ANNEX A
STATEMENT OF WORK

1. INTRODUCTION

1.1. Title

a) ***National Integrated Compliance and Enforcement Management Solution*** hereafter referred to as the "Solution".

1.2. Overview

a) The Government of Canada requires perpetual licenses for a web based National Integrated Compliance and Enforcement Management Solution that will be managed and hosted by the Contractor on a Shared Services Canada (SSC) certified 3rd party Protected B cloud platform that:

i) Allows the Tobacco Control Directorate (TCD) and the Tobacco and Vaping Compliance and Enforcement Program (TVCEP) to:

(A) fulfill its mandate to support and enable Health Canada (HC) to meet the business and legislative needs as required under the ***Tobacco and Vaping Products Act*** (TVPA), it's Regulations, and other related legislations;

(B) plan, carry out, track, document, and evaluate its national Compliance and Enforcement (C&E) program activities with respect to tobacco and vaping products;

(C) receive electronically submitted structured data through a secure portal and secure Representational State Transfer (RESTful) API;

(D) receive public comments and complaints through a secure portal in accordance with Canada's Federal Identity Program; and

(E) perform data analytics.

ii) Must provide a method for the tobacco and vaping product industry to submit mandated reports electronically through a secure portal and secure RESTful API in accordance with Treasury Board Secretariat (TBS) policy (see Section 5. Reference Documents).

iii) Replaces an existing suite of legacy C&E web applications and various software and data tools. The Solution will include functionality from the legacy applications as well as new functionality.

iv) Must be easily modifiable to accommodate ongoing new and developing tobacco and vaping products legislation, and C&E business policies, processes, procedures, guidelines and programs.

v) Must be bilingual (English and French).

vi) Must be complete, bug free and compliant to the specifications of this document.

vii) Must be hosted on a Shared Services Canada (SSC) certified 3rd party Protected B cloud platform in Canada.

viii) Must be compliant with Canada's security requirements.

ix) Must be in conformance with the current Web Content Accessibility Guidelines (WCAG) at the time the RFP closes as specified by TBS.

x) The Government of Canada must have access to its data at all time, as such the data must reside in a nonproprietary format. If the data is store in an encrypted format, Canada must also have the key to access the data. Canada will retain ownership of all data in the Solution including business data, monitoring data, and metadata.

1.3. Background

a) Health Canada's TCD, within the Controlled Substances and Cannabis Branch (CSCB), and TVCEP within the Regional Operations and Enforcement Branch (ROEB), are responsible for:

i) The administration and enforcement of the TVPA and its Regulations;

ii) Developing the policies, processes, procedures, guidelines, and programs, required to support Health Canada's C&E program activities with respect to tobacco and vaping products.

b) TCD and TVCEP are mandated to support Health Canada's C&E program activities authorized under the following federal legislations:

i) the TVPA which came into force May 23, 2018, and it's Regulations, such as but not limited to:

(A) the ***Amended Tobacco Reporting Regulations*** which came into force March 4, 2019;

(B) the ***Tobacco Product Regulations (Plain and Standardized Appearance)*** which came into force November 9, 2019, with several implementation dates between 2019 and 2022;

(C) the ***Vaping Products Labelling and Packaging Regulations*** which came into force July 1, 2020, with exception the child-resistant requirements for refillable vaping devices and their parts that will come into force on January 1, 2021;

(D) the ***Tobacco Product Promotion Regulations*** which came into force August 7, 2020, with exception for point-of-sale display restrictions that came into force on September 6, 2020.

ii) ongoing development of additional regulations under the TVPA.

iii) specific sections of the ***Canada Consumer Product Safety Act*** (CCPSA) as they relate to tobacco and vaping products.

c) C&E program activities are conducted according to established policies, business processes, procedures, matrices, strategies, and guidelines, such as, but not limited to: The Compliance & Enforcement Policy For the ***Tobacco and Vaping Products Act***, the Guidelines on Inspections and Investigations, and Procedures for Inspection.

d) The staff responsible for C&E program activities are located in several organizational units across Canada. Each organizational unit, or region, is composed of specific provinces and territories. The provinces and territories within each organizational unit are occasionally re-organized.

e) C&E program activities may be initiated in, and transferred between, any organizational unit. C&E program activities are carried out across Canada. They are conducted on-site (at establishment locations) or off-site (not at establishment locations) under the authority of the appropriate federal legislation.

f) There are three main categories of C&E program activities. They each follow the same compliance and enforcement process with minor variations. These categories include:

i) Compliance Promotion:

(A) Compliance Promotion activities are conducted by inspectors who provide targeted and specific information to regulated parties to inform them of their responsibilities under the legislation and to assist and encourage compliance with the applicable legislation. In addition to the documentation of time, date and information shared, all feedback, and relevant information regarding the regulated parties, is collected and documented and tracked against specific legislated sections

(B) Compliance Promotion information is also shared and distributed via various modes of communication, such as during on-site visits, mail, public notices, advertising in trade publications, e-mail, websites, etc.

(C) Compliance Promotion activities must be documented and tracked against specific legislation sections.

(D) Compliance Promotion activities never include any enforcement actions.

ii) Inspections:

(A) Inspection activities are conducted by inspectors under the authority of the appropriate federal legislation to verify compliance with the requirements of the legislation. These activities include both cyclical (pre-planned) and reactionary

activities (for example, in response to complaints and observed non-compliances of regulated parties), and inspections of industry report submissions.

(B) Industry reports are submitted according to a mandatory cyclical schedule, a specific business event, or on request. This includes scheduled reports not received according to the prescribed time lines (that is late or absent). All industry report submissions are subjected to the compliance and enforcement process.

(C) When non-compliances are observed, possible enforcement actions, ranging from warning letters to prosecution are considered based on a variety of factors including compliance history, severity of the non-compliances, specific business rules, etc. Along with any necessary management approvals, all non-compliances and enforcement actions must be documented, tracked, and referenced against specific legislation sections.

(D) Upon completion of the original activity, a subsequent, related activity (for example, inspection, investigation or compliance promotion of the regulated parties) may be initiated.

iii) Investigations:

(A) Investigation activities are conducted by inspectors under the authority of the Criminal Code of Canada. The purpose of an investigation is to determine penal liability of the regulated party with respect to non-compliance with the appropriate federal legislation sections.

(B) When non-compliances are found following an investigation, possible enforcement actions, including the preparation of a prosecution brief for consideration by the appropriate judicial authorities, are considered. Along with any necessary management approvals, all non-compliances and enforcement actions must be documented, tracked, and referenced against specific legislation sections.

g) In the context of an inspection or investigation, artifacts may be collected for either internal TCD and TVCEP analysis or external laboratory analysis. All information related to the details of the collected artifact, the chain of custody as required, and the results of the analysis, must be documented.

h) Some inspectors work in remote locations with little or no internet connectivity for extended periods. This results in inefficient duplication of documentation of activities, first using paper based documentation and then, once internet connection is available, re-documenting the activities via data entry into the existing legacy C&E applications.

i) TCD and TVCEP business is currently supported by the following three legacy custom-built C&E web applications that were originally designed to support the ***Tobacco Act*** and it's Regulations:

i) Tobacco Compliance Information Management System (TCIMS), which is used to document compliance and enforcement activities (compliance promotion, inspection, and investigation) with the TVPA and its Regulations;

ii) Tobacco Reporting Regulations System (TRRS), which is used to track the receipt of industry reports and document the compliance of regulated parties with the Tobacco Act's Tobacco Reporting Regulations (TRR); and

iii) Federal Electronic Tobacco Reporting and Evaluation System (FETRES), which is primarily used to validate industry report data used in research and market surveillance work.

j) The three legacy C&E web applications are written in Java and Flex and are hosted on a WebSphere platform with an Oracle database. The applications share a common sign on facility. The Users access the applications using a web browser on their Windows based desktop.

k) Various software and data tools (including, but not limited to, Excel, Access, Lotus Notes databases, email) are used to supplement the functionality not available in the legacy C&E applications.

l) The three legacy C&E web applications and various software and data tools are no longer adequate to meet TCD and TVCEP business and legislative needs under the TVPA. The legacy applications are not easily modified to accommodate ongoing changes to:

(A) C&E policies,

(B) business processes,

(C) procedures,

(D) guidelines,

(E) programs,

(F) new and developing tobacco and vaping products regulations under the TVPA.

m) Each of the legacy applications have some pre-configured reporting functionality. In addition, data in the legacy applications, various software and data tools are exposed to Cognos Analytics for business intelligence (BI) and analytics. Business intelligence and data analytics activities encompass the ability to analyse, summarize, and disseminate data received and/or collected through C&E program activities and other relevant research and surveillance activities. Business Intelligence activities inform evidence-based decision-making for policy and regulatory development, resource allocation for C&E program activities and information for the public.

n) Although the applications are linked in some ways, there is a large amount of data siloing which limits data sharing and collaboration between business units. For example, there is currently no integrated application supporting the transfer of Tobacco Reporting Regulations (TRR) sales data for analysis by the Business Intelligence Division (BID).

o) Currently, approximately 1,800 reports are received annually by HC from approximately 50 regulated parties. The frequency (for example, monthly, quarterly, annually, and bi-annually) of these reports can be found in the ***Tobacco Reporting Regulations*** https://laws-lois.justice.gc.ca/eng/regulations/SOR-2000-273/page-1.html. The majority of reports are required annually and submitted between January and March.

p) These reports are delivered by courier or email, and are written on paper and or in various digital formats. Furthermore, the report data are not consistently structured which makes evaluation and cross report data analysis very laborious and inefficient.

q) The majority of TCD/TVCEP users of the legacy applications and various software and data tools are inspectors located in each province and territory across Canada.

r) The three legacy C&E web applications support the following:

Users:
- **175** active users;
- **175** deactivated accounts (kept for record keeping policy);
- An average of **25** concurrent user sessions at peak times.

Usage:
- **10,000** activities completed annually;
- **1,800** industry reports processed annually.

1.4. Objectives

a) Canada requires a Solution that must:

i) Provide usability, functionality, and configurability.

ii) Integrate the data from the three legacy systems and various software and data tools into one Solution.

iii) Meet the requirements identified in Section 3. Phase 2 – Full Solution of this document.

iv) Implement existing and new workflows and business processes;

v) Provide workload management;

vi) Provide users with the capability to analyze data in order to support decision making;

vii) Provide direct access to real-time Solution data for business intelligence and analytics through API's to support policy and regulatory development;

viii) Support the streamlined processing of submitted industry reports;

ix) Support the submission of large volumes of structured data;

x) Be operational on a SSC certified 3rd party Protected B cloud platform

b) Canada also requires the following services on and as and when requested basis:

i) Training Services for Solution Administrators.

ii) Professional Services for additional configuration, implementation, data migration, and other work identified during the duration of the Contract.

iii) Training Services for end-users.

1.5. Scope of Work

a) Canada is seeking to replace its three existing C&E legacy applications (TCIMS, TRRS, and FETRES) and related software and data tools with an integrated Solution that is configurable to accommodate new legislation and business rules, as well as new functionality.

b) Work will be conducted in accordance with the 2 phases described below:

i) Phase 1 - Prototype Solution: The Contractor must develop and deliver a Prototype Solution in accordance with Phase 1 work as described in Section 2. Phase 1 - Prototype Solution and in Appendix A- Capability and Usability Assessment (CUA).

ii) Phase 2 - Full Solution: On completion of Phase 1 work and following the Capability and Usability Assessment (CUA) of Prototype Solutions submitted to Canada, Canada, at its sole discretion, will exercise the irrevocable option to the top ranked Contractor to develop and deliver the Full Solution in accordance with Phase 2 work as described in section 3. Phase 2 - Full Solution and in Appendix B –Full Solution Requirements.

c) The Full Solution will need to accommodate growth of new potential users and all C&E program activities, including the increase in the number of mandated reports submitted by industry that are expected to occur over the lifespan of the Solution, as the legislation of the TVPA is fully developed and enforced.

1.6. Optional scope

a) Canada also requires the following services on and as and when requested basis, including but not limited to:

i) Professional Services in accordance with Section 4.1 Optional Professional Services.;

ii) Migration to an alternate hosting environment in the event that Canada's business requirements change.

iii) Solution Instances in accordance with Section 4.1 Optional Professional Services, article (v)

iv) Provision of a document management system for documents generated by Canada where the user is able to configure the document management component to meet with record keeping and information management and disposition best practices through the following capabilities, including but not limited to:

(A) Disposition Schedule

(B) Disposition List

(C) Record Disposition

(D) Record Archival and Retrieval

(E) Disposition Hold

v) Configuration of additional workflows, such as policy and regulatory development, surveys, and market research.

1.7. Current Health Canada Technical Environment Overview

a) HC User Environment Overview

i) HC user desktops run on Windows 10 and contain Microsoft Office 2016 applications (Word, Excel, PowerPoint, and Outlook).

ii) All HC user have the ability to connect to the internet, although some connections could be slow or nonexistent in rural areas.

iii) HC users do not have proxies; however, much of the traffic exits through common gateways.

iv) Cognos Analytics 10, Power BI, and other data analytic tools, are available to HC users.

b) Legacy Application Environment Overview

i) The existing legacy applications (TRRS, FETRES, and TCIMS) identified in Section 1.3 g) run on SUSE Linux Enterprise Server 11

ii) The database is Oracle 11g

iii) The application server is WebSphere 8.5

1.8. Estimated Full Solution Volume

Canada projects the following usage estimates over the lifespan of the Solution. The estimates are provided for informational purposes and do not represent a commitment that Canada's future usage will be consistent with this data.

a) Canada estimates an initial requirement of 200 perpetual licenses with an estimated growth over the course of the contract upwards of 400 perpetual licenses.

b) Canada estimates a total requirement of 2,900 regulated parties (tobacco and vaping product industry) and laboratories to access the portal to upload or download data at the time of delivery of the Full Solution; It is estimated that over a 10 year span usage of the Solution will increase to upwards of 3,900 regulated parties (tobacco and vaping product industry) and laboratories.

c) Estimated number of concurrent users without degradation to performance

i) Canada estimates the following Government of Canada (GOC) concurrent Solution usage:

(A) Average: 200 users

(B) Minimum: 100 users

(C) Maximum: 300 user

ii) Canada estimates the following regulated parties (tobacco and vaping product industry) and laboratories secure portal and RESTful API concurrent usage:

(A) Average: 300 regulated parties (tobacco and vaping product industry) and laboratories

(B) Minimum: 100 regulated parties (tobacco and vaping product industry) and laboratories

(C) Maximum: 3,300 regulated parties (tobacco and vaping product industry) and laboratories

d) Estimated Usage

i) Canada estimates a requirement of an average of 60,000 GOC user generated activities completed annually estimated to grow to 74,000 activities completed annually

ii) Canada estimates a requirement of an average of 51,000 industry reports estimated to grow to 65,000, processed annually through the secure portal and secure RESTful API. The reports would be submitted monthly, quarterly, annually, or bi-annually, but the majority of reports are required annually and submitted between January and March.

e) Estimated Data Storage

i) Canada estimates industry report file sizes between 10KB and 5GB.

ii) Canada estimates data storage to be 500 gigabytes (GB), with an estimated growth of up to 5 terabytes (TB) of data over 10 years.

2. PHASE 1 – PROTOTYPE SOLUTION

2.1. Scope of Work

a) The scope of work for the Prototype Solution involves the planning, design, development, configuration, testing and delivery of a production quality, hosted, working Prototype Solution ready to be deployed, in accordance with the Phase 1 - Prototype Solution Requirements and Deliverables.

2.2. Prototype Solution Requirements

a) The Contractor must configure and deliver a Prototype Solution that may be comprised of any combination of Commercial-Off-The-Shelf (COTS) software or open-source software in accordance with the requirements as described in this section and in Appendix A - Capability and Usability Assessment (CUA). Interoperability and Integration points between components of the Prototype Solution must be transparent to the User.

b) The Prototype Solution must provide access for 25 licensed users and support up to six (6) concurrent users without degradation to the Solution's performance.

c) The Contractor's resulting configuration of the Prototype Solution must provide Canada with an integrated web application that supports all capabilities described in the user scenarios detailed in Appendix A – Capability and Usability Assessment (CUA) document.

d) The Contractor must provide the following Phase 1 - Prototype Solution Non-functional requirements identified below:

i) Phase 1 - Prototype Solution Kick-off meeting which must:

(A) Be conducted in accordance with federal public health recommendations related to COVID-19; occur virtually via video conference, teleconference or at a mutually agreed location in Canada's National Capital Region;

(B) Be chaired by the PSPC Contracting Authority;

(C) Include a presentation (if applicable) and an agenda for the meeting to be provided to the PSPC Contracting Authority at least 2 business days prior to the kick-off meeting; and

(D) Include minutes of the meeting to the PSPC Contracting Authority for approval within three (3) business days after the start date of the meeting and prior to distribution to all Authorities.

ii) Draft Phase 2 – Full Solution Project Implementation Plan proposed for Phase 2 work which must include:

(A) Processes, that will be used throughout the project to ensure its timely planning, execution, and control, will include:

1) Quality Management;

2) Communications Management;

3) Risk Management;

4) Change Management.

(B) 1 Draft Phase 2 – Full Solution Project Schedule proposed for Phase 2 work, which must include a detailed listing of stages, tasks and subtasks, with start and completion dates, responsibilities, and predecessors for each. Tasks must include all design, integration and implementation activities, deadlines, milestones, draft deliverables, review periods, final deliverables and sign offs;

iii) Draft Phase 2 – Full Solution Technical Infrastructure Design document proposed for Phase 2 work which must include, at a minimum, information on design details for the hosted cloud environment(s) proposed by the Contractor, containing, at a minimum, detailed information on:

(A) Methodology, tools, procedures, activities, and services;

(B) Security infrastructure and services (identify, protective, monitoring and detective, and responsive and recovery);

(C) Network and connectivity;

(D) Performance characteristics; and

(E) Availability and flexibility requirements.

iv) Solution Support Documentation, which includes, at a minimum:

(A) Details on how to adapt fields, business rules, business process workflows, and data structure, as and when requested, to support Canada's business needs.

(B) Setup and Operations guide that includes, but not limited to, all installation, setup, management, and configuration instructions for the Prototype Solution;

(C) Support documentation or help files for each Use Case (scenario) in the Capability and Usability Assessment;

(D) Test procedures.

v) 1 Prototype Solution Delivery which must include:

(A) Access for 25 Authorized users, with all Prototype Solution usage rights grants;

(B) Sample data provided by Canada migrated to the Prototype Solution;

vi) Contractor Engagement and Progress Update Sessions

(A) Contactor engagement and progress update sessions to be held throughout the Prototype Solution development phase and conducted in accordance with federal public health recommendations related to COVID-19 and occur virtually via video conference, teleconference or at a mutually agreed location in Canada's National Capital Region. This provides a collaborative opportunity for the Business Client and Technical Authority to interact with the Contractor throughout the Prototype development to answer questions on the requirements, and provide feedback on prototypes, thus ensuring a thorough understanding of the requirements while promoting users at the forefront.

(B) Progress Update Sessions must include:

1) Tasks in-progress or completed since last progress update

2) Tasks planned for the next 2 weeks and estimated completion date

3) Issues preventing ongoing and upcoming tasks from being completed

2.3. Capability and Usability Assessment

a) Canada will conduct a Capability and Usability Assessment (CUA) on the Prototype Solution deliverables in accordance with the assessment procedures and criteria identified in Appendix A – Capability and Usability Assessment (CUA).

