functions	Not applicable	X	X	Not allocated								X	Not Selected			
PE-13	Fire Protection	Not applicable	X	X	X			X					X	X	BCR-03 BCR-05 BCR-08	A1.2	A.11.1.4 A.11.2.1
PE-13(1)	Fire Protection | Detection Devices / Systems	Personnel or roles = To be defined as part of the tailoring process Emergency responders = [local fire department]	X	X	Not allocated								X	Not Selected	BCR-03 BCR-05 BCR-08		
PE-13(2)	Fire Protection | Suppression Devices / Systems	Personnel or roles = To be defined as part of the tailoring process Emergency responders = [local fire department]	X	X	X			X					X	X	BCR-03 BCR-05 BCR-08	A1.2	
PE-13(3)	Fire Protection | Automatic Fire Suppression	Not applicable	X	X	X			X					X	X	BCR-03 BCR-05 BCR-08	A1.2	
PE-13(4)	Fire Protection | Inspections	Frequency = To be defined as part of the tailoring process Time period = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-14	Temperature and Humidity Controls	(A) Acceptable levels = To be defined as part of the tailoring process (B) Frequency = [continuously]	X	X	X	X							X	X	BCR-05 BCR-06 BCR-08	A1.2	A.11.1.4 A.11.2.1 A.11.2.2
PE-14(1)	Temperature and Humidity Controls | Automatic Controls	Not applicable	X	X	X								X	Not Selected			
PE-14(2)	Temperature and Humidity Controls | Monitoring with Alarms / Notifications	Not applicable	X	X	X			X					X	X		A1.2	
PE-15	Water Damage Protection	Not applicable	X	X	X			X					X	X	BCR-05 BCR-06	A1.2	A.11.1.4 A.11.2.1 A.11.2.2
PE-16	Delivery and Removal	(A) Types of system components = [all information system components]	X	X	X			X					X	X	DSI-04 DCS-04 DCS-07 DCS-08	CC5.5	A.8.2.3 A.11.1.6 A.11.2.5
PE-17	Alternate Work Site	(A) Security controls = [security controls commensurate with that of the primary site]	X	X	X	X							X	X	BCR-01 DCS-04	CC5.5 CC6.1	A.6.2.2 A.11.2.6 A.13.2.1
PE-18	Location of Information System Components	(A) Physical and environmental hazards = [physical and environmental hazards as specified in TBS and RCMP physical security standards and in accordance with the requirements under the GC Industrial Security Program]	X	X	X			X					X	Not Selected	BCR-05 BCR-06 DCS-02 DCS-07 DCS-09		A.8.2.3 A.11.1.4 A.11.2.1
PE-18(1)	Location of Information System Components | Facility Site	Not applicable	X	X	X	X							X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PL-1	Security Planning Policy and Procedures	(A) Personnel or roles = [personnel or roles with security planning responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 CCC-01 GRM-06 GRM-08 GRM-09 GRM-11 IAM-07	CC3.1 CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PL-2	System Security Plan	(B) Personnel or roles = To be defined as part of the tailoring process (C) Frequency = [at least annually]	X	X	X	X	X						X	X	CCC-01 CCC-05	CC3.1 CC3.3	A.14.1.1
PL-2(3)	System Security Plan | Plan / Coordinate with Other Organizational Entities	Individuals or groups = To be defined as part of the tailoring process	X	X	X	X	X						X	X		CC3.1	
PL-4	Rules of Behavior	(C) Frequency = [at least every 3 years]	X	X	X	X	X						X	X	GRM-07 HRS-06 HRS-07 HRS-08 HRS-10	CC2.3	A.7.1.2 A.7.2.1 A.8.1.3
PL-4(1)	Rules of Behavior | Social Media and Networking Restrictions	Not applicable	X	X	X	X	X						X	X		CC2.3	
PL-7	Security Concept of Operations	(B) Frequency = [at least annually]	X	X	Not allocated		X						X	Not Selected			A.14.1.1*
PL-8	Information System Architecture	(B) Frequency = [at least annually]	X	X	X	X	X						X	X		CC3.2	A.14.1.1*
PL-8(1)	Information System Architecture | Defense-In-Depth	(a) Security safeguards = To be defined as part of the tailoring process (a) Locations and architectural layers = To be defined as part of the tailoring process	X	X	X	X	X						X	Not Selected		CC5.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PL-8(2)	Information System Architecture | Supplier Diversity	Security safeguards = To be defined as part of the tailoring process Locations and architectural layers = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
PS-1	Personnel Security Policy and Procedures	(A) Personnel or roles = [personnel or roles with personnel security responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 GRM-06 GRM-07 GRM-08 GRM-09 HRS-03 HRS-07 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PS-2	Position Risk Designation	(C) Frequency = [at least every three years]	X	X	X	X	X						X	X	DSI-06 HRS-02 HRS-03 HRS-04 HRS-07	CC1.4	None