2.4. List of Prototype Deliverables

a) The Contractor must prepare and submit to the Technical Authority the Phase 1 – Prototype Solution deliverables:

i) 1 Phase 1 - Prototype Solution Kick-off Meeting

ii) 1 Draft Phase 2 – Full Solution Project Implementation Plan, that includes a Draft Phase 2 – Full Solution Project Schedule, proposed for Phase 2 – Full Solution work

iii) 1 Draft Technical Infrastructure Design proposed for Phase 2 – Full Solution work

iv) 1 Prototype Solution Documentation

v) 1 User Documentation

vi) 1 Prototype Solution Delivery

vii) Contractor Engagement and Progress Update Sessions

2.5. Prototype Deliverable Schedule

a) Any document required to be submitted for Phase 1 – Prototype Solution work will be submitted via a method to be communicated by Canada.

b) The following table identifies the dates of the deliverables identified in Section 2.4 List of Prototype Deliverables. The deliverables must be submitted to the Technical Authority in the format and by the delivery dates specified below.

Table 1: Phase 1 – Prototype Solution Deliverable Schedule

Deliverable #	Description of Deliverable	Delivery Date
i)	1 Phase 1 – Prototype Solution Kick-off Meeting	Within 1 week from Contract award date
ii)	Contractor Engagement and Progress Update Sessions, including Progress Reports, digital copy	Two sessions after Contract award date and prior to Prototype Solution Delivery
iii)	1 Draft Phase 2 – Full Solution Project Implementation Plan, including a Draft Phase 2 – Full Solution Project Schedule, proposed for Phase 2 - Full Solution work, digital copy	18 weeks after Contract award date
iv)	1 Draft Technical Infrastructure Design for Phase 2 – Full Solution work, digital copy	18 weeks after Contract award date
v)	1 Prototype Solution Documentation, digital copy	19 weeks after Contract Award date
vi)	1 User Documentation, digital copy	19 weeks after Contract Award date
vii)	1 Prototype Solution Delivery	20 weeks after Contract award date

2.6. Location and Travel

a) Location of work is at the Contractor's facility. No travel is anticipated. Canada will not reimburse any travel expenses incurred.

2.7. Language of Work

a) The primary language of work will be in English and all reports, technical documents and project updates must be provided in English.

b) The Prototype Solution and the interface for the Prototype Solution (i.e., interface used by users) must be in English.

3. PHASE 2 – FULL SOLUTION

a) All work listed under section 3. Phase 2 – Full Solution is subject to and contingent upon, at Canada's sole discretion, Canada's decision to exercise the irrevocable option under Article 7.1.2 i) in the Contract to authorize the Contractor to perform all or a portion of the work described.

3.1. Scope of Work

a) The Contractor must deliver a Full Solution that is a bilingual Solution containing all functional and non-functional requirements as specified in 3.2 Full Solution Requirements and in the Full Solution Requirements section of the Appendix B- Full Solution Requirements document of this SOW.

b) The Contractor must install and deploy the Solution to a SSC certified 3rd party Protected B cloud platform located in Canada.

c) The Contractor must configure and deliver a Solution that may be comprised of any combination of Commercial-Off-The-Shelf (COTS) software or open source software; however, the resulting configuration must comply with the requirements described in this SOW.

d) The Contractor must provide Solution training by user role.

e) The Contractor must provide additional optional services as described in Section 4 on an as-and-when-requested basis, following the Task Authorization process in accordance with Article 7.10.12 of the resulted Contract award that will be applicable after Canada has exercised its irrevocable option to exercise Phase 2 - Full Solution work:.

3.2. Full Solution Requirements

a) The Full Solution must be a fully-functional, bilingual (English and French), managed hosted web Solution on a SSC certified 3rd party Protected B cloud platform located in Canada, with access for 200 licensed users and one administrator account that will be accepted and considered by Canada as having Quality of Use, Configuration, Execution and Results, and be compliant with the requirements of the Contract at all times. The Solution must support the estimated Solution volume identified in section 1.8 – Estimated Full Solution Volumes.

b) The Full Solution must contain all technical, non – functional, and functional requirements as described in 3.2 Full Solution Requirements and in the Full Solution Requirements section of the **Error! Reference source not found.**- **Error! Reference source not found.** document.

c) The Contractor must provide the following Non-functional requirements summarised below:

i) Phase 2 - Full Solution Kick-off Meeting which must:

(A) Discuss the overall phase 2 approach and methodology, requirements, working relationships, timeframe, risks and issues;

(B) Conducted in accordance with federal public health recommendations related to COVID-19 and occur virtually via video conference, teleconference or at a mutually agreed location in Canada's National Capital Region. The Chairperson for the kick-off meeting will be the PSPC Contracting Authority;

(C) Include a presentation (if applicable) and an agenda to the Contracting Authority within three (3) business days prior to the start date of the meeting; and

(D) Include minutes of the kick-off meeting to the Contracting Authority for approval within three (3) business days after the start date of the meeting, and prior to distribution to all Authorities.

ii) The Contractor must prepare, develop, and implement the following plans:

(A) Project Implementation Plan

1) The Contractor must submit a Project Implementation Plan prepared in consultation with the Technical Authority.

2) The Project Implementation Plan will ensure the successful deployment of the Solution.

3) The Project Implementation Plan must include, at a minimum:

I. Processes, that will be used throughout the project to ensure its timely planning, execution, and control, must include:

a. Project integration management process to indicate the contractor's approach and procedures to ensure the various elements of the projects are properly coordinated

b. Scope management process to indicate the contractor's approach and procedures to ensure all the work is included in the project.

c. Schedule management process to indicate the contractor's approach and procedures in handling and managing the project schedule during contract execution.

d. Quality management process to indicate the contractor's approach and procedures in ensuring project quality is met and maintained during contract execution.

e. Communications management process to indicate the contractor's approach and procedures in communicating with the Contracting Authority, Technical Authority, and HC client users during contract execution.

f. Risk management process, indicating how the contractor intends to identify, mitigate, manage, and report risks during contract execution.

g. Requirements management process to indicate the contractor's approach and procedures in handling and managing requirements during contract execution.

h. Change management process to indicate the contractor's approach and procedures in handling and managing changes to the requirements, scope, schedule, and cost during contract execution.

i. Planning assumptions made by the contractor during developing the Project Implementation Plan.

II. Project Schedule, prepared in consultation with the Technical Authority, must include:

a. The scope of the phase 2 work including milestones, events, and deliverables to be delivered under this Statement of Work (SOW);

b. A Gantt chart format schedule based on a planned sequence of events;

c. A clear indication of the phase 2 critical path schedule based on an assessment of the network logic schedule;

d. Identify the roles and responsibilities of the Contractor's personnel, including sub-contractors, involved in the project;

e. Identify the project phases, deadlines, review periods, sign offs, deliverables and milestones of the work;

f. Identify each contract deliverable as a milestone;

g. Identify project milestone dates; and

h. Clearly describe any dependencies on Technical Authority review and approval.

4) Proof Of Portal Staged Demonstrations: Demonstrate External Data Submission workflows for Industry Reports in several staged demonstrations configured and implemented for specific Sections of the TRR. Each stage will include the functionality delivered in the previous stage. The functionality to be demonstrated in each phase will be determined in consultation with Technical Authority. The external data submissions must be demonstrated for the following workflows and Industry Reports:

I. Secure Portal workflow for Section 11 of the TRR.

II. Secure RESTful API workflow for Section 13 of the TRR.

5) Full Solution Staged Demonstrations: Demonstrate functionality in several staged demonstrations configured and implemented as follows:

I. Stage 1:

a. Establishment

b. User Management

c. Solution Administration

d. Single Sign On

II. Stage 2:

a. Online Compliance and Enforcement workflows

b. Address Validation

III. Stage 3: Full External Data Submission Secure Portal and Secure RESTful API workflows

IV. Stage 4:

a. Offline Solution

b. Cloud hosting

c. Bilingual Solution (English and French)

d. WCAG conformance

e. Pre-defined Reports

f. Ad-hoc Search

g. Full Security Controls

V. Stage 5: Business Intelligence and Analytics functionality

(B) Project Status Reporting Plan

1) The plan will define how, for the duration of the contract, the Contractor will provide the most current version of the progress update reports for the approval of the Technical Authority on the status of all work, detailing accomplishments for a bi-weekly period, open issues, and upcoming milestones.

(C) Final Technical Infrastructure Design

1) The plan must include, at a minimum, information on design details for the hosted cloud environment(s) proposed by the Contractor, containing, at a minimum, detailed information on:

I. Methodology, tools, procedures, activities, and services

II. Security infrastructure and services (identify, protective, monitoring and detective, and responsive and recovery)

III. Network and connectivity

IV. Performance characteristics

V. Availability and scalability requirements.

(D) System Security Control

Implement the security control as specified in Appendix E.

(E) Data Migration Plan

1) Prepared in consultation with Technical Authority, the Data Migration Plan must, as a minimum, identify:

I. Legacy Data mapping and conversion process

a. Process to identify the legacy data to be migrated

a. Data cleansing method to identify how the contractor will detect and correct (or remove) corrupt or inaccurate records from a record set, table, or database, and how they will replace, modify, or delete the dirty or coarse data.

b. Migration method to identify the process to select, prepare, extract, transform and transfer data.

c. Data migration schedule to identify the time frame the data migration is planned to occur.

d. Post migration data integrity and quality test method to ensure the data was successfully migrated.

(F) Deployment Plan

1) Prepared in consultation with Technical Authority, the Deployment Plan must, at a minimum, include:

I. Process to deliver the Solution.

II. Transition strategy to have two systems working in parallel until all data and content is fully transitioned from the legacy applications to the new Solution.

III. Timeframe for deployment, which includes how and when the Solution will be released.

IV. Preparation required for the hosting environment, which will include a description of the tasks required prior to standing up the hosting environment.

V. Deployment verification details, which outline the checks or tests that will ensure the Solution has been correctly deployed.

VI. Validation details that describe the tests to ensure that the deployed Solution has met Canada's needs.

VII. Rollback contingency details, which describe the actions that will be taken to return the Solution to its last known good state in response to a failed change and estimated durations for the rollback.

VIII. Security in accordance with the Security Controls.

IX. Data migration timeframes as described in the Data Migration Plan.

X. End user tasks required in preparation for Solution deployment.

XI. End user notification of Solution deployment.

(G) Maintenance and Support Plan

1) The Contractor must submit a plan for ongoing maintenance and support for the duration of the Contract including instructions for resolving Solution problems and requesting enhancements.

(H) Backup and Disaster Recovery Plan (DRP)

1) The Disaster Recovery Plan must identify the backup method and schedule, including regular backup verification and disaster recovery review and testing.

2) The Disaster Recovery Plan must document and describe:

I. A structured approach as to how Canada can quickly resume work after an unplanned incident involving the Solution, including:

a. establishing the range or extent of necessary treatment and activity - the scope of recovery;

b. gathering relevant network infrastructure documents; and

c. identifying the most serious threats and vulnerabilities, and the most critical assets;

II. Procedures for updating the DRP and implementing a DRP audit;

III. Procedures to help Canada resolve data loss and recover system functionality so that it can perform in the aftermath of an incident, even if it operates at a minimal level;

IV. A set of policies, tools and procedures to enable the recovery and continuation of the Solution operation following a natural or human-induced disaster.

V. The Contractor will be required to work collaboratively with Canada to ensure that the DRP for the Solution integrates effectively with Canada's more broadly based DRP for the enterprise technology infrastructure and critical application systems operating within.

VI. The DRP must describe in sufficient detail how Canada can quickly recover and resume work after a major unplanned incident affects the Solution delivered by the Contractor.

VII. The Contractor must describe the approach to achieving Solution recovery and the approach to data recovery.

(I) Solution Testing and Quality Management Plan

1) The Solution Testing and Quality Management Plan must describe how each requirement will be met, including test methods and test cases for each functional category as below:

I. Establishments, User Management, Solution Administration, and Single Sign On

II. Online Compliance and Enforcement workflows, and Address Validation

III. External Data Submission Secure Portal and Secure RESTful API workflows

IV. Offline workflows, Cloud hosting, Bilingual Solution (English and French), WCAG conformance, Pre-defined Reports, and Ad-hoc Search

V. Business Intelligence and Analytics

2) The Contractor must prepare a Solution Testing and Quality Management Plan to describe how the functional and technical capabilities and processes will be tested in order to provide assurance to Canada that the Contractor's testing and quality management plans are in alignment with the requirements as defined in this SOW.

3) The Solution Testing and Quality Management Plan must be approved by Canada. Solution Testing must be conducted in accordance with the approved Solution Testing and Quality Management Plan and in alignment with the approved Solution Implementation Plan.

4) During development of the Solution, the Contractor must participate in quality management activities including reviews with Canada resources and Solution Users as well as testing (performance and regression) of various components and features of the system as needed to ensure acceptance.

5) The Contractor's methodology must follow principles and values allowing frequent quality and review steps to be built in throughout the delivery and integration process.

6) The Contractor's methodology must include Testing Plans consisting of:

   I. Regression Testing: Details on how the Solution will be tested to ensure a change or addition has not broken any existing functionality.

   II. Pre installation Testing: Details on testing to ensure that the hosting environment is configured with the software, user accounts, directories, and other prerequisites required for an initial installation of the Solution.

   III. Security Testing: Details on security tests to be performed to meet Canada's security requirements; and

   IV. Smoke Tests: Outline the set of tests that ensure the major, critical functions of the Solution will work and stable enough to proceed to further testing.

7) The Solution Testing and Quality Management Plan must describe the Contractor's approach to the following best practices, including but not limited to:

   I. Test data for:

      a. Unit Testing (including data and field validation testing);

      b. Integration Testing;

      c. Stress Testing;

      d. Regression Testing; and

e. User Acceptance Testing.

II. Testing and acceptance includes:

a. Collaboration with stakeholders;

b. Definition of "Done"; and

c. End to end unit, functional, usability, accessibility, error, exception, compliance, interoperability, integration, and security (including vulnerability assessment scans) testing.

III. Maintenance Release and Patch Testing including regression testing due to updates;

IV. Test each incremental functional component and include the test results in each requirement's definition of Done in a Test Report;

V. Address quality, both reactively through testing and proactively encouraging practices to set the stage for quality work. Examples of proactive quality approaches include face to face communication, pair programming, and established coding standards;

VI. Create and test riskier features and functionality early in the project when sunk costs are still low; and

VII. Test smaller amounts of functionality that have just been created and do so to make problems easier to find.

8) The Contractor must provide a Solution Test Report(s) providing the results of the tests identified and performed as part of the Solution Testing and Quality Management Plan for each of the Full Solution Staged Demonstrations (as described in section 3.2 c ii) (A) 5).

(J) Business Intelligence Plan that includes a description of the Business Intelligence tools to be used and how the BI tools will be implemented.

(K) Training Plan

1) Prepared in consultation with Technical Authority, the Training Plan must include, at a minimum, recommendations for:

I. Training approach conducted in accordance with federal public health recommendations related to COVID-19 and occur virtually via video conference, teleconference or at a mutually agreed location in Canada's National Capital Region.

II. Training schedule.

III. Full training requirements by user role in preparation for Solution deployment.

IV. Training materials approved by the Technical Authority (as described in section 3.2. c ii) (L)).

(L) Training Materials

1) The Contractor must deliver end user training materials in accordance with the approved Training Plan and in consultation with the Technical Authority.

2) Up to date training materials and course content must be provided each time training is provided.

3) All training material must be made readily available 24 hours per day, 7 days a week for all users.

4) All training material must be provided in both of Canada's official languages (English and French).

iii) The Contractor must prepare and develop the following documentation:

(A) Requirements Compliance Document

1) The Requirements Compliance Document will describe how each requirement has been met for each of the Full Solution Staged Demonstrations (as described in section 3.2 c ii) (A) 5), including test methods and test cases for each functional category as listed below:

I. Establishments and User Management, Solution Administration, and Single Sign On

II. Online Compliance and Enforcement workflows, and Address Validation

III. External Data Submission Secure Portal and Secure RESTful API workflows

IV. Offline workflows, Cloud hosting, Bilingual Solution (English and French), WCAG conformance, Pre-defined Reports, Ad-hoc Search and Full Security Controls

V. Business Intelligence and Analytics

(B) 1 Exit Strategy Document

1) An exit strategy for migrating to an alternate hosting environment in the event that Canada's business requirements change.

(C) Risk Registry Document

1) The Risk Registry document will enable tracking and monitoring of risks throughout the project. The Risk registry must reflect the risk management process identified in the Project Plan.

(D) Solution Support Documentation must include, at a minimum:

1) Setup and Operations guide that includes, but not limited to, all installation, setup, management, and configuration instructions for the Full Solution;

2) Solution documentation;

3) Help files;

4) Source code (for all source code sponsored by the Government of Canada);

5) Database schemas (for all schemas sponsored by the Government of Canada); and

6) Details on how to adapt fields, business rules, business process workflows, and data structure, as and when necessary, to support Canada's business needs.

(E) 1 Project Close-Out Report

1) Develop the Project Close-Out report to mark the completion of the project;

2) Assessing the project's performance and outcomes, identifying the lessons learned, and confirming that essential contractual and other project close-out activities have been completed;

3) Complete the transfer of assets, deliverables, and all ongoing administrative functions to the Technical Authority; and

4) The Contractor may decide the best format and number of artifacts (e.g., diagram, views, models, matrices) that are required. Artifacts submitted must be clearly and concisely described, and allow the Technical Authority to understand how the requirements are being met.

(F) Progress Meetings

1) Progress meetings to be held throughout the Full Solution development phase. This provides a collaborative opportunity for the HC Business Client and Technical Authority to interact with the Contractor throughout the development to answer questions on the requirements, and provide feedback on the development, thus ensuring a thorough understanding of the requirements. The Progress Meetings must include:

I. Tasks in-progress or completed since last progress update

II. Tasks planned for the next 4 weeks and estimated completion date

III. Issues preventing ongoing and upcoming tasks from being completed

IV. Progress reports

iv) Migrate existing TCD and TVCEP legacy application data and applicable data from various software tools. These legacy data sources include, but are not limited to:

(A) Databases (Such as Oracle, MS Access); and

(B) Excel worksheets.

3.3. Deliverables Overview

a) The Contractor is required to implement the project using proven methodologies that includes services for project management, system design configurations, deployment, documentation, testing, training and end-user support and on-going support for the delivery of fully functional Solution, including:

i) Providing in-depth as-and-when requested consultation regarding best practices and process efficiencies, ensuring a successful integration with the Technical Authority processes, procedures and technical environment;

ii) Providing as-and-when requested training and training materials for end users and administrators.

iii) Providing support to ensure that Canada maximizes both the use and cost effectiveness of the Solution.

b) To ensure the success of the implementation of the Solution, the project will include, at minimum, the implementation deliverables as listed below. The creation of each deliverable is the responsibility of the Contractor and must be formally presented to the Technical Authority for review and acceptance. For milestones with multiple stages, each stage is expected to contain each deliverable (unless noted otherwise).

c) The Contractor must use Canada-approved 2016 version of Microsoft Office applications (Word, Excel, PowerPoint, Visio, Project, and Access) to create and update document deliverables. All documents must be fully editable so they can be updated by Canada. At Canada's discretion, the Contractor may be required to submit documents in other softcopy formats.

3.4. List of Full Solution Deliverables

a) The Contractor must prepare and submit to the Technical Authority the following Phase 2 – Full Solution deliverables:

i) 1 Kick-off Meeting

ii) 1 Project Schedule

iii) 1 Project Implementation Plan

iv) 1 Proof Of Portal Staged Demonstration

v) 1 Project Status Reporting Plan

vi) 1 Final Technical Infrastructure Design

vii) 1 Data Migration Plan

viii) 1 Deployment Plan

ix) 1 Maintenance and Support Plan

x) 1 Backup and Disaster Recovery Plan (DRP)

xi) 1 Solution Testing and Quality Management Plan

xii) 1 Business Intelligence Plan

xiii) 1 Training Plan

xiv) 1 Solution Test Report

xv) 1 Exit Strategy

xvi) 1 Risk Registry

xvii) 1 Solution Support Documentation

xviii) 1 Training Materials

xix) 1 Full Solution Staged Demonstrations

xx) 1 Requirements Compliance Document

xxi) 1 Solution Administrator Training

xxii) 1 Data Migration

xxiii) 1 Full Solution Delivery

xxiv) 1 Project Close-Out Report

xxv) Contractor Engagement and Progress Update Sessions

3.5. Full Solution Deliverable Schedule

a) Any document required to be submitted for Phase 2 – Full Solution work will be submitted via a method to be communicated by Canada.

b) The following table identifies the dates of the deliverables identified in Section 3.4. List of Full Solution Deliverables. The deliverables must be submitted to the Technical Authority in the format and by the delivery dates specified below.

Table 2: Phase 2 – Full Solution Deliverable Schedule

Deliverable #	Description of Deliverable	Delivery Date
1.	1 Kick-off Meeting as described in section 3.2 c, i	1 week from award date of Contract Amendment to Exercise Phase 2 Work Option
2.	Contractor Engagement and Progress Update Sessions, including Progress Reports, digital copy as described in section 3.2 c iii) (G)	Monthly after award date of Contract Amendment to Exercise Phase 2 Work Option
3.	1 approved Project Schedule, digital copy as described in section 3.2 c ii) (A) 3) II	3 weeks from award date of Contract Amendment to Exercise Phase 2 Work Option
4.	1 approved Project Implementation Plan, digital copy as described in section 3.2 c ii) (A) 3)	3 weeks from award date of Contract Amendment to Exercise Phase 2 Work Option
5.	1 Proof Of Portal Staged Demonstration as described in section 3.2 c ii) (A) 4)	As depicted in the approved Project Schedule
6.	1 Project Status Reporting Plan, digital copy as described in section 3.2 c ii) (B)	As depicted in the approved Project Schedule
7.	1 Final Technical Infrastructure Design, digital copy as described in section 3.2 c ii) (C)	As depicted in the approved Project Schedule
8.	1 approved Data Migration Plan, digital copy as described in section 3.2 c ii) (E)	As depicted in the approved Project Schedule
9.	1 approved Deployment Plan, digital copy as described in section 3.2 c ii) (F)	As depicted in the approved Project Schedule
10.	1 approved Maintenance and Support Plan, digital copy as described in section 3.2 c ii) (G)	As depicted in the approved Project Schedule
11.	1 approved Backup and Disaster Recovery Plan, digital copy as described in section 3.2 c ii) (H)	As depicted in the approved Project Schedule
12.	1 approved Solution Testing and Quality Management Plan, digital copy as described in section 3.2 c ii) (I)	As depicted in the approved Project Schedule
13.	1 approved Business Intelligence Plan as described in section 3.2 c ii) (J)	As depicted in the approved Project Schedule
14.	1 approved Training Plan, digital copy as described in section 3.2 c ii) (K)	As depicted in the approved Project Schedule
15.	1 approved Solution Test Report for Full Solution Staged Demonstration Stage 1, digital copy as described in section 3.2 c ii) (I) 8)	As depicted in the approved Project Schedule
16.	1 approved Solution Test Report for Full Solution Staged Demonstration Stage 2, digital copy as described in section 3.2 c ii) (I) 8)	As depicted in the approved Project Schedule

Deliverable #	Description of Deliverable	Delivery Date
17.	1 approved Solution Test Report for Full Solution Staged Demonstration Stage 3, digital copy as described in section 3.2 c ii) (I) 8)	As depicted in the approved Project Schedule
18.	1 approved Solution Test Report for Full Solution Staged Demonstration Stage 4, digital copy as described in section 3.2 c ii) (I) 8)	As depicted in the approved Project Schedule
19.	1 approved Solution Test Report for Full Solution Staged Demonstration Stage 5, digital copy as described in section 3.2 c ii) (I) 8)	As depicted in the approved Project Schedule
20.	1 approved Exit Strategy, digital copy as described in section 3.2 c iii) (B)	As depicted in the approved Project Schedule
21.	1 approved Risk Registry, digital copy as described in section 3.2 c iii) (C)	As depicted in the approved Project Schedule
22.	1 approved Solution Support Documentation, digital copy as described in section 3.2 c iii) (D)	As depicted in the approved Project Schedule
23.	1 approved Training Materials, digital copy as described in section 3.2 c iii) (E)	As depicted in the approved Project Schedule
24.	1 Full Solution Staged Demonstration Stage 1 as described in section 3.2 c ii) (A) 5) I	As depicted in the approved Project Schedule
25.	1 Full Solution Staged Demonstration Stage 2 as described in section 3.2 c ii) (A) 5) II	As depicted in the approved Project Schedule
26.	1 Full Solution Staged Demonstration Stage 3 as described in section 3.2 c ii) (A) 5) III	As depicted in the approved Project Schedule
27.	1 Full Solution Staged Demonstration Stage 4 as described in section 3.2 c ii) (A) 5) IV	As depicted in the approved Project Schedule
28.	1 Full Solution Staged Demonstration Stage 5 as described in section 3.2 c ii) (A) 5) V	As depicted in the approved Project Schedule
29.	1 approved Requirements Compliance Document for Full Solution Staged Demonstration Stage 1, digital copy as described in section 3.2 c iii) (A)	As depicted in the approved Project Schedule
30.	1 approved Requirements Compliance Document for Full Solution Staged Demonstration Stage 2, digital copy as described in section 3.2 c iii) (A)	As depicted in the approved Project Schedule
31.	1 approved Requirements Compliance Document for Full Solution Staged Demonstration Stage 3, digital copy as described in section 3.2 c iii) (A)	As depicted in the approved Project Schedule
32.	1 approved Requirements Compliance Document for Full Solution Staged Demonstration Stage 4, digital copy as described in section 3.2 c iii) (A)	As depicted in the approved Project Schedule
33.	1 approved Requirements Compliance Document for Full Solution Staged Demonstration Stage 5, digital copy as described in section 3.2 c iii) (A)	As depicted in the approved Project Schedule
34.	1 approved Solution Administrator Training as described in section 3.2 c v)	As depicted in the approved Project Schedule

Deliverable #	Description of Deliverable	Delivery Date
35.	1 approved Data Migration as described in section 3.2 c iv)	As depicted in the approved Project Schedule
36.	Full Solution Delivery – Go live	As depicted in the approved Project Schedule
37.	1 approved Project Closeout Report, digital copy as described in section 3.2 c iii) (F)	As depicted in the approved Project Schedule

3.6. Location and Travel

a) Location of work is at the Contractor's facility. No travel is anticipated. Canada will not reimburse any travel expenses.

3.7. Solution Maintenance and Support

a) Until the completion of the warranty period, the Contractor must:

i) Track incidents and cases through their own incident management system. Provide reports on incidents/tickets and their resolution as requested by Canada and must be delivered to the requestor. The ticket should describe the issue and incidents in detail, ensure that reviews were performed corrective measures were approved, and that post-incident Quality Assurance (QA) activities were completed. Hold meetings as requested by Canada to discuss major incidents with the Solution.

ii) Ensure that the Contractor's personnel must be qualified and able to respond to client and User questions and, to the extent possible, be able to resolve User problems by telephone or email and provide advice regarding functionality, configuration, and technical issues.

iii) Must notify Canada of forthcoming changes and potential operational issues with new releases for the Solution and provide notifications to Users of any changes that may impact service.

iv) Must provide a documented, incident management procedure that includes how the Contractor will respond to incidents and issues reported by Canada.

v) Must assign an account representative as an escalation point for support and account issues.

vi) Provide Level 1-3 Support, in both of Canada's official languages, of the Full Solution along with development and support of new features and share knowledge of ongoing development Solutions and initiatives.

(A) Level 1 – Initial support for basic customer contact and triage

(B) Level 2 – More in-depth technical support for troubleshooting and analysis

(C) Level 3 – Highest level of support for handling difficult or advanced problems

vii) Include Support capabilities, including training of features and enhancements, along with any additional support that Canada may require.

3.8. Official Language Requirements and language of Work

a) The primary language of work will be in English and all reports, technical documents and project updates must be provided in English.

b) The Full Solution must allow all users to work in both of Canada's official languages (English and French). The Full Solution, including the interface, must comply with relevant policies of the Government of Canada ***Official Languages Act*** and the Directive on Official Languages for Communications and Services.

4. ADDITIONAL OPTIONAL DELIVERABLES

a) All Additional Optional Deliverables listed in this section are subject to and contingent upon, at Canada's sole discretion, Canada's decision to exercise the respective irrevocable options identified in the Contract at Part 7 – Resulting Contract Clauses, Article 7.1.2.

4.1. Optional Professional Services

a) The Contractor must provide additional Professional Services, on an as-and-when-requested basis, in accordance with the Contract, Article 7.10. Professional Services must follow the Task Authorization process in accordance with Article 7.10.12.

b) All Task Authorized work must be within the scope of the Contract. Work considered to be in accordance with the scope of the Contract may include, but is not limited to work associated with:

i) Updating the accepted Solution to accommodate changes to the Government of Canada Web Accessibility Standard Guidelines.

ii) Adding new functionalities to the accepted Solution to support changes to workflow due to policy or legislative changes.

iii) Adapting to changes in the Solution's IT environment.

iv) Migration to an alternate hosting environment in the event that Canada's business requirements change.

v) Test and Training Solution instances as and when required by Canada. In addition to the Production Instance, the following must be available:

(A) Test Instance must enable Canada to implement and test changes to the Solution prior to implementation in the Production Instance. The Test Instance must be

created on demand and be identical to the Production Instance. This instance must also be shut down and deleted on demand, for example, once new functionality has been implemented in Production.

(B) Training Instance must enable Canada to perform end user training independent of the Production Instance. The Training Instance must be created on demand and be identical to the Production Instance. This instance must also be shut down or deleted on demand, for example, once training has completed.

4.2. Optional Training Services

a) The Contractor must provide additional Training Services on an as-and-when-requested basis in accordance with the Contract, Article 7.10. Training Services must follow the Task Authorization process in accordance with Article 7.10.12 of the Contract.

b) All Task Authorized Training Services must be within the scope of the Contract. Training Services considered to be in accordance with the scope of the Contract may include, but is not limited to, Solution-relevant training for administrators, and other identified users accessing the Solution.

5. REFERENCE DOCUMENTS

- ***Accessible Canada Act*** (https://laws-lois.justice.gc.ca/eng/acts/A-0.6/)
- ***Library and Archives of Canada Act*** (https://laws-lois.justice.gc.ca/eng/acts/L-7.7/index.html);
- ***Access to Information Act*** (https://laws-lois.justice.gc.ca/eng/acts/A-1/index.html);
- ***Privacy Act*** (https://laws-lois.justice.gc.ca/eng/acts/P-21/);
- Web Experience Toolkit (https://www.canada.ca/en/treasury-board-secretariat/services/government-communications/web-experience-toolkit.html)
- Web Standards for the Government of Canada (https://www.tbs-sct.gc.ca/ws-nw/),which include:
  - Accessibility (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601)
  - Usablity (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227)
  - Branding (https://www.canada.ca/en/treasury-board-secretariat/services/government-communications/canada-content-information-architecture-specification/usage-canadaca-design.html, https://cenw-wscoe.github.io/sgdc-cdts/docs/index-en.html)
  - Interoperability (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25875)
  - Optimizing Websites and Applications for Mobile Devices (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=27088)

- Technical specifications for the Web and mobile presence (https://www.canada.ca/en/treasury-board-secretariat/services/government-communications/federal-identity-program/technical-specifications/web-mobile-presence.html)

- Policy on Government Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)
- Policy on Management of Information Technology (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12755)
- Implementing HTTPS for Secure Web Connections: Information Technology Policy Implementation Notice (ITPIN) (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html)
- Direction for Electronic Data Residency (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html)
- Directive on the Business Number (BN) (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32579)
- ***Tobacco and Vaping Products Act*** (https://laws-lois.justice.gc.ca/eng/acts/T-11.5/)
- ***Food and Drugs Act (FDA)*** (https://laws-lois.justice.gc.ca/eng/acts/F-27/)
- ***Canada Consumer Product Safety Act (CCPSA)*** (https://laws-lois.justice.gc.ca/eng/acts/C-1.68/)
- ***Official Languages Act*** (https://laws-lois.justice.gc.ca/eng/acts/O-3.01/)
- ***Directive on Official Languages for Communications and Services:***
  - http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26164
  - http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26164
- Federal Identity Program (FIP) (https://www.canada.ca/en/treasury-board-secretariat/topics/government-communications/federal-identity-requirements.html)

6. DOCUMENTS PROVIDED AT CONTRACT AWARD

Any document referenced in this document and not included in the Appendix will be provided at time of contract award or upon Canada exercising its irrevocable option on Phase 2 – Full Solution work.

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

APPENDIX A - CAPABILITY AND USABILITY ASSESSMENT (CUA)

GENERAL

Purpose

This document outlines the Capability, Usability, Accessibility, Official Languages, General Specifications, Work Plan/Workload, User Interface, and Search Assessment process***.***

Instructions

Upon the award of up to 3 Contracts, Contractors must plan, design, develop, configure, test and deliver a production quality, hosted, working prototype solution for Canada's assessment.

The Contractor must provide both support for and unrestricted access to the Prototype Solution, including all Solution usage rights grants, Software Documentation, Warranty, Hosting, Storage, and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, CUA Scenario test scripts, or other releases to Canada for up to 25 Users to use the Prototype Solution for Capability and Usability Assessment purposes during the initial contract period. These designated hands-on capability/usability assessments will be conducted by Health Canada. The testers may include inspectors and managers from the Regional Operations and Enforcement Branch (ROEB), staff from the Reports Control Division and the Compliance Division, TCD. Their structured feedback will be included in the Capability and Usability Assessment score.

Any document referenced in this document will be provided at time of contract award.

Any ***italicized*** text indicates the name of a field.

Selection of Prototype Solution

The Capability and Usability Assessment (CUA) Prototype Solution deliverables provided under the Contract will be assessed by Canada against the criteria detailed in this Appendix A Capability and Usability Assessment to Annex A – Statement of Work.

Capability and Usability Assessment (CUA) Categories

The Capability and Usability Assessment will be comprised of the following individual Assessment Categories:

Part 1: Capability Scenarios Assessment: Measures the functional technical ability of the Prototype Solution to perform and meet the specified requirements under Annex A – Statement of Work.
Part 2: General Solution Specifications Assessment: Assesses the ability of the Prototype Solution to perform and meet the requirements that are general to the entire Prototype.
Part 3: Work Plan/Workload Assessment: Assesses the ability of the Prototype Solution to perform and meet the requirements specific to work planning and workload.
Part 4: User Interface and Usability Assessment: Assesses the ability of the Prototype Solution to meet specific graphical user interface (GUI) and usability requirements.
Part 5: Search Assessment: Assesses the ability of the Prototype Solution to perform and meet the requirements specific to search capabilities.
Part 6: User Account Administration: Assesses the ability of the Prototype Solution to perform and meet the requirements specific to user account administration.
Part 7: System Usability Scale (SUS): Measures user ease-of-use within the Prototype Solution, including assessing overall user experience and satisfaction with the Prototype Solution.

Maximum Points

The maximum amount of points that can be assessed is listed in the table below:

CUA Assessment Category	Maximum Score	Percent of Total
Part 1: Capability Scenarios Assessment	**1200Points**	**45%**
Establishment Profile (225 Points)		
Compliance and Enforcement (C&E) Activity (905 Points)		
Electronic Data Submission (50 Points)		

PRE-DEFINED REPORTING AND TEMPLATES (20 POINTS)		
PART 2: GENERAL SPECIFICATIONS ASSESSMENT	**250 POINTS**	**9%**
PART 3: WORK PLAN/WORKLOAD ASSESSMENT	**50 POINTS**	**2%**
PART 4: USER INTERFACE AND USABILITY ASSESSMENT	**640 POINTS**	**24%**
PART 5: SEARCH ASSESSMENT	**160 POINTS**	**6%**
PART 6: USER ACCOUNT ADMINISTRATION ASSESSMENT	**150 POINTS**	**6%**
Part 7: System Usability Scale Assessment	**200 POINTS**	**8%**
TOTAL CUA Score:	**2650 POINTS**	**100%**

Sum of Individual Assessment Scores

The sum of the scores for each individual Assessment Category will be calculated in accordance with the assessment criteria and maximum points listed in each category of this Appendix A Capability and Usability Assessment to Annex A – Statement of Work to arrive at the total CUA Score for the Prototype Solution.

Ranking of Prototype Solution

The top ranked Prototype Solution will be determined based on the highest responsive combined rating of technical merit, price, and CUA.

- 10% weighting will be given to the Technical Evaluation Score from the Bid Evaluation.
- 20% weighting will be given to the Financial Evaluation Score from the Bid Evaluation.
- 70% weighting will be given to the CUA Score, as per the following table:

ASSESSMENT	WEIGHTING
TECHNICAL EVALUATION SCORE	**10%**
FINANCIAL EVALUATION SCORE	**20%**
CAPABILITY AND USABILITY ASSESSMENT SCORE	**70%**

In the event of a tie, the CUA Score will be used to rank the Contractors from highest to lowest score. If there are further ties, the lowest Financial Score will be used to rank the Contractor.

Canada, at its discretion, will exercise its irrevocable option to select a Contractor to perform all or a portion of the Work under article 3. Phase 2 - Solution of Annex A – Statement of Work.

Canada may also, at its discretion, exercise its irrevocable option with other Contractors who participated in the CUA for all or a portion of the Work if it is determined that this would best meet the needs of Canada.

PART 1: CAPABILITY SCENARIOS ASSESSMENT

CAPABILITY AND USABILITY ASSESSMENT – PART 1: CAPABILITY SCENARIOS ASSESSMENT

LEGEND

Did Not Demonstrate = 0 Points – Prototype Solution does not demonstrate capability and functionality requirements.

Partially Demonstrated = 1 (or 10) Points – Prototype Solution has minimal capability and has demonstrated more than two deficiencies in meeting the requirements.

Mostly Demonstrated = 3 (or 30) Points – Prototype Solution has high degree of capability and has demonstrated no more than one deficiency in meeting the requirements.

Fully Demonstrated = 5 (or 50) Points – Prototype Solution fully meets all requirements. Prototype Solution has not demonstrated any deficiencies in meeting the requirements.

Scenario include:

a. Establishment Profile
b. Compliance and Enforcement (C&E) Activity
c. Electronic Data Submission
d. Pre-defined Reporting and Templates.

Establishment Profile

Scenario 1. **Create Establishment Profile**

SCENARIO #1 – Create Establishment Profile

Context

The User has identified the need to create a "Convenience Store" type of "Retailer" establishment within their assigned region. The establishment has a business address and a mailing address, and two contacts, one of whom is the owner. The User wants to include comments regarding the establishment prior to confirming and saving the new establishment profile.
A new draft activity is automatically created when the new establishment profile information is confirmed.

The Prototype Solution should have the functionality for the User to:

1. Select the "Create New Establishment Profile" function.
2. Enter the establishment field set information, including the name and address of the establishment.
3. Initiate the address validation function.
4. Have the option to correct an invalid address, as required.
5. Initiate the establishment duplicate check function.
6. Have the option to identify potential matching establishment profile(s) and views the details of any potential match as required.
7. Confirm the establishment profile is not a duplicate.
8. Enter values for all remaining mandatory information as required for the establishment type.
9. Enter values for all optional information according to establishment type, as required.
10. Save the completed establishment profile.
11. Enter the establishment create reason.
12. Confirm the new establishment profile.
13. Exit the "Create New Establishment Profile" function.
14. The prototype solution creates an activity for the newly created and confirmed establishment.