PS-3	Personnel Screening	(B) Conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening = [the TBS Standard on Security Screening and any related provisions of the Industrial Security Program]	X	X	X	X	X						X	X	HRS-02	CC1.4	A.7.1.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PS-4	Personnel Termination	(A) Time period = [same day] (C) Information security topics = To be defined as part of the tailoring process in accordance with the TBS Standard on Security Screening and any related provisions of the Industrial Security Program (F) Personnel or roles = [terminated personnel's manager] (F) Time period = [24 hours]	X	X	X	X	X						X	X	HRS-01 HRS-04 IAM-11	A1.2 CC5.2 CC5.4 CC5.6	A.7.3.1 A.8.1.4
PS-5	Personnel Transfer	(B) Transfer or reassignment actions = [reassignment of access to data] (B) Time period = [within 5 days of the formal transfer action] (D) Personnel or roles = [transferring personnel's manager] (D) Time period = [5 days]	X	X	X	X	X						X	X	HRS-04 IAM-11	CC5.4 CC5.5	A.7.3.1 A.8.1.4
PS-6	Access Agreements	(B) Frequency = [at least annually] (C)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	HRS-03 HRS-04 HRS-06 HRS-07 IAM-09 IAM-10	CC1.4	A.7.1.2 A.7.2.1 A.13.2.4

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PS-7	Third-Party Personnel Security	(D) Personnel or roles = To be defined as part of the tailoring process (D) Time period = [the same day]	X	X	X	X	X						X	X	HRS-03 HRS-07 IAM-10 STA-05	CC1.2 CC1.4 CC4.1 CC5.5	A.6.1.1* A.7.2.1*
PS-8	Personnel Sanctions	(B) Personnel or roles = To be defined as part of the tailoring process (B) Time period = To be defined as part of the tailoring process	X	X	X	X	X						X	X	GRM-07 HRS-04	CC1.1	A.7.2.3
RA-1	Risk Assessment Policy and Procedures	(A) Personnel or roles = [personnel or roles with risk assessment responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 GRM-08 GRM-09 GRM-10 GRM-11 IAM-07	CC3.1	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
RA-2	Security Categorization	Not applicable	X	X	X	X	X						X	X	AAC-03 DSI-01 DSI-06 DCS-01 GRM-02 GRM-10 GRM-11	CC3.1	A.8.2.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
RA-3	Risk Assessment	(B) Document = [security assessment report] (C) Frequency = [at least every 3 years or when a significant change occurs] (D) Personnel or roles = [personnel or roles with risk assessment responsibilities] (E) Frequency = [at least every 3 years or when a significant change occurs]	X	X	X	X	X						X	X	BCR-09 GRM-02 GRM-08 GRM-10 GRM-11	CC3.1	A.12.6.1*
RA-5	Vulnerability Scanning	(A) Frequency = [monthly for operating systems/infrastructure, web applications, and database management systems] (D) Response times = [within 30 days for high-risk vulnerabilities and 90 days for moderate-risk vulnerabilities from the date of discovery] (E) Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	X	AAC-02 TVM-02	CC4.1	A.12.6.1*
RA-5(1)	Vulnerability Scanning | Update Tool Capability	Not applicable	X	X	X	X	X						X	X	AAC-02 TVM-02	CC4.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
RA-5(2)	Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified	Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported = [prior to a new scan] Frequency (if selected) = Not selected	X	X	X	X	X						X	X	AAC-02 TVM-02	CC4.1	
RA-5(3)	Vulnerability Scanning | Breadth / Depth of Coverage	Not applicable	X	Not allocated	X	X							Not Selected	X	AAC-02 TVM-02	CC4.1	
RA-5(5)	Vulnerability Scanning | Privileged Access	Information system components = [operating systems, web applications, databases] Vulnerability scanning activities = [all scans]	X	Not allocated	X				X	X	X		Not Selected	X		CC4.1	
RA-5(6)	Vulnerability Scanning | Automated Trend Analyses	Not applicable	X	Not allocated	X	X							Not Selected	X	AAC-02 TVM-02	CC4.1	
RA-5(8)	Vulnerability Scanning | Review Historic Audit Logs	Not applicable	X	Not allocated	X	X							Not Selected	X		CC4.1	
SA-1	System and Services Acquisition Policy and Procedures	(A) Personnel or roles = [personnel or roles with system and services acquisition responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 CCC-01 GRM-06 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SA-2	Allocation of Resources	Not applicable	X	X	X	X	X						X	X	DSI-06 GRM-01	CC1.3 CC3.3	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-3	System Development Lifecycle	(A) SDLC = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-10 CCC-01 CCC-03	CC7.1 CC7.4	A.6.1.1 A.6.1.5 A.14.1.1 A.14.2.1 A.14.2.6
SA-4	Acquisition Process	***NOTE: Items (AA) and (BB) are not applicable to CSPs.***	X	X	X	X	X						X	X	BCR-10 CCC-01 CCC-02 CCC-03 GRM-01 IVS-04	CC7.1	A.14.1.1 A.14.2.7 A.14.2.9 A.15.1.2
SA-4(1)	Acquisition Process | Functional Properties of Security Controls	Not applicable	X	X	X	X	X						X	X	BCR-10 CCC-01 CCC-02 CCC-03 GRM-01 IVS-04	CC7.1	
SA-4(2)	Acquisition Process | Design / Implementation Information for Security Controls	Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information] = [security-relevant external system interfaces and high-level design] Design/implementation information (if selected) = Not selected Level of detail = To be defined as part of the tailoring process	X	Not allocated	X	X							Not Selected	X		CC7.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-4(5)	Acquisition Process | System / Component / Service Configurations	(b) Security configurations = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-4(8)	Acquisition Process | Continuous Monitoring Plan	Level of detail = [at least the minimum requirement as defined in CA-7]	X	Not allocated	X	X							Not Selected	X		CC7.1	
SA-4(9)	Acquisition Process | Functions / Ports / Protocols / Services in Use	Not applicable	X	Not allocated	X	X							Not Selected	X		CC7.1	
SA-5	Information System Documentation	(C) Actions = To be defined as part of the tailoring process (E) Personnel or roles = [developer or tester roles]	X	X	X	X	X						X	X	BCR-04 BCR-10 CCC-02 CCC-03	CC1.3 CC5.1 CC7.1	A.12.1.1*
SA-8	Security Engineering Principles	Not applicable	X	X	X	X	X						X	X	AIS-01 BCR-10 CCC-02 CCC-03	CC7.1	A.14.2.5
SA-9	External Information System Services	(A) Security controls = [applicable security controls if GC data is processed or stored within the external system] (C) Processes, methods, and techniques = [GC continuous monitoring strategies, processes, methods, and techniques for external systems where GC data is processed or stored]	X	X	X	X	X						X	X	CCC-02 HRS-06 STA-03 STA-05 STA-09	CC4.1	A.6.1.1 A.6.1.5 A.7.2.1 A.13.1.2 A.13.2.2 A.15.2.1 A.15.2.2
SA-9(1)	External Information System Services | Risk Assessments / Organizational Approvals	(b) Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	X	CCC-02 GRM-11 HRS-06 STA-03 STA-05 STA-09	CC7.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-9(2)	External Information System Services | Identification of Functions / Ports / Protocols / Services	External information system services = [any external service where GC information is processed or stored]	X	X	X	X	X						X	X		CC7.1	
SA-9(3)	External Information System Services | Establish / Maintain Trust Relationships with Providers	Security requirements, properties, factors, or conditions = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-9(4)	External Information System Services | Consistent Interests of Consumers and Providers	Security safeguards = To be defined as part of the tailoring process External service providers = [any external service provider that is responsible to process, transmit, or store GC information]	X	X	X	X	X						X	X		CC3.1	
SA-9(5)	External Information System Services | Processing, Storage, and Service Location	Selection (one or more): information processing; information/data; information system services = [information processing, transmission, information/data, and information system services] Locations = [within Canada] Requirements or conditions = [ITPIN 2017-02 for Direction on Data Residency (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html)]	X	X	X	X	X						X	X		CC5.5	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-10	Developer Configuration Management	(A) [Selection (one or more): design; development; implementation; operation = [development, implementation, and operation] (B) Configuration items under CM = [all items under configuration management] (E) Personnel = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-04 BCR-10 CCC-02 CCC-03	CC7.1 CC7.4	A.12.1.2 A.14.2.2 A.14.2.4 A.14.2.7
SA-10(1)	Developer Configuration Management | Software / Firmware Integrity Verification	Not applicable	X	X	X	X	X						X	X		CC7.1	
SA-10(2)	Developer Configuration Management | Alternative Configuration Management Processes	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-11	Developer Security Testing and Evaluation	(B) Selection (one or more): unit; integration; system; regression = To be defined as part of the tailoring process (B) Depth and coverage = To be defined as part of the tailoring process	X	X	X	X	X						X	X	BCR-04 BCR-10 CCC-02 CCC-03 DSI-05	CC7.1	A.14.2.7 A.14.2.8
SA-11(1)	Developer Security Testing and Evaluation | Static Code Analysis	Not applicable	X	Not allocated	X	X							Not Selected	X	BCR-04 BCR-10 CCC-02 CCC-03 DSI-05	CC7.1	