Create Establishment Profile – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (10)	Mostly Demonstrated (30)	Fully Demonstrated (50)
	The Prototype Solution should have the functionality:				
1.	**Create New Establishment Profile** To provide a new establishment "tabbed pane" for the User to create a new establishment profile record and enter all information relating to the new establishment (as described in Part 4: User Interface and Usability Assessment, Indicator 35).	O			O
2.	**Workflow Steps to Create a New Establishment Profile record** To move the User through the following establishment business process workflow steps to create a new establishment profile record: a. Enter establishment information for the fields in the Establishment field set and related fields, including all mandatory information. b. Existing Establishment Verification that the mandatory establishment profile data is not the same as an existing establishment profile data. c. Continue to enter the establishment profile information.	O	O	O	O

	The outcome of this requirement is based on the cumulative result of indicators 3 to 12 below. **0** ***Points Did Not Demonstrate (Scored 0 points on indicators 3-12)*** ***10 Points Partially Demonstrated (Scored 1-29 points on indicators 3-12)*** ***30 Points Mostly Demonstrated (Scored 30-49 points on indicators 3-12)*** ***50 Points Fully Demonstrated (Scored 50 points on indicators 3-12)***				
	Score for Indicators 1 and 2:				**/100**
	Scoring for indicators 3 to 12 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
3.	**Establishment Information Component** To provide an Establishment Information component of the Establishment "tabbed pane" for the User to enter, update, and view all data (as described in Part 4: User Interface and Usability Assessment, Indicator 36.	O			O
4.	**New Establishment Information** To prevent the User from entering additional establishment information for a physical address until the Existing Establishment Verification has been completed.	O			O
5.	**Existing Establishment Verification** For the User to perform a search on the existing establishments profiles to verify the uniqueness of the new establishment profile.	O			O
6.	**Establishment Verification – Next Components** To provide the following components of the Establishment "tabbed pane" for the User to enter, update, and view all data when the establishment has been verified as unique (as described in Part 4: User Interface and Usability Assessment, Indicator 35): a. Concerns and Issues (as described in Part 4: User Interface and Usability Assessment, Indicator 37). b. Contacts (as described in Part 4: User Interface and Usability Assessment, Indicator 38). c. Associated Activities (as described in Part 4: User Interface and Usability Assessment, Indicator 39). d. Comments (as described in Part 4: User Interface and Usability Assessment, Indicator 40).	O			O
7.	**Associate an Establishment** For the User to associate (link) an existing establishment to the selected establishment.	O			O
8.	**Remove Associated Establishment** For the User to remove an associated (linked) establishment from the selected establishment.	O			O
9.	**Concerns and Issues Component** For the User to enter concerns and issues information for the establishment.	O			O

10.	**Contacts Component** For the User to enter contact information for the establishment.	O			O
11.	**Comments Component** For the User to enter comments concerning the establishment.	O			O
12.	**Establishment Create/Update Reason** For the User to perform the following actions when prompted by the Prototype Solution: a. Select the value "New Establishment" for ***Reason for Establishment Create/Update.*** b. Enter the ***Background*** value (description of reason). c. Confirm the establishment profile information is complete.	O			O
Score for Indicators 3 to 12:					**/50**
Scoring for indicator 13 below:		**Did Not Demonstrate (0)**	**Partially Demonstrated (10)**	**Mostly Demonstrated (30)**	**Fully Demonstrated (50)**
13.	**Create New Activity Associated with New Establishment Profile** To provide an activity "tabbed pane" for the User to enter all information relating to a new activity record when a new establishment profile is confirmed as complete (as described in Part 4: User Interface and Usability Assessment, Indicator 43).	O			O
Score for Indicator 13:					**/50**
Scoring for indicators 14 to 16 below:		**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
14.	**Populate New Activity with Default Values** To populate the following fields in the new activity record with the following values: a. ***Activity Reason Type*** to "Scheduled: Workplan"; b. ***Activity Type*** to "Inspection"; c. ***Priority*** to "Normal".	O			O
15.	**Associate New Activity with New Establishment Profile** To associate the new activity record with the new establishment profile.	O			O
16.	**Establishment Comments** To copy values entered into the ***Establishment Comments*** field during the creation of a new establishment profile record into the ***Activity Comments History*** field upon the creation of the new activity.	O			O
Score for Indicators 14 to 16					**/15**
Scenario 1. Create Establishment Profile Total Score:					**/215**

Scenario 2. **Update Establishment Profile**

SCENARIO #2 – Update Establishment Profile

Context

The User has identified the need to update a "Convenience Store" type of "Retailer" establishment within their assigned region. The User wants to update the address and a contact associated with the establishment.

A new draft activity is automatically created when the updated establishment profile information is confirmed.

The Prototype Solution should have the functionality for the User to:

1. Search for the establishment.
2. Select the establishment for updating from the search results.
3. Update the establishment information as applicable.
4. Initiate the address validation function, if the address was modified.
5. Have the option to correct an invalid address, as required.
6. Initiate the establishment duplicate check function, if the address was modified.
7. Have the option to identify potential matching establishment profile(s) and views the details of any potential match as required.
8. Confirm the establishment profile is not a duplicate.
9. Save the completed establishment profile.
10. Enter the establishment update reason.
11. Confirm the updated establishment profile.
12. Exit the "Establishment Profile".
13. The prototype solution creates an activity for the updated and confirmed establishment.

Update Establishment Profile – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should have the functionality:				
1.	**Update Establishment Profile** For the User to update an existing establishment profile record (as assessed in Scenario 2, Indicators 5 to 8, below).				
2.	**Perform a Pre-defined Establishment Profile Search** For the User to perform a pre-defined Establishment Profile Search (as assessed in Part 1: Capability Scenarios Assessment, Scenario 3, Indicator 1).				
3.	**Select an Existing Establishment** For the User to select an establishment from the pre-defined Establishment Profile Search results list (as assessed in Part 1: Capability Scenarios Assessment, Scenario 3, Indicator 2).				
4.	**Update Establishment Profile Information** For the User to update establishment profile information (as assessed in Part 1: Capability Scenarios Assessment, Establishment Profile, Scenario 1, Indicators 3 to 11).				
5.	**Create/Update Establishment Reason** For the User to perform the following actions when prompted by the Prototype Solution: a. Select the value "Update of Establishment Profile" for ***Reason for Establishment Create/Update*** b. Enter background text. c. Confirm the updated establishment profile information is complete.	O	O	O	O

6.	**Create New Activity to be Associated with Updated Establishment Profile** To provide an activity "tabbed pane" for the User to enter all information relating to a new activity record when an updated establishment profile is confirmed as complete (as assessed in Part 1: Capability Scenarios Assessment, Scenario 1, Indicator 13).				
7.	**Populate New Activity with Default Values** To populate the following fields in the new activity record with the following values as follows: a. ***Activity Reason Type*** to "Unscheduled: Update of Establishment Profile"; b. ***Activity Type*** to "Inspection"; c. ***Priority*** to "Normal".	O	O	O	O
8.	**Associate New Activity with Updated Establishment Profile** To associate the new activity record with the updated establishment profile (as assessed in Part 1: Capability Scenarios Assessment, Scenario 1, Indicator 15).				
Scenario 2. Update Establishment Total Score:		**/10**			

Establishment Profile: Scenarios 1 and 2 Total Score:	**/225**

Compliance and Enforcement (C&E) Activity

C&E Activity – On-site Retail Inspection - Overview

C&E Activity – On-site Retail Inspection Overview

Context

An Inspector needs to create a new C&E activity to add to his/her own workload as part of workload planning. The new activity will involve planning and documenting an inspection at the premises of an establishment. The activity is part of the inspector's annual inspection plan. The establishment's location is in the same region as the inspector. At the previous inspection, the establishment was selling both tobacco and vaping products. The inspector will plan, conduct, and document the inspection activity following the procedures outlined in the Tobacco Control Directorate's (TCD) Procedures for Inspection document.

Prior to conducting the inspection, the inspector should review all aspects of the selected establishment's profile and history stored in the solution, including previous activities, before the inspector can proceed to entering inspection activity information. The inspector will plan the inspection to take place the following week. The scope of the inspection will be a general inspection that, by default, should encompass all legislative sections/subsections of the Tobacco and Vaping Products Act (TVPA), and specific legislation of the Canada Consumer Product Safety Act (CCPSA) and the Food and Drugs Act (FDA).

During the inspection at the establishment's premises, the inspector should verify the establishment's location, record the person spoken to, verify the establishment's profile information with the person spoken to, and update the profile information stored in the solution as necessary. The inspector should follow steps outlined in the appropriate procedures/guidelines/tools to perform the inspection and document information gathered during the on-site inspection.

After conducting the on-sight inspection, the inspector should document the outcomes/results of analysis performed on the gathered information. The inspector will determine and document the state of compliance of the establishment based on the assessment of relevant outcomes/results.

After the assessment of compliance is completed the inspector will determine, based on the state of compliance, if an enforcement action is required. The inspector should document all information of the selected enforcement action(s) if required, and its implementation.

Once all documentation on the enforcement action(s) is completed, the inspector will close the activity.

Because the C&E Activity scenario involves many processes and steps, this scenario has been broken down into separate scenarios as follows:

- Scenario 3 - Create and Initialize a New activity
- Scenario 4 - Select the Scope of the Activity
- Scenario 5 - Document the Onsite portion of the activity
- Scenario 6 - Document Compliance Assessment and Analysis
- Scenario 7 - Document Enforcement Actions
- Scenario 8 - Close Activity

The Prototype Solution should have the functionality for the User to:

1. Create and initialize a new activity:
   (i) Search for and select an establishment to connect to the new activity.
   (ii) Review all aspects of the establishment's history stored in the solution, including previous activities.
   (iii) Plan the inspection by completing, at a minimum, the mandatory information.

(iv) Select a General scope for the inspection.
(v) De-select any legislative section(s)/subsection(s) that will not be assessed during the inspection.

2. Document the onsite inspection:
   (i) Verify the establishment's location.
   (ii) Record the name of all people spoken to during the inspection.
   (iii) Verify the establishment's profile information with that stored in the solution, and update the profile information as necessary.
   (iv) Document information gathered during the on-site inspection.
3. Document compliance analysis and assessment results:
   (i) Document the outcomes/results of analysis performed on the gathered information.
   (ii) Determine and document the state of compliance of the establishment based on the assessment of relevant outcomes/results.
4. Document Enforcement Actions:
   (i) Determine, based on the state of compliance, if an enforcement action is required.
   (ii) If an enforcement action is required, document all information of the selected enforcement action and its implementation.
5. Close the activity.

Scenario 3. **C&E Activity - Create a New Activity**

SCENARIO #3 - C&E Activity - Create and Initialize a New Activity

Context

An Inspector needs to create a new activity to add to their own workload as part of workload planning. The activity is part of the inspector's annual inspection plan. The establishment's location is in the same region as the inspector and, at the previous inspection, was selling both tobacco and vaping products. The inspector will plan the activity.

During the creation of the activity, the inspector should review all aspects of the selected establishment's profile and history stored in the solution, including previous activities, before the inspector can proceed to entering the initial inspection activity information. The inspector will plan the inspection to take place during the following week.

The Prototype Solution should have the functionality for the User to:

1. Search for and select an establishment to connect to the new activity.
2. Review all aspects of the establishment's history stored in the solution, including previous activities.
3. Plan the inspection by completing, at a minimum, the mandatory information.

C&E Activity - Create and Initialize a New Activity – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality for the User to:				
1.	**Perform a Pre-defined Establishment Profile Search** For the User to perform a pre-defined Establishment Profile Search (as described in Part 5: Search Assessment, Indicator 2. Establishment Profile Search), to find an	O			O

	establishment that matches the following criteria to connect to a new activity: a. An ***Establishment Status*** value of "Active"; b. An ***Establishment Type*** value of "Retailer"; c. An ***Establishment Subtype*** value of "Convenience Store".				
2.	**Select an Existing Establishment** For the User to: a. Select an establishment from the pre-defined Establishment Profile Search results list to connect with a new activity (as described in Part 4: User Interface and Usability Assessment, Indicator 29) b. To add the new activity to the User's Workload Overview (dashboard).	O			O
3.	**Create New Activity Associated with an Existing Establishment** To provide an activity "tabbed pane" for the User to enter all information relating to a new activity record associated with an existing establishment with an ***Establishment Status*** value of "Active" (as assessed in Part 1: Capability Scenarios Assessment, Scenario 1, Indicator 13).				
4.	**General Information Component** To provide a General Information component of the Activity "tabbed pane" for the User to enter, update, and view all data (as described in Part 4: User Interface and Usability Assessment, Indicator 44).	O			O
	Score for Indicators 1-4:				**/15**
	Scoring for Indicator 5 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (10)**	**Mostly Demonstrated (30)**	**Fully Demonstrated (50)**
5.	**Workflow Steps to Enter New Activity Information** To move the User through the following activity workflow steps to enter information for new activity: a. View detailed profile information for the selected establishment (Scenario 3, Indicator 6). b. Update concerns and issues (Scenario 3, Indicator 7). c. Update establishment contact information (Scenario 3, Indicator 8). d. Confirm the review of establishment information is complete (Scenario 3, Indicator 9 and 10). e. View detailed information about an establishment associated with the selected establishment (if any) (Scenario 3, Indicator 11). f. View detailed information about an activity connected to the selected establishment (if any) (Scenario 3, Indicator 12). g. Confirm the review of the associated establishments and the review of the establishment activity history information is complete (Scenario 3, Indicator 13). h. Enter activity information into the Core Information and remaining field sets (Scenario 3, Indicator 15). i. Confirm the activity information is complete (Scenario 3, Indicator 16).	O	O	O	O

	Score for this indicator will be based on the cumulative score of the indicators 6-17 specified for each workflow step and the sequence as specified in this requirement. **0** ***Points Did Not Demonstrate (Scored 0 points on indicators 6-17)*** ***10 Points Partially Demonstrated (Scored 1-35 points on indicators 6-17)*** ***30 Points Mostly Demonstrated (Scored 36-59 points on indicators 6-17)*** ***50 Points Fully Demonstrated (Scored 60 points on indicators 6-17)***				
	Score for Indicator 5:				**/50**
	Scoring for Indicators 6 to 17 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
6.	**View Entire Establishment Profile from Activity General Information** For the User to view from the Establishment field set the entire profile information for the selected establishment (as described in Part 4: User Interface and Usability Assessment, Indicator 44).	O			O
7.	**Update the Concerns and Issues** For the User to update the concerns and issues connected with the selected establishment profile in the Establishment field set in the General Information component (as described in Part 4: User Interface and Usability Assessment, Indicator 38).	O			O
8.	**Update Contact Information** For the User to update contact information connected with the selected establishment profile, in the Establishment Contacts field set in the General Information component (as described in Part 4: User Interface and Usability Assessment, Indicator 39).	O			O
9.	**Confirm Review of Establishment and Establishment Contacts** To require the User to confirm the review of the selected establishment and establishment contacts information is complete in the General Information component.	O			O
10.	**Enable Associated Establishments and other Activities Field Sets** For the User to view the following information in the Associated Establishments field set and in the Other Activities for this Establishment field set in the General Information component (as described in Part 4: User Interface and Usability Assessment, Indicator 44), when the review of the establishment and establishment contacts information has been confirmed as complete by the User: a. All establishments associated with the selected establishment, if any. b. All activities connected to the selected establishment, if any.	O	O		O

	0 Points if none of the listed actions are demonstrated ***1 Point if one of the listed actions is demonstrated*** ***5 Points if both of the listed actions are demonstrated***				
11.	**Associated Establishments Field Set** For the User to select and view, in the Associated Establishments field set in the General Information component, information about an establishment associated with the selected establishment, if any (as described in Part 4: User Interface and Usability Assessment, Indicator 44).	O			O
12.	**Other Activities for this Establishment Field Set** For the User to select and view, in the Other Activities for this Establishment field set in the General Information component, information about an activity connected to the selected establishment, if any (as described in Part 4: User Interface and Usability Assessment, Indicator 44).	O			O
13.	**Confirm Review of Information** To limit the User from moving to the next workflow step until the User confirms the review of the information in the Associated Establishments and the Other Activities for this Establishment field sets in the General Information component is complete.	O			O
14.	**Activity Related Information Field Sets** **For the User to input and view the following activity related information field sets and fields in the General Information component, when the review of the information in the Associated Establishments field set and in the Other Activities for this Establishment field set has been confirmed as complete by the User (as described in Part 4: User Interface and Usability Assessment, Indicator 44):** **a. Core Information:** **i. Activity Reason Type;** **ii. Activity Type;** **iii. Priority.** b. Activity Timeline: i. ***Proposed Start Date;*** ii. ***Bring Forward Date.*** c. Sent To History (viewing only); d. Online Presence; e. Links; f. Comment History. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
15.	**Enter Activity Information**	O	O	O	O

	For the User to enter the following activity values into the following field sets and fields in the General Information component: a. Core Information: i. ***Activity Reason Type: "Scheduled: Workplan"*** (required); ii. ***Activity Type***: "Inspection" (required). b. Activity Timeline: i. ***Proposed Start Date***: [any date value] (required). c. Online Presence; d. Links; e. Comment History. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***				
16.	**Confirm General Information is Complete** To limit the User from moving to the next workflow step until the User confirms that the entry of the initial information for the new activity in the General Information component is complete.	O			O
17.	**Set Values and Enable Next Components in Workflow** **To perform the following actions when the information in the General Information component of the new activity has been confirmed by the User and successfully verified as complete:** **a. Set the following fields to the following values:** **i. Activity Status value to "Planning in Progress";** **ii. Activity Plan Status Type value to "Draft Plan";** **iii. Priority value to "Normal".** b. Set the mandatory field values to read-only; c. Add the new activity to the User's "Activities" list in the My Workload field set of the Workload Overview (dashboard); d. Enable for input and viewing the following components of the Activity "tabbed pane": ***i. Scope Plan;*** ii. ***Cl***ose. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are***	O	O	O	O
	Score for Indicators 6 to 17				**/60**

Scenario 3. Create and Initialize a New Activity Total Score:	**/125**

Scenario 4. **C&E Activity - Select Scope of Activity**

SCENARIO #4 - C&E Activity - Select Scope of Activity

The scope of the inspection will be a general inspection that, by default, should encompass all legislative sections/subsections of the Tobacco and Vaping Products Act (TVPA), and specific legislation of the Canada Consumer Product Safety Act (CCPSA) and the Food and Drugs Act (FDA).

The Prototype Solution should have the functionality for the User to:

1. Select a General scope for the inspection.
2. De-select any legislative section(s)/subsection(s) that will not be assessed during the inspection.