SA-11(2)	Developer Security Testing and Evaluation | Threat and Vulnerability Analyses	Not applicable	X	X	X	X	X						X	X		CC7.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-11(4)	Developer Security Testing and Evaluation | Manual Code Reviews	Specific code = [all code] Processes, procedures, and/or techniques = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-11(5)	Developer Security Testing and Evaluation | Penetration Testing / Analysis	Breadth/depth = To be defined as part of the tailoring process Constraints = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-11(6)	Developer Security Testing and Evaluation | Attack Surface Reviews	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-11(7)	Developer Security Testing and Evaluation | Verify Scope of Testing / Evaluation	Depth of testing/evaluation = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-11(8)	Developer Security Testing and Evaluation | Dynamic Code Analysis	Not applicable	X	X	X	X	X						X	X		CC7.1	
SA-15	Development Process, Standards, and Tools	(B) Frequency = [at least annually] (B) Security requirements = To be defined as part of the tailoring process	X	X	X	X	X						X	Not Selected			A.6.1.5 A.14.2.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-15(1)	Development Process, Standards, and Tools | Quality Metrics	(b) Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery = To be defined as part of the tailoring process (b) Frequency (is selected) = To be defined as part of the tailoring process (b) Program review milestones (if selected) = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-15(2)	Development Process, Standards, and Tools | Security Tracking Tools	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-15(3)	Development Process, Standards, and Tools | Criticality Analysis	Breadth/depth = To be defined as part of the tailoring process Decision points in the SDLC = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-15(4)	Development Process, Standards, and Tools | Threat Modeling / Vulnerability Analysis	Breadth/depth = To be defined as part of the tailoring process (a) Information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels = To be defined as part of the tailoring process (b) Tools and methods = To be defined as part of the tailoring process (c) Acceptance criteria = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction	Thresholds = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-15(6)	Development Process, Standards, and Tools | Continuous Improvement	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-15(7)	Development Process, Standards, and Tools | Automated Vulnerability Analysis	(a) Tools = To be defined as part of the tailoring process (d) Personnel or roles = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-15(8)	Development Process, Standards, and Tools | Reuse of Threat / Vulnerability Information	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-15(9)	Development Process, Standards, and Tools | Use of Live Data	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-15(10)	Development Process, Standards, and Tools | Incident Response Plan	Not applicable	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-15(11)	Development Process, Standards, and Tools | Archive Information System / Component	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-16	Developer-Provided Training	(A) Training = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			None
SA-17	Developer Security Architecture and Design	Not applicable	X	X	Not allocated		X						X	Not Selected			A.14.2.1 A.14.2.5
SA-17(1)	Developer Security Architecture and Design | Formal Policy Model	(a) Elements of organizational security policy = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-17(2)	Developer Security Architecture and Design | Security-Relevant Components	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-17(3)	Developer Security Architecture and Design | Formal Correspondence	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-17(4)	Developer Security Architecture and Design | Informal Correspondence	(b) Selection: informal demonstration; convincing argument with formal methods as feasible = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SA-17(5)	Developer Security Architecture and Design | Conceptually Simple Design	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-17(6)	Developer Security Architecture and Design | Structure for Testing	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-17(7)	Developer Security Architecture and Design | Structure for Least Privilege	Not applicable	X	X	Not allocated		X						X	Not Selected			
SA-18	Tamper Resistance and Detection	Not applicable	X	X	Not allocated		X						X	Not Selected			None
SA-22	Unsupported System Components	Not applicable	X	X	X		X						X	Not Selected			None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-22(1)	Unsupported System Components | Alternative Sources for Continued Support	Selection (one or more): in-house support; [Assignment: organization-defined support from external providers] = To be defined as part of the tailoring process Support from external providers (if selected) = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SC-1	System and Communications Protection Policy and Procedures	(A) Personnel or roles = [personnel or roles with system and communications protection responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AIS-04 AAC-03 GRM-06 GRM-08 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SC-2	Application Partitioning	Not applicable	X	X	X				X	X	X	X	X	X	AIS-01 IVS-08 IVS-09	CC5.1	None
SC-2(1)	Application Partitioning | Interfaces for Non-Privileged Users	Not applicable	X	X	Not allocated					X	X	X	X	Not Selected			
SC-4	Information in Shared Resources	Not applicable	X	Not allocated	X				X				Not Selected	X	AIS-01	CC5.1	None
SC-5	Denial of Service Protection	(A) Types of denial of service attacks = [attacks on bandwidth, transactional capacity, and storage] (A) Security safeguards = [geo-replication, IP address blocking, network-based DDoS protections]	X	X	X				X	X	X		X	X	AIS-01 TVM-01	CC5.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-5(2)	Denial of Service Protection | Excess Capacity / Bandwidth / Redundancy	Not applicable	X	X	Not allocated					X	X		X	Not Selected			
SC-5(3)	Denial of Service Protection | Detection / Monitoring	(a) Monitoring tools = To be defined as part of the tailoring process (b) Information system resources = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SC-7	Boundary Protection	(B) Selection: physically; logically = [physically and logically]	X	X	X				X	X			X	X	AIS-01 EKM-03 IVS-06 IVS-09 IVS-12 STA-09	CC5.1 CC5.6	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.3
SC-7(3)	Boundary Protection | Access Points	Not applicable	X	X	X	X	X						X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
SC-7(4)	Boundary Protection | External Telecommunications Services	(e) Frequency = [at least annually]	X	X	X	X	X						X	X	AIS-01 EKM-03 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
SC-7(5)	Boundary Protection | Deny by Default / Allow by Exception	Not applicable	X	X	X				X	X			X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-7(7)	Boundary Protection | Prevent Split Tunneling for Remote Devices	Not applicable	X	X	X				X	X			X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	Internal communications traffic = To be defined as part of the tailoring process External networks = To be defined as part of the tailoring process	X	X	X				X	X			X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	Not applicable	X	X	Not allocated					X	X		X	Not Selected			
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	Authorized sources = To be defined as part of the tailoring process Authorized destinations = To be defined as part of the tailoring process	X	X	X				X	X			X	Not Selected		CC5.6	
SC-7(12)	Boundary Protection | Host-Based Protection	Host-based boundary protection mechanisms = To be defined as part of the tailoring process Information system components = To be defined as part of the tailoring process	X	X	X	X	X						X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
SC-7(13)	Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components	Information security tools, mechanisms, and support components = To be defined as part of the tailoring process	X	X	X	X							X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-7(18)	Boundary Protection | Fail Secure	Not applicable	X	X	X				X	X	X		X	X	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
SC-8	Transmission Confidentiality and Integrity	(A) Selection (one or more): confidentiality; integrity = [confidentiality and integrity]	X	X	X				X	X	X	X	X	X	AIS-01 AIS-04 DSI-03 DSI-04 (mapped to SC-9) EKM-03	CC5.7	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	Selection (one or more): prevent unauthorized disclosure of information; detect changes to information = [prevent unauthorized disclosure of information and detect changes to information] Alternative physical safeguards = Selection (one or more): [physical security safeguards applied in applied in accordance with, or uses an adequate risk-based approach aligned with the practices specified in TBS and RCMP physical security standards and any related provisions of the Industrial Security Program]	X	X	X				X	X	X	X	X	X	AIS-01 DSI-03 DSI-04 (mapped to SC-9(1)) EKM-03	CC5.7	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-10	Network Disconnect	(A) Time period = [no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions]	X	X	X				X	X	X	X	X	X	AIS-01 IAM-12	CC5.1 CC5.6	A.13.1.1