C&E Activity - Select Scope of Activity – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should have the functionality for the User to:				
1.	**Scope Plan Component** To provide a Scope Plan component of the Activity "tabbed pane" for the User to enter, update, and view all data (as described in Part 4: User Interface and Usability Assessment, Indicator 45).				
2.	**Activity Scope Plan Type** For the User to select an ***Activity Scope Plan Type*** value of "General" in the Scope Plan component to create a scope plan.	O			O
3.	**Legislative Section/Subsection** To display in the Activity Scope Details field set the ***Legislative Section/Subsection*** values depending on values previously populated in the following activity field values when the User selects an ***Activity Scope Plan Type*** value of "General": a. ***Activity Scope Plan Type*** value of "General"; b. ***Establishment Type*** value of "Retailer"; c. ***Activity Reason Type*** value of "Scheduled: Workplan"; d. ***Proposed Start Date*** value entered when the activity was created. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than three of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
4.	**Default Selected State**	O			O

	To set all ***Legislative Section/Subsection*** value(s) associated with the selected ***Activity Scope Plan Type*** value to a "selected" state when the ***Activity Type*** value is "Inspection" and the ***Activity Scope Plan Type*** value is "General".				
5.	**Select /De-select Legislative Section/Subsection** For the User to select and de-select any available ***Legislative Section/Subsection*** values listed in the Activity Scope Details field set at any time prior to confirming the information in the Scope Plan is complete.	O			O
6.	**Minimum Legislative Section/Subsection** To verify a minimum of one ***Legislative Section/Subsection*** value has been selected before the User can confirm the Scope Plan is complete.	O			O
7.	**Confirm Scope Plan as Complete** To limit the User from moving to the next workflow step until the User confirms the information in the Scope Plan component is complete.	O			O
8.	**Set Values and Enable Next Components in Workflow** To perform the following actions when the information in the Scope Plan component has been confirmed by the User, and successfully validated and verified as complete: a. Set the ***Activity Status*** value to "Pending Compliance"; b. Set the Ac***tivity Plan Status Type*** value to "Approved"; c. Set all Scope Plan field values to read-only; d. Enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane" and the fields in the Establishment Location Verification field set. ***0 Points if none of the listed actions are demonstrated*** ***1 Points if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than three of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
Scenario 4. Select Scope of Activity Total Score:					**/35**

Scenario 5. **C&E Activity - Document Onsite Portion of the Activity**

SCENARIO #5 - C&E Activity - Document Onsite Portion of the Activity

Context

During the inspection at the establishment's premises, the inspector should verify the establishment's location, record the person spoken to, verify the establishment's profile information with the person spoken to, and update the profile information stored in the solution as necessary.

The Prototype Solution should have the functionality for the User to:

Document the on-site inspection in the following steps:
1. Verify the establishment's location.
2. Record the name of all people spoken to during the inspection.
3. Verify the establishment's profile information with that stored in the solution.
4. Update the profile information as necessary.

C&E Activity - Document Onsite Portion of the Activity – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality:				
1.	**Compliance Assessment Component** To provide the following field sets for the User to enter, update, and view all data in the Compliance Assessment component of the Activity "tabbed pane" (as described in Part 4: User Interface and Usability Assessment, Indicator 46): a. Establishment Location Verification; b. Person Spoken To.				
	Scoring for Indicator 2 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (10)**	**Mostly Demonstrated (30)**	**Fully Demonstrated (50)**
2.	**Guided Workflow Steps for Compliance Assessment Component – Establishment Location Verification Field Set** To move the User through the following workflow steps to document the Establishment Location Verification field set of compliance assessment (as described in Part 4: User Interface and Usability Assessment, Indicator 49): a. Verify establishment location (Scenario 5, Indicators 3 and 4). b. Confirm establishment location verification is complete (Scenario 5, Indicator 5). c. Document person spoken to (Scenario 5, Indicator 7). d. Confirm establishment profile information was verified (Scenario 5, Indicator 8 and 9). Score for this indicator will be based on the cumulative score of the Indicators 3-9 specified for each workflow step and the sequence as specified in this requirement. ***0 Points Did Not Demonstrate (Scored 0 points on indicators*** 3-9***)*** ***10 Points Partially Demonstrated (Scored 1-20 points on indicators*** 3-9***)*** ***30 Points Mostly Demonstrated (Scored 21-34 points on indicators*** 3-9***)*** ***50 Points Fully Demonstrated (Scored 35 points on indicators*** 3-9)	O	O	O	O
	Score for Indicator 2:				**/50**

	Scoring for Indicators 3 to 9 below:	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
3.	**Compliance Assessment Component - Establishment Location** For the User to select the ***Activity Establishment Verification Code*** value of "Establishment Verified At Specified Location" in the Establishment Location Verification field set in the Compliance Assessment component (as described in Part 4: User Interface and Usability Assessment, Indicator 49).	O			O
4.	**Compliance Assessment Component – Actual Date and Time** For the User to enter the ***Actual Start Date*** and ***Actual Start Time*** values in the Establishment Location Verification field set in the Compliance Assessment component.	O			O
5.	**Establishment Location Verification** To limit the User from moving to the next workflow step until the User confirms when finished entering information in the Establishment Location Verification field set in the Compliance Assessment component.	O			O
6.	**Establishment Location Verification - Confirm location is verified** **To perform the following actions:** **a. Set all field values in the Establishment Location Verification field set to read-only.** **b. Set the following fields to the following values:** **i. Activity Status value to "Compliance In Progress";** **ii. Activity Plan Status Type value to "Approved".** **c. Enable for input and viewing the following field sets and fields of the Compliance Assessment component:** **i. Person Spoken To;** **ii. Add Person Spoken To;** **iii. Establishment Profile Verified (field).** When the entry of information in the Establishment Location Verification field set of the Compliance Assessment component is confirmed as complete by the User and the ***Activity Establishment Verification Code*** value has been set to "Establishment Verified at Specified Location". ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are***	O	O	O	O
7.	**Compliance Assessment Component - Person Spoken To**	O	O		O

	For the User to perform the following actions in the Person Spoken To field set in the compliance Assessment component (as described in Part 4: User Interface and Usability Assessment, Indicator 50): a. Select a minimum of one person spoken to as the contact; b. Add a new establishment contact to the contact list connected to the establishment profile. ***0 Points if neither of the listed actions is demonstrated*** ***1 Point if only one of the actions is demonstrated*** ***5 Points if both of the listed actions are demonstrated***				
8.	**Compliance Assessment Component – Verify Establishment Profile** To limit the User from moving to the next workflow step in the Compliance Assessment component until the User confirms the establishment profile information has been verified and updated.	O			O
9.	**Set Values and Enable Next Field Sets in Workflow** To input, update, and view the following field sets in the Compliance Assessment component, (as described in Part 4: User Interface and Usability Assessment, Indicator 46) when the establishment profile information is confirmed as verified by the User: a. Compliance Results; b. Artifacts Summary; c. Responsible Party Summary.	O			O
Score for Indicators 3 to 9:					**/35**
Scenario 5. Document Onsite Portion of the Activity Total Score:					**/85**

Scenario 6. **C&E Activity - Document Compliance Assessment and Analysis**

SCENARIO #6 - C&E Activity - Document Compliance Assessment and Analysis

Context

After conducting the on-sight inspection, the inspector should document the results of the compliance assessments and analysis performed on the gathered information. The inspector will determine and document the state of compliance of the establishment based on the assessment of relevant outcomes/ results.

The Prototype Solution should have the functionality for the User to:

1. Document the outcomes/results of analysis performed on the gathered information.
2. Determine and document the state of compliance of the establishment based on the assessment of relevant outcomes/results.

C&E Activity - Document Compliance Assessment and Analysis – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (10)	Mostly Demonstrated (30)	Fully Demonstrated (50)
	The Prototype Solution should provide the functionality:				
1.	**Compliance Results Field Set** To provide a Compliance Assessment component of the Activity "tabbed pane" for the User to enter, update, and view compliance results information (as described in Part 4: User Interface and Usability Assessment, Indicator 51).				
2.	**Populate Compliance Results Field Set** To populate the ***Legislation*** field in the Compliance Results field set with all ***Legislative Section/Subsection*** values previously selected in the Scope Plan component (as described in Part 4: User Interface and Usability Assessment, Indicator 52).	O			O
3.	**Guided Workflow Steps to Document Compliance Assessment and Analysis Portion** **To move the User through the following workflow steps to document the Compliance Assessment and Analysis Portion of compliance assessment:** **a. Document compliance assessment results by legislative section/subsection:** **i. Document Artifact Collection (Scenario 6, Indicator 10).** **ii. Document Artifact Analysis results for each legislative section/subsection for the artifact (Scenario 6, Indicator 11 and 12).** **iii. Document the responsible party for each non-**compliant legislative section/subsection in the artifact analysis (Scenario 6, Indicator 13). iv. Document Linked files (Scenario 6, Indicator 14). b. Update Compliance Result data set. (Scenario 6, Indicator 4, 5, and 6). c. View and update details of an artifact from the Artifacts Summary field set. (Scenario 6, Indicators 17, 18 and 19). d. View and update details of a responsible party from the Responsible Party Summary field set. (Scenario 6, Indicators 20, 21 and 22). e. Confirm Compliance Assessment information is complete. (Scenario 6, Indicator 23). **Score for this indicator will be based on the cumulative score of the indicators 6-17 specified for each workflow step and the sequence as specified in this requirement.** 0 ***Points Did Not Demonstrate (Scored 0 points on indicators 4-24)*** ***10 Points Partially Demonstrated (Scored 1-62 points on indicators 4-24)*** ***30 Points Mostly Demonstrated (Scored 63-104***	O	O	O	O

	50 Points Fully Demonstrated (Scored 105 points on indicators 4-24)				
	Score for Indicators 1 to 3:				**/100**
	Scoring for Indicator 4 to 24 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
4.	**Legislation Section Compliance Outcome** For the User to select one of the following ***Legislation Section Compliance Outcome*** values for a ***Legislative Section/Subsection*** value listed in the Compliance Results field set where compliance analysis is not required: a. "Not Inspected"; b. "Not Applicable".	O			O
5.	**Artifact Analysis Type** For the User to select the ***Artifact Analysis Type*** value of "Observation" for a ***Legislative Section/Subsection*** value when compliance assessment is required for a ***Legislative Section/Subsection*** value listed in the Compliance Results field set.	O			O
6.	**Add an Artifact** For the User to select to add an artifact for the ***Legislative Section/Subsection*** value that has the ***Artifact Analysis Type*** value of "Observation".	O			O
7.	**Legislation Section Compliance Outcome Read-only** To set the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value in the Compliance Results field set as read-only when an artifact has been added.	O			O
8.	**Artifact "Tabbed pane"** To provide an Artifact "tabbed pane" for the selected ***Artifact Analysis Type*** value for the User to enter, update, and view all data (as described in Part 4: User Interface and Usability Assessment, Indicator 52).	O			O
9.	**Artifact "Tabbed pane" Header Information** To populate the following artifact field values in the header field set of the Artifact "tabbed pane" (as described in Part 4: User Interface and Usability Assessment, Indicator 53): a. ***Establishment Name*** value is "[***Establishment Name*** value for the activity]". b. ***Artifact Id*** value is "[system generated by concatenating system generated number + Legislation number + number of artifact for this Legislative section/subsection, starting at the number 1]". c. ***Legislation Section/Subsection*** value is "[value previously selected in the Compliance Assessment field set for which the artifact is being assessed]***".*** d. ***Artifact Analysis Type*** is "[value previously selected by the User in the Compliance Assessment field set]". ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than one of the listed actions are demonstrated***	O	O	O	O

	3 Points if no fewer than three of the listed actions are demonstrated ***5 Points if all of the listed actions are demonstrated***				
10.	**Artifact "Tabbed pane": Collection Component** For the User to enter the following artifact collection information values for the following fields in the Collection component of the Artifact "tabbed pane" (as described in Part 4: User Interface and Usability Assessment, Indicator 54) when the ***Artifact Analysis Type*** value is "Observation": a. ***Artifact Id:*** "1"; b. ***Description:*** "[any text]"; c. ***Observed By***: "[accept the default value of the User's name]"; d. ***Observed Date***: "[any date <= system date]". ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***3 Points if no fewer than three of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
11.	**Select Overall Compliance Assessment Outcome** For the User to select the ***Overall Artifact Compliance Assessment Outcome*** value for the artifact when the artifact is assessed against only one ***Legislative Section/S/subsection*** value,	O			O
12.	**Artifact "Tabbed pane": Analysis Component** For the User to enter the following artifact analysis information values for the fields in the Analysis component of the Artifact "tabbed pane" (as described in Part 4: User Interface and Usability Assessment, Indicator 55), when the ***Artifact Analysis Type*** value is "Observation": a. ***Analysis Comments***: [any text]; b. ***Overall Artifact Compliance Outcome***: "Non-Compliance"; c. ***Contact***: [select a name from the provided Contact list]. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***3 Points if no fewer than two of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
13.	***Responsible Party*** For the User to select a ***Full Name*** value name from the list of contacts associated with the establishment profile as the ***Responsible Party*** for each ***Legislative Section/Subsection***	O			O

	value listed in the Analysis component where non-compliant is indicated.				
14.	**Artifact "Tabbed pane": Links Component** For the User to enter the following linked document information values for the fields in the Linked component of the artifact (as described in Part 4: User Interface and Usability Assessment, Indicator 56): a. ***Link Id Number***: "1", combination of a unique number generated by the Prototype Solution plus the User updateable number. The Solution generated portion of the Id cannot be changed by the User. b. ***File name***: [any document file name], name of the document being linked; c. ***Description***: [description of the linked document]; d. ***Linked By***: [defaults to User name], the name of the User who linked the file; e. ***Linke***d ***Date***: [any date <= system date], the date the file was linked. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
15.	**Derive and Display Legislation Section Compliance Outcome** To derive and display in the Compliance Results field set the ***Legislation Section Compliance Outcome*** value for each ***Legislative Section/Subsection*** value derived from the ***Overall Artifact Compliance Outcome*** value of each artifact added to the legislative section/subsection, as follows: a. If the ***Overall Artifact Compliance Outcome*** value for any artifact is "Non-Compliance", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "Non-Compliance". b. If no artifact has an ***Overall Artifact Compliance Outcome*** value of "Non-Compliance" and the ***Overall Artifact Compliance Outcome*** value for at least one artifact is "No Evidence of Non-Compliance", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "No Evidence of Non-Compliance". c. If the ***Overall Artifact Compliance Outcome*** value for all artifacts is "Not Applicable", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "Not Applicable". d. If the ***Overall Artifact Compliance Outcome*** value for all artifacts is "Not Inspected", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "Not Inspected".	O			O

	0 Points if none of the listed values are derived and displayed ***5 Points if the correct value is derived and displayed***				
16.	**Total Number of Artifacts** To display the value for the total number of artifacts added to each legislative section/subsection in the Compliance Results field set.	O			O
17.	**Artifact Summary** To populate and display details of each added artifact in the Artifacts Summary field set in the Compliance Assessment component (as described in Part 4: User Interface and Usability Assessment, Indicator 57).	O			O
18.	**Update an Artifact** For the User to select and update a previously documented artifact from the Artifacts Summary field set.	O			O
19.	**Delete an Artifact** For the User to select and delete a previously documented artifact and all related artifact information from the Artifacts Summary field set.	O			O
20.	**Responsible Party Summary** To populate and display details of each added responsible party in the Responsible Party Summary field set in the Compliance Assessment component (as described in Part 4: User Interface and Usability Assessment, Indicator 58).	O			O
21.	**Update Responsible Party** For the User to select, update, and view a previously documented Responsible Party from the Responsible Party Summary field set.	O			O
22.	**Delete Responsible Party** For the User to select and delete a previously documented Responsible Party and all related artifact information from the Responsible Party Summary field set.	O			O
23.	**Confirm Compliance Assessment is Complete** **To require the User to confirm the information in the Compliance Assessment component is complete after the following conditions have been met:** **a. Each legislative section/subsection has a Legislative Compliance Outcome value indicated in the Compliance Result field set.** **b. For each artifact:** **i. All required artifact information has been completed.** **ii. An Overall Artifact Compliance Outcome value has been selected.** **iii. A minimum of one Contact Name has been** selected as the Responsible Party for each legislative section/subsection with a ***Overall Artifact Compliance Outcome*** value of "Non-Compliance". ***0 Points if none of the listed actions are***	O	O	O	O

	1 Point if no fewer than two of the listed actions are demonstrated ***3 Points if no fewer than three of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***				
24.	**Set Values and Enable Next Component in Workflow** **To perform the following actions:** **a. Set the following fields to the following values:** **i. Activity Status value to "Enforcement Action Plan Required";** **ii. Compliance Assessment Completion Date value to the system date value;** **iii. Compliance Assessment Completion Time** value to the system time ***value*** b. Set all fields to read-only. c. Enable for input and viewing the Enforcement Action component of the Activity "tabbed pane. When the information in the Compliance Assessment component is confirmed by the User, and successfully validated and verified as complete, and there is a ***Legislative Section/Subsection*** value with a ***Legislation Section Compliance Outcome*** value of one of the following: a. "Non-Compliance"; b. "Non-Compliance – Minor"; c. "Non-Compliance – Major". ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
Score for Indicators 4 to 24:					**/105**
Scenario 6. Document Compliance Assessment and Analysis Total Score:					**/205**

Scenario 7. **C&E Activity - Document Enforcement Actions**

SCENARIO #7 - C&E Activity - Document Enforcement Actions

Context

After the assessment of compliance and analysis is completed the inspector will determine, based on the state of compliance, if an enforcement action is required. The inspector should document all information of the selected enforcement action(s) if required, and it's implementation.

The Prototype Solution should have the functionality for the User to:

1. Determine, based on the state of compliance, if an enforcement action is required.
2. If an enforcement action is required, document all information of the selected enforcement action and its implementation.

C&E Activity - Document Enforcement Actions – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality:				
1.	**Enforcement Actions Component** To provide an Enforcement Actions component of the Activity "tabbed pane" (as described in Part 4: User Interface and Usability Assessment, Indicator 47) for the User to enter, update, and view the following enforcement action information: a. Data in the Recommended Enforcement Action field set. b. Data in the following enforcement action field sets for the following ***Enforcement Action Type*** values selected in the Recommended Enforcement Action field set: i. Warning Letter; ii. Warning Letter Links.				
2.	**Recommended Enforcement Action** To display "Warning Letter" as the ***Enforcement Action Type*** value in the Recommended Enforcement Action field set for each legislative section/subsection with a ***Legislation Section Compliance Outcome*** value of any of the following: a. "Non-Compliance"; b. "Non-Compliance-Minor"; c. "Non-Compliance-Major".	O			O
3.	**Enforcement Action Plan** For the User to select the ***Enforcement Action Type*** value for each responsible party and ***Legislative Section/Subsection*** value where non-compliance is indicated.	O			O
4.	**Standard Letter Generation from a Template: Warning Letter** To populate the information in a letter template to generate a letter. When the User selects "Warning Letter" as the ***Enforcement Action Type*** value, the Prototype Solution should perform the following actions to generate a warning letter: a. Use fields, with the applicable options, that can be selected and pre-populated. For example: i. Name, Address, and contact information of the regulated party or establishment; ii. ***Legislative Sections/Subsections*** values associated with the non-compliance. b. Use applicable standard text. For example: i. text informing the regulated party there are non-compliances ii. text outlining the time given to correct the non-compliances and the consequences of not correcting the non-compliances	O	O		O

	0 Points if none of the listed actions are demonstrated ***1 Point if only one of the listed actions is demonstrated*** ***5 Points if all of the listed actions are demonstrated***				
5.	**Warning Letter Saved** For the User to perform the following actions on documents generated from templates: a. Save the warning letter document to the HC approved repository; b. Provide a link to the warning letter document. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O		O
6.	**Enforcement Action Validation** To ensure the following conditions have been completed for each ***Legislative Section/Subsection*** value where non-compliance is indicated before the Enforcement Action component can be confirmed as complete: a. A responsible party is assigned; b. An enforcement action is selected; c. The enforcement action is in a completed state. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***3 Points if no fewer than two of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
7.	**Enforcement Action Confirmation** To perform the following actions: a. set the ***Activity Status*** value to "Pending Closure" b. set all the values in the Enforcement Action field set to read-only when the information in the Enforcement Action component is: a. confirmed by the User b. successfully validated and verified as complete ***0 Points if neither of the listed actions are demonstrated***	O	O		O

	1 Point if only one of the listed actions is demonstrated ***5 Points if all of the listed actions are demonstrated***				
Scenario 7. Document Enforcement Actions Total Score:					**/30**

Scenario 8. **C&E Activity - Close Activity**

SCENARIO #8 - C&E Activity - Close Activity

Context

Once all documentation on the enforcement action(s) is completed, the User will close the activity.

The Prototype Solution should have the functionality for the User to:

1. Once all documentation on the enforcement action(s) is completed, close the activity.

C&E Activity - Close Activity – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality :				
1.	**Link/Close Component** To provide a Link/Close component of the Activity "tabbed pane", (as described in Part 4: User Interface and Usability Assessment, Indicator 48, and assessed in Part 1: Capability Scenarios Assessment, Scenario 3, Indicator 17) for the User to enter, update, and view all data at any time after the activity plan information in the General Information component has been confirmed as complete.				
2.	**Activity Workflow Step: Close Activity** For the User to close an activity with no linked activity in the Link/Close component by performing the following workflow steps: a. within the Recommended Next Steps field set: i. select "No linked activity required at this time" as the value for ***Linked To*** ii. select a value for ***Activity Close Reason*** iii. select "Yes" as the value for ***Close Activity Now*** b. within the Justification field set, provide a justification for closing the activity ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than three of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O

3.	**Activity Complete** To require the User to confirm that the information in the activity is complete when the ***Close Activity Now*** value is "Yes".	O			O
4.	**Activity Complete and Close** To perform the following actions in the specified order when the User confirms the information in the activity is complete: a. Set the ***Activity Completed*** value to "Yes". b. Set the ***Activity Close Date*** value to the current system date value. c. Set the ***Activity Status*** value to "Closed". d. Append the ***Activity Close Reason*** value and the ***Activity Close Justification*** value to the activity's ***Comments*** value. e. Set all the activity field values to read-only to prevent further updating to the closed activity. f. Add the closed activity to the "Activities of Previous Interest" list in the User's Workload Overview (dashboard) view. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
Scenario 8. Close Activity Total Score:					**/15**

C&E Activity - Industry Reports - Overview

C&E Activity - Industry Reports - Overview

Context

Prototype Solution:

When an Industry Report for an establishment is submitted to the Prototype Solution, the Solution should create a new activity (see Scenario 9- Industry Reports-Create a new Activity for a Submitted Industry Report) and perform initial compliance assessment and analysis on the industry report data. Once the initial compliance assessment and analysis is completed, the Solution will add the activity to the workload of the User who is assigned to work on the establishment.

After the assessment of compliance is completed by the User, the Prototype Solution will select a recommended enforcement action for each non-compliant legislative section/subsection.

User:

When a new activity for an Industry Report is added to the User's workload, the User will perform a compliance assessment of an Industry Report that has been submitted into the solution. The User will review the initial compliance assessment results of the industry report performed by the solution. After reviewing the results, the User should document any overrides required of the outcomes/results of analysis performed by the Prototype Solution.

After the assessment of compliance is completed, the User will review the enforcement action(s) recommended by the Prototype Solution and determine if an override of the recommended enforcement action(s) is required. The User should document all information of the selected enforcement action(s) as required, and its implementation.

Once all documentation of the enforcement action(s) is completed, the User will close the activity.

Because the User portion of the C&E of industry reports scenario involves many processes and steps, this scenario has been broken down into separate scenarios as follows:

- Scenario 10 - Industry Reports - Perform Compliance Assessment and Analysis Review
- Scenario 11 - Industry Reports - Review Enforcement Actions and document any overrides required

Scenario 9. **A C&E Activity - Industry Report Section 11 - Create a new Activity for a Submitted Industry Report**

SCENARIO #9 A - C&E Activity - Industry Report Section 11 - Create a new Activity for a Submitted Industry Report

Context

When an Industry Report for an establishment is successfully submitted to the Prototype Solution via XML as described in Scenario 14, the Prototype Solution should create a new activity and perform initial compliance assessment and analysis on the industry report data. Once the initial compliance assessment

and analysis is completed, the Solution will add the activity to the workload of the User who is assigned to work on the establishment.

The Prototype Solution should provide the functionality:

1. To create a new activity when an Industry Report is submitted.
2. To perform the initial compliance assessment and analysis of the industry report data.
3. To document the outcomes/results of analysis performed on the Industry Report data information.
4. To document the ***State of Compliance*** and ***Level of Compliance*** of the industry Report data based on the relevant outcomes/results.
5. To add the activity to the workload of the ***Designated User*** who is assigned to work on the establishment.

C&E Activity - Industry Report Section 11 - Create a new Activity for a Submitted Industry Report – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (10)	Mostly Demonstrated (30)	Fully Demonstrated (50)
	The Prototype Solution should provide the functionality:				
1.	**Create New Activity for a Submitted Industry Report Section 11** To create a new activity record connected to an existing active establishment for a submitted industry report (as described in Part 4: User Interface and Usability Assessment, Indicator 43, and assessed in Part 1: Capability Scenarios Assessment, Scenario 1, Indicator 13).				
2.	**Create New Activity Record Connected to Existing Active Establishment** To perform the following activity steps to create a new activity record connected to an existing active establishment for a submitted industry report data, as described in Part 1: Scenario 14: 1. Create and populate a new activity record connected to an existing active establishment (as assessed in Scenario 9.A, Indicator 3, below). 2. Document initial compliance analysis and assessment results, (as assessed in Scenario 9.A, Indicators 4 to 14, below). **Score for this indicator will be based on the cumulative score of the indicators 3-14 for the activity created and populated with the appropriate information for an industry report activity.** ***0 Points Did Not Demonstrate (Scored 0 points on indicators 3-14)*** ***10 Points Partially Demonstrated (Scored 1-59 points on indicators 3-14)*** ***30 Points Mostly Demonstrated (Scored 60-99 points on indicators 3-14)***	O	O	O	O

	50 Points Fully Demonstrated (Scored 100 points on indicators 3-14)				
3.	**Create and Populate a New Activity Record Connected to Existing Active Establishment** To perform the following actions, when an industry report is received: 1. Set the ***Report Status*** value to "Registered"; 2. Search for and select an existing establishment that matches the establishment information identified in the industry report: e.g., ***Establishment Name***, ***Street***, ***City***, ***Province***, ***Postal Code;*** 3. Provide a Product and Brands component of the Establishment "tabbed pane" (as described in Part 4: User Interface and Usability Assessment, Indicator 42) in which to enter, update, and view establishment product and brand information; 4. Populate the Product and Brand component with data found in the industry report; 5. Provide an Industry Reporting History component of the Establishment "tabbed pane"(as described in Part 4: User Interface and Usability Assessment, Indicator 43),in which to enter, update, and view industry reporting history information; 6. Populate the Industry Reporting History; 7. Create an activity for the establishment connected to the industry report based on the industry report information values (for example, ***Report Section);*** 8. Set the value to indicate the review of establishment information is confirmed as complete; 9. Set the value to indicate the review of the associated establishments and the establishment activity history information is confirmed as complete; 10. Set the ***Activity Type*** value to "Inspection"; 11. Set the ***Activity Reason Type*** value to "Scheduled: Industry Report"; 12. Set the ***Proposed Start Date*** value to the ***Report Status Effective Date*** value; 13. Set the value to indicate the activity initialization information is confirmed as complete; 14. Set the mandatory field values to read-only 15. Set the ***Activity Scope Plan Type*** value to the ***Report Section Name*** value; 16. Set the value to indicate the Scope Plan is confirmed as complete; 17. Set the ***Activity Status*** value to "Pending Compliance"; 18. Set the Ac***tivity Plan Status Type*** value to "Approved"; 19. Set all Scope Plan field values to read-only; 20. Set ***Activity Establishment Verification Code*** value to "Verified by Portal"; 21. Set the ***Industry Report Received Date*** to the system date; 22. Set the ***Industry Report Received Time*** to the system time; 23. Set all field values in the Establishment Location Verification field set to read-only;	O			O

	24. Populate the Legislation field in the Compliance Results field set with the industry report ***Legislation Section*** name; 25. Set the ***Artifact Analysis Type*** value to "In House" in the Compliance Results field set; 26. Set the ***Number of Artifacts*** value to "1"; 27. Populate the ***Legislative Section/Subsection*** field in the Compliance Results field set with the Legislative Section/ Subsection values appropriate for the industry report Legislation section; 28. Populate the fields in the Artifacts Summary field set in the Compliance Assessment component with the ***Artifact Id*** and ***Legislation Section*** values. **Rating will be dependent on the resultant activity created and populated with the appropriate information for an industry report activity.** ***0 Points if none of the listed actions are demonstrated*** ***50 Points if all of the listed actions are demonstrated***				
	Score for Indicators 2 to 3:				**/100**
	Scoring for Indicators 4 to 14 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
4.	**Industry Report Submission Data in Artifact** To populate the following industry report submission data in the Artifact Analysis component of the Artifact pane (as described in Part 4: User Interface and Usability Assessment, Indicator 63): a. ***Establishment Name*** (for the activity); b. ***Artifact Id Number*** (Prototype Solution generated by concatenating Prototype Solution generated number + Legislation number + number of artifact for this Legislative section/subsection, starting at the number 1); c. ***Artifact Information*** (Submitted industry report data). ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O		O
5.	**Artifact Analysis** To perform Artifact Analysis against the appropriate legislation assessed by Indicators 6 to 13, below, in this scenario.				
6.	**Verify Submission Data and Populate Error Data** To verify the industry report artifact based on the ***Legislative Section/Subsection*** of the Industry Report and populate	O	O	O	O

	errors according to the legislated submission requirements, as follows: a. Identify information required in the submission but not provided; b. Incorrect unit of measures; c. Values outside of a range; d. Incorrect Totals ***0 Points if none of the listed verifications are demonstrated*** ***1 Point if only one of the listed of the listed verifications is demonstrated*** ***3 Points if 2 to 3 of the listed verifications are demonstrated*** ***5 Points if all of the listed verifications are demonstrated***				
7.	**Perform Calculations** To perform calculations and set the non-compliance values for the legislative requirements as a read-only value, as follows: a. Sum the ***Ingredient Amounts*** for each brand, and compare it against any of the following: i. the reported ***Product Weight***. If the sum is greater than ± a specified range of the ***Product Weight***, the Solution flags this error and sets the ***Legislative Section/Subsection*** 11(1)(d) value to "Non-Compliance". ii. the ***Total Ingredient Amount.*** If the sum does not equal the ***Total Ingredient Amount,*** the Solution flags this error and associates it with the ***Legislative Section/Subsection*** 11(1)(d) value as an additional "Non-Compliance" b. Sum the ***Substance Amounts*** for each ingredient and compare it against reported ***Ingredient Amount*** for each brand. If the sum is greater than ± a specified range of the ***Ingredient Amount***, the Solution flags this error and sets the ***Legislative Section/Subsection*** 11(2) value to "Non-Compliance".	O			O
8.	**Populate Error Display in Compliance Results field set** To display the following values in the Compliance Results field set (as described in Part 4: User Interface and Usability Assessment, Indicator 59): a. ***Number of Errors*** by ***Legislative Section/Subsection*** value; b. ***Total Number of Errors*** for all ***Legislative Sections/Subsections.*** ***0 Points if neither of the listed action is demonstrated*** ***1 Point if only one of the listed actions is demonstrated***	O	O		O

	5 Points if both of the listed actions are demonstrated				
9.	**Derive and Display Activity Compliance Outcome Value** To derive and populate, in the Compliance Summary field set, the ***Activity Compliance Outcome*** value for the activity by setting the ***State of Compliance*** and ***Level of Compliance*** values to one of the following values: a. "Non-Compliance-Minor" if the legislative sections/subsections found to be "Non-Compliance" were set to "Minor" Compliance Level in a specified number of instances. b. "Non-Compliance-Major" if the legislative sections/subsections found to be "Non-Compliance" had at least one where a "Major" Compliance Level was set. c. "No Evidence of Non-Compliance" if at least one legislative section/subsection was found to be "No Evidence of Non-Compliance", and **no** legislative sections/subsections were found to be "Non-Compliance". d. "Not assessed" if all legislative sections/subsections were found to be "Not assessed". e. "Not Applicable" if all legislative sections/subsections were found to be "Not Applicable". ***0 Points if none of the listed values are derived and displayed*** ***5 Points if the correct value is derived and displayed***	O			O
10.	**Calculations of Compliance Outcome Value** To perform the following calculations: a. Calculate the total number of legislative sections/subsections with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Minor". b. Calculate the total number of legislative sections/subsections with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Major". c. Calculate the number of errors for legislative sections/subsections with a the ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Minor". d. Calculate the number of errors for legislative sections/subsections with a the ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Major". ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***3 Points if 2 to 3 of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
11.	**Non-compliances Summary**	O	O		O

	To display a summary table of non-compliances in the Compliance Summary field set in the following manner: a. The number of non-compliances by ***Compliance Outcome Level***, Major and Minor; b. The number of errors by ***Compliance Outcome Level***, Major and Minor; c. The sum total of non-compliances and errors. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***5 Points if all of the listed actions are demonstrated***				
12.	**No Override** To prevent the User from overriding the selected value in the Overall Assessment of Compliance Section, for example, by setting the selected value to read-only.	O			O
13.	**Enable Compliance Assessment Component** To enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane".	O			O
14.	**Add New Activity to Workload** To add the new activity to the "Activities" list in the ***Assigned User***'s My Workload field set in the Workload Overview (dashboard).	O			O
	Score for 4 to 14:				**/50**
	Scenario 9A. Industry Reports Section 11 - Create a new Activity for a Submitted Industry Report Total Score:				**/150**

Scenario 9. **B C&E Activity - Industry Report Section 13 - Create a new Activity for a Submitted Industry Report**

SCENARIO #9 B - C&E Activity - Industry Report Section 13 - Create a new Activity for a Submitted Industry Report

Context

When an Industry Report for an establishment is successfully submitted to the Prototype Solution via a guided form as described in Scenario 15, the Prototype Solution should create a new activity and perform initial compliance assessment and analysis on the industry report data. Once the initial compliance assessment and analysis is completed, the Solution will add the activity to the workload of the User who is assigned to work on the establishment.

The Prototype Solution should provide the functionality:

1. To create a new activity when an Industry Report is submitted.
2. To perform the initial compliance assessment and analysis of the industry report data.
3. To document the outcomes/results of analysis performed on the Industry Report data information.
4. To document the ***State of Compliance*** and ***Level of Compliance*** of the industry Report data based on the relevant outcomes/results.

5. To add the activity to the workload of the ***Designated User*** who is assigned to work on the establishment.

C&E Activity - Industry Report Section 13 - Create a new Activity for a Submitted Industry Report – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (10)	Mostly Demonstrated (30)	Fully Demonstrated (50)
	The Prototype Solution should provide the functionality:				
1.	**Create New Activity for a Submitted Industry Report Section 13** To create a new activity record connected to an existing active establishment for a submitted industry report (as described in Part 4: User Interface and Usability Assessment, Indicator 43, and assessed in Part 1: Capability Scenarios Assessment, Scenario 1, Indicator 13).				
2.	**Create New Activity Record Connected to Existing Active Establishment** To perform the following activity steps to create a new activity record connected to an existing active establishment for a submitted industry report data, as described in Part1: Scenario 15: 1. Create and populate a new activity record connected to an existing active establishment (as assessed in Scenario 9.B, Indicator 3, below). 2. Document initial compliance analysis and assessment results, (as assessed in Scenario 9.B, Indicators 4 to 15, below). **Score for this indicator will be based on the cumulative score of the indicators 3-17 for the activity created and populated with the appropriate information for an industry report activity.** ***0 Points Did Not Demonstrate (Scored 0 points on indicators 3-15)*** ***10 Points Partially Demonstrated (Scored 1-47 points on indicators 3-15)*** ***30 Points Mostly Demonstrated (Scored 48-79 points on indicators 3-15)*** ***50 Points Fully Demonstrated (Scored 80 points on indicators 3-15)***	O	O	O	O
3.	**Create and Populate a New Activity Record Connected to Existing Active Establishment** To perform the following actions when an industry report is received: 1. Set the ***Report Status*** value to "Registered"; 2. Search for and select an existing establishment that matches the establishment information identified in the industry report: e.g., ***Establishment Name, Street, City, Province, Postal Code;***	O			O

	3. Provide a Product and Brands component of the Establishment "tabbed pane"(as described in Part 4: User Interface and Usability Assessment, Indicator 42) in which to enter, update, and view establishment product and brand information; 4. Populate the Product and Brand component with data found in the industry report; 5. Provide an Industry Reporting History component of the Establishment "tabbed pane"(as described in Part 4: User Interface and Usability Assessment, Indicator 43) in which to enter, update, and view industry reporting history information; 6. Populate the Industry Reporting History; 7. Create an activity for the establishment connected to the industry report based on the industry report information values (for example, ***Report Section);*** 8. Set the value to indicate the review of establishment information is confirmed as complete; 9. Set the value to indicate the review of the associated establishments and the establishment activity history information is confirmed as complete; 10. Set the ***Activity Type*** value to "Inspection"; 11. Set the ***Activity Reason Type*** value to "Scheduled: Industry Report"; 12. Set the ***Proposed Start Date*** value to the ***Report Status Effective Date*** value; 13. Set the value to indicate the activity initialization information is confirmed as complete; 14. Set the mandatory field values to read-only 15. Set the ***Activity Scope Plan Type*** value to the ***Report Section Name*** value; 16. Set the value to indicate the Scope Plan is confirmed as complete; 17. Set the ***Activity Status*** value to "Pending Compliance"; 18. Set the Ac***tivity Plan Status Type*** value to "Approved"; 19. Set all Scope Plan field values to read-only; 20. Set ***Activity Establishment Verification Code*** value to "Verified by Portal"; 21. Set the ***Industry Report Received Date*** to the system date; 22. Set the ***Industry Report Received Time*** to the system time; 23. Set all field values in the Establishment Location Verification field set to read-only; 24. Populate the Legislation field in the Compliance Results field set with the industry report ***Legislation Section*** name; 25. Set the ***Artifact Analysis Type*** value to "In House" in the Compliance Results field set; 26. Set the ***Number of Artifacts*** value to "1"; 27. Populate the ***Legislative Section/Subsection*** field in the Compliance Results field set with the Legislative Section/ Subsection values appropriate for the industry report Legislation section; 28. Populate the fields in the Artifacts Summary field set in the Compliance Assessment component with the ***Artifact Id*** and ***Legislation Section*** values.				