SC-12	Cryptographic Key Establishment and Management	(A) Requirements for key generation, distribution, storage, access, and destruction = [CSE-approved cryptography]	X	X	X	X	X						X	X	AIS-01 EKM-02	CC5.1	A.10.1.2
SC-12(1)	Cryptographic Key Establishment and Management | Availability	Not applicable	X	X	Not allocated		X						X	Not Selected			
SC-12(2)	Cryptographic Key Establishment and Management | Symmetric Keys	Selection: CSE-compliant; CSE-approved = [CSE-compliant]	X	Not allocated	X	X							Not Selected	X	AIS-01 EKM-02	CC5.1	
SC-12(3)	Cryptographic Key Establishment and Management | Asymmetric Keys	Selection: CSE-approved key management technology and processes; approved PKI medium assurance certificates or prepositioned keying material; approved medium assurance or high assurance certificates and hardware security tokens that protect the user's private key = [CSE-approved key management technology and processes]	X	Not allocated	X	X							Not Selected	X		CC5.1	
SC-13	Cryptographic Protection	(A) Cryptographic uses and type of cryptography required for each use = [CSE-compliant cryptography as per CSE's Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111), or subsequent versions]	X	X	X				X	X	X	X	X	X	AIS-01 AAC-03 EKM-02 EKM-03	CC5.1	A.10.1.1 A.14.1.2 A.14.1.3 A.18.1.5
SC-15	Collaborative Computing Devices	(A) Exceptions = [no exceptions]	X	X	X								X	X		CC5.1	A.13.2.1*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-15(3)	Collaborative Computing Devices | Disabling / Removal in Secure Work Areas	Information systems or components = To be defined as part of the tailoring process Secure work areas = To be defined as part of the tailoring process	X	X	Not allocated								X	Not Selected			
SC-17	Public Key Infrastructure Certificates	(A) Certificate policy = To be defined as part of the tailoring process	X	X	X	X	X						X	X	AIS-01 EKM-02	CC5.1	A.10.1.2
SC-18	Mobile Code	Not applicable	X	X	X	X	X						X	X	AIS-01 IVS-01	CC5.8	None
SC-18(1)	Mobile Code | Identify Unacceptable Code / Take Corrective Actions	Unacceptable mobile code = To be defined as part of the tailoring process Corrective actions = To be defined as part of the tailoring process	X	X	Not allocated					X	X		X	Not Selected			
SC-18(2)	Mobile Code | Acquisition / Development / Use	Mobile code requirements = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SC-18(3)	Mobile Code | Prevent Downloading / Execution	Unacceptable mobile code = [unacceptable mobile code and mobile code technologies defined under SC-18]	X	X	X				X	X	X		X	Not Selected		CC5.8	
SC-18(4)	Mobile Code | Prevent Automatic Execution	Software applications = To be defined as part of the tailoring process Actions = To be defined as part of the tailoring process	X	X	Not allocated					X	X		X	Not Selected		CC5.8	
SC-18(5)	Mobile Code | Allow Execution only in Confined Environments	Not applicable	X	X	Not allocated		X						X	Not Selected			
SC-19	Voice over Internet Protocol	Not applicable	X	X	X	X							X	X		CC5.1	None
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	Not applicable	X	Not allocated	X				X				Not Selected	X		CC5.1 CC5.6	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-22	Architecture and Provisioning for Name / Address Resolution Service	Not applicable	X	X	X				X				X	X	IVS-06	A1.1	None
SC-23	Session Authenticity	Not applicable	X	X	X				X	X	X	X	X	X	EKM-03	CC5.1 CC5.3	None
SC-23(1)	Session Authenticity | Invalidate Session Identifiers at Logout	Not applicable	X	X	X				X	X	X	X	X	Not Selected		CC5.3	
SC-23(3)	Session Authenticity | Unique Session Identifiers with Randomization	Randomness requirements = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	Not Selected		CC5.3	
SC-24	Fail in Known State	(A) Known-state = To be defined as part of the tailoring process (A) Types of failures = To be defined as part of the tailoring process (A) System state information = To be defined as part of the tailoring process	X	X	Not allocated					X	X		X	Not Selected			None
SC-28	Protection of Information at Rest	(A) Selection (one or more): confidentiality; integrity = [confidentiality and integrity] (A) Information at rest = [all Protected B data and all medium integrity data]	X	X	X				X	X	X		X	X	EKM-03	CC5.1	A.8.2.3*