	Rating will be dependent on the resultant activity created and populated with the appropriate information for an industry report activity. ***0 Points if none of the listed actions are demonstrated*** ***50 Points if all of the listed actions are demonstrated***				
	Score for Indicators 2 to 3:				**/100**
	Scoring for Indicators 4 to 15 below:	**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
4.	**Industry Report Submission Data in Artifact** To populate the following industry report submission data in the Artifact Analysis component of the Artifacts pane (as described in Part 4: User Interface and Usability Assessment, Indicator 63): a. ***Establishment Name*** (for the activity); b. ***Artifact Id*** (Prototype Solution generated by concatenating Prototype Solution generated number + Legislation number + number of artifact for this Legislative section/subsection, starting at the number 1); c. ***Artifact Information*** (Submitted industry report data). ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O		O
5.	**Artifact Analysis** To perform Artifact Analysis against the appropriate legislation assessed by Indicators 6 to 14, below, in this scenario.				
6.	**Verify Submission Data** To verify the industry report artifact based on the ***Legislative Section/Subsection*** of the Industry Report and populate errors according to the legislated submission requirements, as follows: a. Identify information required in the submission but not provided; b. Identify information missing in the submission but found in the Prototype Solution; c. Identify information found in the submission but missing in the Prototype Solution; d. Incorrect unit of measures; e. Values outside of a range; f. Incorrect Totals. ***0 Points if none of the listed verifications are demonstrated***	O	O	O	O

	1 Point if only one of the listed of the listed verifications is demonstrated ***3 Points if 2 to 5 of the listed verifications are demonstrated*** ***5 Points if all of the listed verifications are demonstrated***				
7.	**Perform Calculations** To perform calculations and set the non-compliance values for the legislative requirements as a read-only value as follows: a. Verify the ***Total Volumes Sold*** for each ***Brand*** value. If the validation fails, then the Prototype Solution should flag this error and set the ***Legislative Section/Subsection*** 13(2) value to "Non-Compliance". Perform the validation in the following manner: i. If ***Unit of Measure of Package*** is "g", then this value should equal ***Amount_Per_Package*** * ***Total_Packs_Sold***/1000; ii. If ***Unit of Measure of Package*** is not "g", then ***Total_Volume_Sold*** should equal ***Amount_Per_Package*** * ***Total_Packs_Sold.*** b. Verify the ***Total Sales CAD*** for the ***Canadian Market Region*** value of "Canada" and compare it against the sum of the ***Total Sales CAD*** all the other ***Canadian Market Region*** values. If the "Canada" total does not match the sum, the Solution flags this error and sets the Legislative Section/Subsection 13(1)(a) value to "Non-Compliance".	O			O
8.	**Brand Validation Check** To perform the following brand validation check: a. Identify brands found in the report but not stored in the Prototype Solution for the establishment. b. Identify brands found in the solution for the establishment but missing in the report. c. Display the identified brands in the Summary of Errors as described in the Artifact Pane Format – Industry Report in Part 4: User Interface and Usability Assessment, Indicator 66 .	O			O
9.	**Populate Error Display in Compliance Results field set** To display the following values in the Compliance Results field set (as assessed in Part 1, Scenario 9.A, Indicator 8): a. ***Number of Errors*** by ***Legislative Section/Subsection;*** b. ***Total Number of Errors*** for all ***Legislative Sections/Subsections.***				
10.	**Derive and Populate Activity Compliance Outcome Value** To derive and populate, in the Compliance Summary field set, the ***Activity Compliance Outcome*** value for the activity by setting the ***State of Compliance*** and ***Level of Compliance*** values to one of the following values: a. "Non-Compliance-Minor" if the legislative sections/subsections found to be "Non-Compliance" were set to "Minor" Compliance Level to a maximum of 5 instances.	O			O

	b. "Non-Compliance-Major" if the legislative sections/subsections found to be "Non-Compliance" had at least one where a "Major" Compliance Level was set. c. "No Evidence of Non-Compliance" if at least one legislative section/subsection was found to be "No Evidence of Non-Compliance", and **no** legislative sections/subsections were found to be "Non-Compliance". d. "Not assessed" if all legislative sections/subsections were found to be "Not assessed". e. "Not Applicable" if all legislative sections/subsections were found to be "Not Applicable". ***0 Points if none of the listed values are derived and displayed*** ***5 Points if the correct value is derived and displayed***				
11.	**Calculations of Compliance Outcome Value** To perform the following calculations: a. calculate the total number of legislative sections/subsections with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Minor" b. calculate the total number of legislative. sections/subsections with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Major" c. calculate the number of errors for legislative. sections/subsections with a the ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Minor" d. calculate the number of errors for legislative. sections/subsections with a the ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Major". ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***3 Points if 2 to 3 of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***	O	O	O	O
12.	**Non-compliances Summary** To display a summary table of non-compliances in the Compliance Summary field set in the following manner, (as assessed in Part 1, Scenario 9.A, Indicator 11): a. The number of non-compliances by ***Compliance Outcome Level***, Major and Minor; b. The number of errors by ***Compliance Outcome Level***, Major and Minor; c. The sum total of non-compliances and errors.				
13.	**No Override** To prevent the User from overriding the selected value in the Overall Assessment of Compliance Section, for example, by setting the selected value to read-only, (as assessed in Part 1, Scenario 9.A, Indicator 12)..				

14.	**Enable Compliance Assessment Component** To enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane", (as assessed in Part 1, Scenario 9.A, Indicator 13).				
15.	**Add New Activity to Workload** To add the new activity to the "Activities" list in the ***Assigned User***'s My Workload field set in the Workload Overview (dashboard), (as assessed in Part 1, Scenario 9.A, Indicator 14).				
	Score for 4 to 15:				**/30**
	Scenario 9. B Industry Reports Section 13 - Create a new Activity for a Submitted Industry Report Total Score:				**/130**

Scenario 10. **C&E Activity - Industry Reports - Perform Compliance Assessment and Analysis Review**

SCENARIO #10 - C&E Activity - Industry Reports - Perform Compliance Assessment and Analysis Review

Context

A new activity for a submitted Industry Report has been created by the Prototype Solution and added to the Assigned User's workload. The Assigned User will select and open the new activity. The User will navigate directly to the Compliance Assessment component of the Activity "tabbed pane-like" format and perform a review of the initial compliance assessment and analysis results of the industry report performed by the Prototype Solution.

After reviewing the results, the Assigned User will document any overrides of the compliance assessment outcomes and/or results of analysis performed by the Prototype Solution.

The Prototype Solution should have the functionality for the User to:

1. Select an activity from the Workload Overview (dashboard).
2. Indicate Start of Compliance Assessment in the Compliance Assessment component
3. Review the outcomes/results of analysis performed by the Prototype Solution on the gathered information.
4. Document any overrides to the compliance assessment results, as required.
5. Follow Scenario #6 starting at Indicator 20 to complete the Compliance Assessment of an Industry Report.

C&E Activity – Industry Reports - Perform Compliance Assessment Review - Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality:				
1.	**Open Activity from My Workload Field Set** For the User to select and open an activity from My Workload field set in the Workload Overview (dashboard) to view and edit activity details.	O			O
	Score for Indicator 1:				**/5**

	Scoring for Indicator 2:	Did Not Demonstrate (0)	Partially Demonstrated (10)	Mostly Demonstrated (30)	Fully Demonstrated (50)
2.	**Workflow Steps to Review Compliance Assessment – Industry Reports** To move the User through the following workflow steps to review compliance assessment of an industry report performed by the Prototype Solution: 1. Review compliance assessment results by ***Legislative Section/Subsection*** value; 2. Override ***Compliance Outcome*** value for a ***Legislative Section/Subsection*** value (as required); 3. Manually add an error (as required); 4. View submitted industry report data from the Artifacts Summary field set; 5. View and update details of a responsible party from the Responsible Party Summary field set; 6. Confirm Compliance Assessment information is complete. **Score for this indicator will be based on the cumulative score of the indicators specified for each workflow step and the sequence as specified in this requirement.** ***0 Points Did Not Demonstrate (Scored 0 points on indicators 3-9)*** ***10 Points Partially Demonstrated (Scored 1-20 points on indicators 3-9)*** ***30 Points Mostly Demonstrated (Scored 21-34 points on indicators 3-9)*** ***50 Points Fully Demonstrated (Scored 35 points on indicators 3-9)***	O	O	O	O
	Score for Indicator 2:				**/50**
	Scoring for Indicator 3 to 12:	**Did Not Demonstrate (0)**	**Partially Demonstrated (1)**	**Mostly Demonstrated (3)**	**Fully Demonstrated (5)**
3.	**Moved to Compliance Results Field Set** To move the User to the Compliance Results field set of the Compliance Assessment component.	O			O
4.	**Enable Compliance Assessment Component Field Sets** To perform the following actions: a. Set the ***Activity Status*** value to "Compliance In Progress"; b. Enable for input and viewing the following field sets and fields in the Compliance Assessment component: i. Compliance Results (as described in Industry Report in Part 4: User Interface and Usability Assessment, Indicator 59). ii. Compliance Summary (as described in Industry Report in Part 4: User Interface and Usability Assessment, Indicator 60).	O	O	O	O

	iii. Sections Overridden (as described in Industry Report in Part 4: User Interface and Usability Assessment, Indicator 61). iv. Artifacts Summary (as described in Industry Report in Part 4: User Interface and Usability Assessment, Indicator 62). v. Responsible Party Summary (as described in Industry Report in Part 4: User Interface and Usability Assessment, Indicator 58). ***0 Points if none of the listed actions are demonstrated*** ***1 Point if no fewer than two of the listed actions are demonstrated*** ***3 Points if no fewer than four of the listed actions are demonstrated*** ***5 Points if all of the listed actions are demonstrated***				
5.	**View Submitted Industry Report Data** For the User to view the submitted industry report data in the ***Artifact Information*** field in the Artifact pane (as described in Industry Reports – Artifact "Analysis" Component in Part 4: User Interface and Usability Assessment, Indicator 63) where the report data is in a structured, readable, and viewable format.	O			O
6.	**View Summary of Errors** For the User to view a summary of the errors grouped by ***Legislative Section/Subsection*** value (as described in the Part 4: User Interface and Usability Assessment, Indicator 64) after the User selects either of the following from the Compliance Results field set (as described in Part 4: User Interface and Usability Assessment, Indicator 59): a. the ***Number of Errors*** value by each any legislative subsection; b. the ***Total Number of Errors*** value. ***0 Points if none of the listed actions are demonstrated*** ***1 Point if one of the two of the listed actions are demonstrated*** ***5 Points if both of the listed actions are demonstrated***	O	O		O
7.	**Manually Identify and Document Errors** For the User to manually identify and document errors related to the artifact that were not flagged by the Prototype Solution's validation.	O			O
8.	**Override Compliance Outcome Value** For the User to perform the following when the ***Compliance Outcome*** value for a ***Legislative Section/Subsection*** needs to	O	O		O

	be changed from the ***Compliance Outcome*** value selected by the Prototype Solution: a. Change the ***Compliance Outcome*** value for the ***Legislative Section/Subsection***; b. Confirm the change in value; c. Enter a reason for the override in the Sections Overridden field set, ***0 Points if none of the listed actions are demonstrated*** ***1 Point if only one of the listed actions is demonstrated*** ***5 Points if all of the listed actions are demonstrated***				
9.	**Legislative Section/Subsection Refresh After Update** To update the ***Compliance Outcome*** value based on the actions of the User, when the User manually identifies an error or overrides the ***Compliance Outcome*** value set by the Solution***.***	O			O
10.	**Review the Compliance Summary for Accuracy and Completeness** For the User to review the following in the Compliance Summary field set (as described in Part 4: User Interface and Usability Assessment, Indicator 60) for accuracy and completeness: a. the summary table of non-compliances and errors by ***Compliance Level;*** b. ***State of Compliance*** value; c. ***Level of Compliance*** value.	O			O
11.	**Responsible Party** For the User to select a name from the Contact List as the value for the ***Responsible Party*** for the non-compliant legislative section of the Industry Report.	O			O
12.	**Confirm Compliance Assessment is Complete and Set Values and Enable Next Component in Workflow** For the User to follow Scenario 6 to confirm compliance assessment is complete (as assessed in Part 1: Capability Scenarios Assessment, Scenario 6, Indicator 23 and 24).				
	Score for 3 to 12:				**/45**
	Scenario 10. Industry Reports - Perform Compliance Assessment Review Total Score:				**/100**

Scenario 11. **C&E Activity - Industry Reports - Document Enforcement Actions**

SCENARIO #11 - C&E Activity - Industry Reports - Document Enforcement Actions

Context

After the assessment of compliance is completed, The Prototype Solution will select a recommended enforcement action for each non-compliant legislative section/subsection.

The User will review the enforcement action(s) selected by the Prototype Solution for both Section 11 and Section 13 Industry Reports and determine, based on the state of compliance, if an override of the selected enforcement action(s) is required. The User will document all information of the selected enforcement action (s), and its implementation.
Once all documentation on the enforcement action(s) is completed, the User will follow Scenario 8 to close the activity.

The Prototype Solution should have the functionality for the User to:

1. Review the ***Enforcement Action Type*** value(s), if any, selected by the Prototype Solution.
2. Document any overrides to the enforcement action(s) if any, and as required.
3. Follow Scenario 8. C&E Activity - Close Activity to Close the activity.

C&E Activity - Industry Reports - Document Enforcement Actions - Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality:				
1.	**Industry Report Section 11 - Recommend Enforcement Action** To set the ***Enforcement Action Type*** value to "Warning Letter" in the Recommended Enforcement Action field set for each non-compliant legislative section/subsection in the Enforcement Action component when the ***Activity Reason Type*** value is "Scheduled: Industry Report".	O			O
2.	**Industry Report Section 13 - Recommend Enforcement Action** To set the ***Enforcement Action Type*** value to "Warning Letter" in the Recommended Enforcement Action field set for each non-compliant legislative section/subsection in the Enforcement Action component when the ***Activity Reason Type*** value is "Scheduled: Industry Report".	O			O
3.	**Industry Reports - Enforcement Actions Component** To provide an Enforcement Action component of the Activity "tabbed pane" for the User to enter, update, and view the following enforcement action information (as assessed in Part 1: Capability Scenarios Assessment, Scenario 7, Indicator 1): a. Data in the Recommended Enforcement Action field set; b. Data in the following enforcement action field sets for the following ***Enforcement Action Type*** values selected in the Recommended Enforcement Action field set: i. Warning Letter; ii. Warning Letter Links.				
4.	**Industry Reports - Recommended Enforcement Action** To display "Warning Letter" as the ***Enforcement Action Type*** value in the Recommended Enforcement Action field set for each legislative section/subsection with a ***Legislation Section Compliance Outcome*** value of any of the following (as assessed in Part 1: Capability Scenarios Assessment, Scenario 7, Indicator 2): a. "Non-Compliance";				

	b. "Non-Compliance-Minor"; **C.** "Non-Compliance-Major".				
5.	**Industry Report Section 13 - Enforcement Action Override** For the User to: a. Select "No Action" as the ***Enforcement Action Type*** value to override the enforcement action selected by the Prototype Solution. b. Provide a reason for the override. ***0 Points none of the listed actions are demonstrated*** ***1 Point if one of the listed actions is demonstrated*** ***5 Points if both of the listed actions are demonstrated***	O	O		O
6.	**Industry Reports - Standard Letter Generation: Warning Letter** For the User to generate and update a warning letter from a Warning Letter template (as assessed in Part 1: Capability Scenarios Assessment, Scenario 7, Indicator 4) where the following information can be inserted: a. The address and contact information of the regulated party or establishment; b. A list of the non-compliant legislative section(s)/subsection(s) where a Warning Letter has been selected as the Enforcement Action. The list can be modified by the User.				
7.	**Industry Reports - Enforcement Action Validation** For the User to confirm that the information in the Enforcement Actions component (as assessed in Part 1: Capability Scenarios Assessment, Scenario 7, Indicator 6) is complete after ensuring the following conditions have been completed for each non-compliant legislative section/subsection: a. A responsible party is assigned; b. An enforcement action is selected; c. The enforcement action is in a completed state.				
8.	**Industry Reports - Enforcement Action Confirmation** When the information in the Enforcement Actions component (as assessed in Part 1: Capability Scenarios Assessment, Scenario 7, Indicator 7) is confirmed by the User, and successfully validated and verified as complete, the Prototype Solution should perform the following actions: a. Set the ***Activity Status*** value to "Pending Closure"; b. Set all the values in the Enforcement Action field set to read-only.				
9.	**Industry Reports - Close Activity** For the User to follow Scenario 8 to close the activity (as assessed in Part 1: Capability Scenarios Assessment, Scenario 8, Indicators 1 to 4.)				
	Scenario 11. Industry Reports - Document Enforcement Actions Total Score:				**/15**

Scenario 12. **C&E Activity – Update Existing Activity**

SCENARIO #12 - C&E Activity - Update Existing Activity

If an activity is not closed, the User is permitted to return at any time to the activity to update the fields available for input.

The Prototype Solution should have the functionality for the User to:

1. Select an activity from the Workload Overview (dashboard).
2. Navigate to an available component in the Activity tabbed pane-like format to continue working on the activity.
3. Save the work when finished entering information.

C&E Activity - Update Existing Activity – Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality:				
1.	**Open Existing Activity** For the User to select and open an activity from the My Workload field set (as assessed in Part 1: Capability Scenarios Assessment, Scenario 10, Indicator 1).				
2.	**Update Activity Comment** For the User to update the ***Comment*** field information for an existing Activity.	O			O
3.	**Save Updated Information.** For the User to save the updated information for an existing Activity.	O			O
Scenario 12. Update Existing Activity Total Score:					**/10**

Scenario 13. **C&E Activity – No Enforcement Action Required**

SCENARIO #13 - C&E Activity - No Enforcement Action Required

Context
At the end of Compliance Assessment, it is determined that the Compliance Assessment Outcome value is "No Evidence of Non-Compliance". The activity can be closed without documenting enforcement actions.

The Prototype Solution should have the functionality for the User to:

1. Move directly from the Compliance Assessment Component to the Close component of the Activity tabbed pane-like format.

C&E Activity - No Enforcement Action Required - Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should provide the functionality:				
1.	**No Enforcement Action Required** To perform the following actions: a. Set the following fields to the following values:	O			O

	i. Activity Status value to "Pending Closure"; ii. Compliance Assessment Completion Date value to the system date value; iii. Compliance Assessment Completion Time value to the system time value. b. Set previously confirmed fields to read-only. c. Enable for input and viewing the Close component of the Activity "tabbed pane". When the information in the Compliance Assessment component is confirmed by the User, and successfully validated and verified as complete, and no ***Legislative Section/Subsection*** value has a ***Legislation Section Compliance Outcome*** value of any of the following: a. "Non-Compliance"; b. "Non-Compliance – Minor"; c. "Non-Compliance – Major".				
2.	**Close Activity** For the User to follow Scenario 8 to close the activity (as assessed in Part 1: Capability Scenarios Assessment, Scenario 8, Indicators 1 to 4).				
Scenario 13. No Enforcement Action Required Total Score:		**/5**			

Compliance and Enforcement (C&E) Activity: Scenarios 3 to 13 Total Score:	**/905**

Electronic Data Submission

Scenario 14. **Electronic Data Submission via XML**

SCENARIO #14 – Electronic Data Submission via XML

Context

Industry is required to submit reports of different types to Health Canada. These range from sales to product or brand data. Industry reports are submitted according to a mandatory cyclical schedule, a specific business event, or on request. Industry reports are required to be submitted in a form and manner prescribed by Health Canada. In this instance, the industry report section 11 (Ingredients) is submitted via an XML structured file format.

The Prototype Solution should have the functionality for the User to:

1. Access the Solution.
2. Submit the electronic data in the prescribed form and manner.
3. Receive an acknowledgement that submission has been successfully received along with a ***Submission Confirmation Id***.