SC-28(1)	Protection of Information at Rest | Cryptographic Protection	Information = To be defined as part of the tailoring process Information system components = To be defined as part of the tailoring process	X	Not allocated	X				X	X	X		Not Selected	X		CC5.1	
SC-29	Heterogeneity	(A) Information systems or components = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SC-39	Process Isolation	Not applicable	X	Not allocated	X				X	X	X		Not Selected	X		CC5.1	None
SI-1	System and Information Integrity Policy and Procedures	(A) Personnel or roles = [personnel or roles with system and information integrity responsibilities] (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	X	AAC-03 CCC-04 DSI-04 GRM-06 GRM-08 GRM-09 IAM-07 TVM-02	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SI-2	Flaw Remediation	(C) Time period = [30 days of release of updates]	X	X	X	X	X						X	X	AIS-03 CCC-05 TVM-02	CC6.1 CC6.2 CC7.3	A.12.6.1 A.14.2.2 A.14.2.3 A.16.1.3
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	Frequency = [at least monthly]	X	Not allocated	X	X							Not Selected	X	AIS-03 CCC-05 TVM-02	CC7.3	
SI-2(3)	Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions	(b) Benchmarks = [30 days for high risk flaws, 90 days for moderate risk flaws]	X	Not allocated	X	X							Not Selected	X		CC7.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-3	Malicious Code Protection	(C)(a) Frequency = [at least weekly] (C)(a) Selection (one or more); endpoint; network entry/exit points = For CSP = [to include endpoints] For GC = [to include endpoints and network entry/exit points] (C)(b) Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] = [quarantine malicious code] (C)(b) Action (if selected) = To be defined as part of the tailoring process but to include [alerting administrator or defined security personnel]	X	X	X				X	X	X		X	X	AIS-03 CCC-04 TVM-01	CC5.8	A.12.2.1
SI-3(1)	Malicious Code Protection | Central Management	Not applicable	X	X	X	X	X						X	X	AIS-03 CCC-04 TVM-01	CC5.8	
SI-3(2)	Malicious Code Protection | Automatic Updates	Not applicable	X	X	X				X	X	X		X	X	AIS-03 CCC-04 TVM-01	CC5.8	
SI-3(4)	Malicious Code Protection | Updates only by Privileged Users	Not applicable	X	X	Not allocated					X	X		X	Not Selected			
SI-3(6)	Malicious Code Protection | Testing / Verification	(a) Frequency = [at least annually]	X	X	Not allocated		X						X	Not Selected			
SI-3(7)	Malicious Code Protection | Non Signature-Based Detection	Not applicable	X	X	X				X	X	X		X	X		CC5.8	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-4	Information System Monitoring	(A)(a) Monitoring objectives = [monitoring objectives consistent with the GC CSEMP] (B) Techniques and methods = To be defined as part of the tailoring process (G) Information system monitoring information = To be defined as part of the tailoring process (G) Personnel or roles = To be defined as part of the tailoring process (G) Selection (one or more): as needed; [Assignment: organization-defined frequency] = To be defined as part of the tailoring process (G) Frequency (is selected) = To be defined as part of the tailoring process	X	X	X	X	X						X	X	AIS-03 CCC-04 GRM-11 IAM-05 IVS-01 SEF-03 TVM-02	CC3.2 CC6.1	None
SI-4(1)	Information System Monitoring | System-Wide Intrusion Detection System	Not applicable	X	Not allocated	X	X							Not Selected	X		CC6.1	
SI-4(2)	Information System Monitoring | Automated Tools for Real-Time Analysis	Not applicable	X	X	X	X	X						X	X	AIS-03 CCC-04 GRM-11 IAM-05 IVS-01 SEF-03	CC6.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-4(4)	Information System Monitoring | Inbound and Outbound Communications Traffic	Frequency = [continually]	X	X	X				X	X	X		X	X	AIS-03 CCC-04 GRM-11 IAM-05 IVS-01 SEF-03	CC6.1	
SI-4(5)	Information System Monitoring | System-Generated Alerts	Personnel or roles = To be defined as part of the tailoring process but to include [GC governance body] Compromised indicators = To be defined as part of the tailoring process but to include [indicators of compromise specified in the GC CSEMP]	X	X	X				X	X	X		X	X	AIS-03 CCC-04 GRM-11 IAM-05 IVS-01 SEF-03	CC6.1	
SI-4(7)	Information System Monitoring | Automated Response to Suspicious Events	Incident response personnel = To be defined as part of the tailoring process Actions to terminate suspicious events = To be defined as part of the tailoring process	X	X	Not allocated					X	X		X	Not Selected			
SI-4(9)	Information System Monitoring | Testing of Monitoring Tools	Frequency = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SI-4(10)	Information System Monitoring | Visibility of Encrypted Communications	Encrypted communications traffic = To be defined as part of the tailoring process Information system monitoring tools = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-4(11)	Information System Monitoring | Analyze Communications Traffic Anomalies	Interior points within the system = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SI-4(12)	Information System Monitoring | Automated Alerts	Activities that trigger alerts = To be defined as part of the tailoring process	X	X	X	X	X						X	Not Selected		CC6.1	
SI-4(13)	Information System Monitoring | Analyze Traffic /E vent Patterns	Not applicable	X	X	Not allocated		X						X	Not Selected			
SI-4(14)	Information System Monitoring | Wireless Intrusion Detection	Not applicable	X	X	X	X							X	X		CC6.1	
SI-4(15)	Information System Monitoring | Wireless to Wireline Communications	Not applicable	X	X	Not allocated								X	Not Selected			
SI-4(16)	Information System Monitoring | Correlate Monitoring Information	Not applicable	X	Not allocated	X	X							Not Selected	X		CC6.1	
SI-4(23)	Information System Monitoring | Host-Based Devices	Host-based monitoring mechanisms = [system logging] Information system components = [components running a general purpose operating system]	X	Not allocated	X	X							Not Selected	X		CC6.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-5	Security Alerts, Advisories, and Directives	(A) External organizations = To be defined as part of the tailoring process but to include [GC governance body] (C) Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations] = To be defined as part of the tailoring process but to include [Assignment: organization-defined personnel or roles] (C) Personnel or roles (if selected) = To be defined as part of the tailoring process but to include [system security personnel and administrators with configuration/patch-management responsibilities] (C) Elements within the organization (if selected) = To be defined as part of the tailoring process (C) External organizations (if selected) = To be defined as part of the tailoring process	X	X	X	X	X						X	X	SEF-01 SEF-03 TVM-01 TVM-02	CC6.1 CC7.3	A.6.1.4*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-7	Software, Firmware, and Information Integrity	(A) Software, firmware, and information = To be defined as part of the tailoring process	X	X	X	X	X						X	X	AIS-03 CCC-04 CCC-05 TVM-01	CC6.1	None
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	Software, firmware, and information = To be defined as part of the tailoring process Selection (one or more): at start-up; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency] = [Assignment: organization-defined frequency] Transitional states or security-relevant events (if selected) = Not selected Frequency (if selected) = [no longer than 30 days]	X	X	X	X	X						X	X	AIS-03 CCC-04 CCC-05 TVM-01	CC6.1	
SI-7(2)	Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations	Personnel or roles = To be defined as part of the tailoring process	X	X	Not allocated		X						X	Not Selected			
SI-7(3)	Software, Firmware, and Information Integrity | Centrally-Managed Integrity Tools	Not applicable	X	X	Not allocated		X						X	Not Selected			
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Security-relevant changes = To be defined as part of the tailoring process	X	X	X	X	X						X	X		CC6.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture (Figure 3-1)							Informative References				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile PBMM	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)	ITSG-33 Profile 1 PBMM	FedRAMP Moderate	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-7(14)	Software, Firmware, and Information Integrity | Binary or Machine Executable Code	Not applicable	X	X	Not allocated		X						X	Not Selected			
SI-8	Spam Protection	Not applicable	X	X	X	X	X						X	X	EKM-03 TVM-01	CC5.8	None
SI-8(1)	Spam Protection | Central Management of Protection Mechanisms	Not applicable	X	X	X	X	X						X	X		CC5.8	
SI-8(2)	Spam Protection | Automatic Updates	Not applicable	X	X	X				X			X	X	X		CC5.8	
SI-10	Information Input Validation	(A) Information inputs = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	X	AIS-03	PI1.2	None
SI-11	Error Handling	(B) Personnel or roles = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	X	AIS-03	PI1.1	None
SI-12	Information Handling and Retention	Not applicable	X	X	X	X	X						X	X	DSI-04 GRM-02	PI1.4	None
SI-16	Memory Protection	(A) Security safeguards = To be defined as part of the tailoring process	X	X	X				X				X	X		CC5.1	None