Electronic Data Submission - Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should have the functionality:				

1.	**Capturing and Processing Electronically Submitted Data** To capture and process electronically submitted data.	O			O
2.	**Industry Report Section 11 Data Submission** For the User to electronically submit structured industry report data in a prescribed form and manner for the Section 11 (Ingredients) industry report to the Prototype Solution via an XML structured file format.	O			O
3.	**Update Views: Registered** To perform the following actions when an industry report is received: a. Set the ***Report Status*** value to "Registered" and display it in the General Information section of the Activity. b. Add the industry report data as the artifact. c. Set the ***Submission Timing Status*** value to "Prior to or on the submission date" and display it in the General Information section of the Activity.	O			O
4.	**Data Capture Brand Via Submission of Required Industry Reports** To perform the following actions for any brand submitted in the Industry Report 11: a. Add the brand information to the Prototype Solution. b. Set the Brand Status value to "Pending".	O			O
5.	**Industry Report – Submission Confirmation** To send an email confirmation to the submitter acknowledging that the submission has been received along with a ***Submission Confirmation Id*** value when industry report data has been successfully submitted.	O			O
Scenario 14. Electronic Data Submission Total Score:					**/25**

Scenario 15. **Electronic Data Submission via a Guided Form**

SCENARIO #15 – Electronic Data Submission via a Guided Form

Context

Industry is required to submit reports of different types to Health Canada. These range from sales to product or brand data. Industry reports are submitted according to a mandatory cyclical schedule, a specific business event, or on request. Industry reports are required to be submitted in a form and manner prescribed by Health Canada. In this instance, the industry report section 13 (Sales) is submitted via a guided form.

Scenario #15 - Electronic Data Submission via a Guided Form

The Prototype Solution should have the functionality for the User to:

1. Access the Solution.
2. Submit the electronic data in the prescribed form and manner.
3. Receive an acknowledgement that submission has been successfully received along with a ***Submission Confirmation Id.***

Electronic Data Submission - Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should have the functionality:				
1.	**Capturing and Processing Electronically Submitted Data** To capture and process the electronically submitted data (as assessed in Part 1: Capability Scenarios Assessment, Scenario 14, Indicator 1).				
2.	**Industry Report 13 Data Submission** For the User to electronically submit structured industry report data in a prescribed form and manner for the Section 13 (Sales) industry report to the Prototype Solution via a guided form-based submission process.	O			O
3.	**Update Views: Registered** When an industry report is submitted, to perform the following actions (as assessed in Part 1: Capability Scenarios Assessment, Scenario 14, Indicator 3): a. Set the ***Report Status*** value to "Registered". b. Add the industry report data as the artifact. c. Set the ***Submission Timing Status*** value to "Prior to or on the submission date".				
4.	**Industry Report Update/View Screen of Tombstone Information** To provide an update/view screen of the fields reflecting mandatory tombstone information as stipulated by S.3 (2) and S.3 (3) of the TRR pre-populated with Establishment Profile information stored in the Solution**.**	O			O
5.	**Update and Confirm Tombstone Information** For the User to update and confirm the tombstone information.	O			O
6.	**Form-based Submission Process - Update Previously Saved Data** For the User to continue updating any previously saved data in the form when an industry report submission has not been completed but saved in progress.	O			O
7.	**Data Capture Brand Via Submission of Required Industry Reports** To perform either of the following actions for each brand submitted in the industry report 13: a. Update the brand information and change the ***Brand Status*** value to "Active" when the brand exists in the Prototype Solution. b. Add the brand information and set the Brand Status value to "Pending" when the brand does not exist in the Prototype Solution.	O			O
8.	**Industry Report – Submission Confirmation** To send an email confirmation to the submitter acknowledging that the submission has been received along with a Submission Confirmation Id (as assessed in Part 1: Capability Scenarios Assessment, Scenario 14, Indicator 5) when industry report data has been successfully submitted.				
Scenario 15. Electronic Data Submission Total Score:					**/25**

Electronic Data Submission: Scenarios 14 and 15 Total Score:	**/50**

Pre-defined Reporting and Templates

Scenario 16. **Pre-Defined Reporting and Templates**

SCENARIO #16 – Pre-defined Reports and Templates

Context

The User generates pre-defined reports from within the Solution on the stored data, where the field values have been set and a given set of user-selectable constraints are available to the User. For example, the User generates a pre-defined report of active establishments from their region with the option to narrow the report to certain types and subtypes of establishments. The User then prints and exports the pre-defined report.
In preparing documentation to be sent to a regulated party concerning non-compliances the User generates a warning letter based on a template.

Scenario #16A – Pre-defined Reporting

The Prototype Solution should have the functionality for the User to:

1. Generate, print and export a pre-defined report detailing a list of active establishments with their addresses.

Scenario #16B – Generating Letters Using Templates

The Prototype Solution should have the functionality for the User to:

1. Select the appropriate template for the letter.
2. Specify the fields values to be included in the letter.
3. Generate the letter.

Reporting and Templates - Scoring Grid

Indicator #	Indicators	Did Not Demonstrate (0)	Partially Demonstrated (1)	Mostly Demonstrated (3)	Fully Demonstrated (5)
	The Prototype Solution should have the functionality :				
1.	**Pre-defined reports with user-selectable constraints: List of Active Establishments** **For the User to generate a pre-defined report showing all establishments in Ottawa with a status value of "Active" and based on user-selectable constraints showing the list of establishments where the following are met:** **a. the following field values have already been set:** **i. Establishment Status value of "Active";** **ii. Region value of "East";** **iii. City value of "Ottawa".** b. the User can select values of other fields to further limit the report results, for example: i. ***Establishment Type;*** ii. ***Establishment Subtype.***	O			O

2.	**Print a Pre-defined Report** For the User to print a pre-defined report showing the list of active establishments.	O			O
3.	**Export a Pre-defined Report** For the User to export a pre-defined report showing the list of active establishments in the following file formats: a. Txt; b. Csv; c. Pdf. ***0 Points Export is not demonstrated*** ***1 Point if the report can be exported in one of the export formats*** ***3 Points if the report can be exported in no fewer than two of the export formats*** ***5 Points if the report can be exported in three or more formats***	O	O	O	O
4.	**Generate documents from templates** For the User to generate documents based on templates.	O			O
Scenario 16. Pre-defined Reporting and Templates Total Score:					**/20**

Part 1: Total Capability Scenarios Assessment Score

PART 1: TOTAL CAPABILITY SCENARIOS ASSESSMENT SCORE: (SUM OF TOTAL SCORES FOR SCENARIOS 1 TO 16)	**/1200**

PART 2: GENERAL PROTOTYPE SOLUTION SPECIFICATIONS ASSESSMENT

CAPABILITY AND USABILITY ASSESSMENT – PART 2: GENERAL PROTOTYPE SOLUTION SPECIFICATIONS ASSESSMENT			
Indicator #	**General Prototype Solution Specifications Indicators** **The Prototype Solution should have the functionality:**	**Not Demonstrated (0)**	**Demonstrated (10)**
1.	**Display of Context Specific Help** To display the context specific Help information in the "Establishment Information" component such that it will minimally affect the current work of the User. For example, in a new window, pop up, tooltip.	O	O
2.	**Concurrent Users** To permit up to 6 concurrent Users without degradation to the Prototype Solution's performance.	O	O
3.	**Prototype Solution Modules** **To provide the following modules:** **a. C&E:** **i. Work Plan and Workload** **ii. Establishment Profile** **iii. Compliance and Enforcement (C&E) Activity** **iv. Reporting** v. Search vi. User Management vii. Application Management	O	O
4.	**Single Sign On** For the User to log in through single sign-on (SSO) .	O	O
5.	**Workflow – Move to Next Step** To move the User to the next step in the business process workflow upon completion of a step in the workflow. For example, the User should be moved from the "Scope Plan" step to the "Compliance Assessment" step in the business process workflow for C&E activities.	O	O
6.	**Workflow Information Update** For the User to navigate to a previously confirmed (that is, locked down) workflow step to view and update information that has not been set to read-only. For example, the User should be permitted to navigate to a previously confirmed General Information component of the Activity "tabbed pane" to update the ***Bring Forward Date*** value.	O	O
7.	**Resume Last Workflow Step** For the User to resume updating information at the last workflow step that was worked on previously, when returning to a business process workflow.	O	O
8.	**Confirm Workflow Step**	O	O

	To alert the User that choosing to continue will lock information (that is, set data to read-only) in the field set/component when the User indicates a workflow step is complete. To set the data in the field set/component that has been locked to read-only when the User confirms a workflow step is complete. .		
9.	**Save** For the User to save data entered at any point in a workflow and continue the workflow.	O	O
10.	**Loss of Unsaved Data** To provide the User with the option to cancel an action that would result in the loss of any data entered but not yet saved.	O	O
11.	**Business Rules** For the Prototype Solution Administrator to configure the business rules without the need to modify the Prototype Solution code.	O	O
12.	**Immediate Effect of Prototype Solution Changes** To ensure any changes to the Prototype Solution take immediate effect.	O	O
13.	**Linked Files List** To display a list of all files contextually associated with the item in the GUI. For example, all documents associated with a single activity record.	O	O
14.	**Preview Attached Files** To provide a preview pane to view the attached file. For example, when the User selects an attached file, the User selects a preview option where the file viewer displays the file within the GUI. Files can be: a. Image files (jpg, png, etc.); b. Word files version 2003 or higher; c. Excel files version 2003 or higher; d. PDF files.	O	O
15.	**Open Attached Files in Native Application** For the User to open attached files in the file's native software applications installed on Government of Canada computers. For example: a. a .jpg image file is opened using Windows Photos. b. a word document is opened using MS Word. c. an excel document is opened using MS Excel. d. a .pdf file is opened using Foxit PhantomPDF.	O	O
16.	**References to External Document Management Systems** For the User to enter read-across linkages across multiple platforms. For example, GC Docs.	O	O
17.	**Export Data** For the User to export the following Prototype Solution data: a. Results from a search; b. Workload Overview (dashboard) view based on current filters and sorts; c. Originally submitted industry reports. Export formats should include: a. Txt;	O	O

	b. Csv; c. Pdf.		
18.	**Print** For the User to print each of the following: a. Search results; b. Complete establishment information; c. Complete activity information: d. Workload Overview (dashboard) view.	O	O
19.	**Print Preview and Print Quantity** For the User to: a. Preview the information to be printed; b. Select the number of copies to be printed.	O	O
20.	**Notifications and Alerts Document** To perform the following actions: a. Display Notifications in a specific notification area of the Prototype Solution. b. Display Alerts as triggered.	O	O
21.	**Email Notification** To generate and send emails based upon events (triggers), other than the trigger identified in Part1: Scenario 14 Indicator 5.	O	O
22.	**Email Notification Frequency** To provide a default email notification frequency. For example, the default email notification frequency is set to weekly.	O	O
23.	**Notifications For Specific Users** To send email notifications that are applicable only to the specified User.	O	O
24.	**Recurring Email Notification Based on User Action** To resend an email notification that requires User action at a set notification frequency, if the User defers the required action, until the User performs the required action.	O	O
25.	**Notification Receipt** To document the date a notification is accessed when either of the following occurs: a. When the User views the notification in the notification area of the Prototype Solution. b. When the User accesses the link within the email notification.	O	O
Part 2: General Prototype Solution Specifications Assessment Total Score:			**/250**

PART 3: WORK PLAN/WORK LOAD ASSESSMENT

CAPABILITY AND USABILITY ASSESSMENT – PART 3: WORK PLAN/WORK LOAD ASSESSMENT			
Indicator #	**Work Plan/Work Load Indicators** **The Prototype Solution should have the functionality:**	**Not Demonstrated (0)**	**Demonstrated (10)**
1.	**Workload Planning**	O	O

	For the User to define their workload plan by creating activities and defining the activity scope and future start date.		
2.	**Default Workload Overview** To provide up to date Workload Overview (dashboard) for the following Users: a. For Supervisor: Activities (and core information including assigned User) grouped by a region or sub-region within a chosen time period. b. For Subordinate: Activities the User has, or has had, control of within a chosen period. c. For Dual Role (Supervisor and Subordinate): i. Activities (and core information including assigned User) grouped by a region or sub-region within a chosen time period. ii. Activities the User has, or has had, control of within a chosen time period. For example: a. Supervisor – see own work and that of their subordinates. b. Subordinate – see own work only.	O	O
3.	**Anticipated Workload Display** To display, in the Anticipated Workload field set of the Workload Overview (dashboard), a schedule of industry reports for the ***Designated User*** based on the submission frequency for a specified period by specified manufacturer(s) in various User-selected display formats, for example, calendar, list, etc.	O	O
4.	**Establishment Profile Information** To provide a direct link via the ***Establishment Name*** value to the establishment information of each establishment listed in the User's Workload Overview (dashboard).	O	O
5.	**New Activities** To provide an up to date Workload Overview (dashboard) displaying the following field sets: a. My Workload - activities the User currently has control of, including newly assigned and created activities. b. Activities of Previous Interest – activities in which the User has interact with, but no longer has control of.	O	O
	Part 3: Work Plan/Work Load Assessment Total Score:		**/50**

PART 4: USER INTERFACE AND USABILITY ASSESSMENT

CAPABILITY AND USABILITY ASSESSMENT – PART 4: USER INTERFACE AND USABILITY ASSESSMENT			
Indicator #	**User Interface and Usability Indicators** ~~**The Prototype Solution should have the functionality:**~~	**Not Demonstrated (0)**	**Demonstrated (10)**
1.	**Organization of Data Entry Fields** To provide the User with a logical organization of fields that share the same space. For example: a. Grouping related fields into field sets; b. Grouping related field sets into components;	O	O

	c. Grouping related components into a tabbed pane.		
2.	**Show and Hide Relevant Fields, Field Sets, and Components** To show and hide fields, field sets, and components in the GUI depending on the relevance of that field, field set, and component based on the context of data previously entered. For example, display fields for input of additional information where the value in another field is "Yes".	O	O
3.	**Input Control** To use input controls to ensure valid data are entered. For example: a. Pick lists; b. Multi-select pick lists; c. Check boxes; d. Radio buttons; e. Dropdown lists; f. List boxes; g. toggles; h. Date picker; i. Form data validation.	O	O
4.	**Context Relevant Data Options** To display, for selection purposes, only the input options that apply based on the context of the data previously entered. For example: a. A city list would be restricted to the values associated with the previously selected province or territory value. b. A brand list would be restricted to the values associated with the previously selected establishment value.	O	O
5.	**Data Entry Format Display** To indicate in the GUI the required data entry format in the label or placeholder text for field that require specifically formatted input. For example: a. Dates; b. Times; c. Postal codes.	O	O
6.	**Mandatory Data Fields: Indication, Validation, Notification** To control mandatory fields in the following way: a. Visually indicate to the User mandatory fields in a consistent manner on all data input screens. b. Visually indicate to the User invalid upon entry, for example, non-numeric characters in a numeric field. c. Alert the User of any of the following when the User attempts to confirm completion of data entry step (for example, submitting an industry report via the guided form-based submission process): i. Any field requiring validation that has not passed data validation. ii. Any mandatory fields missing values. d. Navigate the User directly to the first instance of any of the following: i. Invalid data in a field; ii. Missing mandatory data.	O	O

	e. Permit the User to complete or correct the input for all fields and repeat the confirmation data entry completion action. f. Permit the User to repeat the confirmation of completing the data entry. g. Set validated and confirmed fields to read-only.		
7.	**Conditionally Mandatory Fields** To configure conditionally mandatory fields.	O	O
8.	**Undefined and Unselected Field Values** To indicate when a field has not been populated with a value by the User and has not been populated with a value by the Prototype Solution. For example: a. Default value for a pick list is "Select". b. Default state for a check box is not selected.	O	O
9.	**Clear Values** For the User to clear an existing value from the User editable field where the User cannot delete the value. For example: a. Click an eraser icon to clear: i. a date field; ii. a radio button set. b. Click an "x" to clear a filter or search term.	O	O
10.	**Reset Data Entry Forms** For the User to clear all User entered values from a form and reset any default values.	O	O
11.	**Read-only Fields** To visually indicate read-only fields from fields where data entry is permitted. For example: a. Grey out; b. Prevent data input.	O	O
12.	**Null Field Values** To visually indicate an empty or null field value and set the field to read-only. Example of a visual indicator: a. "n/a"'; b. "-".	O	O
13.	**Data Validation** To enforce data validation rules.	O	O
14.	**Real-Time Updates** To refresh the value of a field displayed in the GUI, as soon as that value is updated: a. A calculation; b. Derived from logic.	O	O
15.	**Calculated and Derived Data Values** To calculate, derive, and display values based on user-entered or Prototype Solution-stored information. Upon entry of the field values, the Prototype Solution should generate calculated and derived values and update the GUI with the values in real-time. For example:	O	O

	a. The User enters data into numeric fields A and B. The Prototype Solution displays the sum in a third calculated numeric field C. b. The User enters data into four numeric fields. The Prototype Solution displays the standard deviation in a fifth, calculated, numeric field. c. The User sets two ***Legislation Section Compliance Outcome*** values as "No Evidence of Non-Compliance", and one ***Legislation Section Compliance Outcome*** value as "Non-Compliant". The Prototype Solution uses logic on the text values to derive and display the ***Activity Compliance Outcome*** text value as "Non-Compliant".		
16.	**Time Format** To store all times in Coordinated Universal Time (UTC) format with offset for the time zone.	O	O
17.	**User-Entered Time Zone** For the User to select the time zone for any time entered.	O	O
18.	**Default Offset Time Zone** To set the default-offset time zone to that of the User's time zone.	O	O
19.	**User-Entered Time Display** To display all user-entered times in the time zone of the User who entered the time.	O	O
20.	**System-Generated Time Display** To display all system-generated times in the User's time zone.	O	O
21.	**Large Data Values** For the User to view the entire value of a field when the length of the value is larger than the display width of the field (for example, in a multi-column list view (table/data grid), or dropdown lists), for example, mouse-over display or in a manner that does not disrupt the layout.	O	O
22.	**Language** To provide all GUI elements in English.	O	O
23.	**Default Sort Order** To default all sorts using standard sort parameters unless explicitly identified. For example, alphabetical (a to z), numerical (0 to 9), and reverse chronological dates.	O	O
24.	**Legislative Display Order** **To display contextually relevant Legislative Sections/Subsections values sorted by Parts, Sections (within parts) and Regulations (within Sections) in ascending order, that is, using natural sort order where multi-digit numbers are treated atomically.** **For example:** **a. Part I – Tobacco Products** **i. 5 – Product Standards** **ii. 5.1 Prohibition – Manufacture** **iii. 5.2 Prohibition – Sale** **iv. 6(1) – Information required** **v. 6(2) – Supplementary Information** **vi. 6.1 – Disclosure** **b. Part II Access** **i. 8(1) – Furnishing to Youth** **ii. 9(1) – Sending and Delivering** **iii. 9.1(1) – Interprovincial Sending and Delivering** **iv. 9.1(2) – Advertising**	O	O

25.	**Default Case Insensitive Sort** To default all sorts to be case insensitive. For example, variations of the spelling of "Montreal" would appear in the sorted list together, regardless of the case contained in the spelling when case insensitive is selected: a. montreal b. Montreal c. MONTREAL	O	O
26.	**"Case" Sort** For the User to select the option to change the sort from sensitive to insensitive to case.	O	O
27.	**"Diacritic" Sort** For the User to select the option to change the sort from sensitive to insensitive to diacritic/accents, for example, à, é, ç. For example, variations of the spelling of "Montreal" would appear in the sorted list together, regardless of the accented characters contained in the spelling: a. Montreal b. Montréal	O	O
28.	**Updating a Record Listed in a Multi-column List View (table/data grid)** For the User to select a record in any multi-column list view (table/data grid) to access it directly for updating, and return to the multi-column list view after the action on the record is completed. For example, selecting an activity from within an establishment profile will open the activity to update.	O	O
29.	**Viewing a Record Listed in a Multi-column List View (table/data grid)** For the User to select a record in any multi-column list view (table/data grid) to access it directly for viewing, and return to the multi-column list view after the action on the record is completed. For example, selecting an establishment profile from within an activity will open the relevant establishment's profile for viewing.	O	O
30.	**Filtering in a Multi-Column List View (table/data grid)** For the User to filter any multi-column list view (table/data grid) by any criteria or combination of criteria. For example: a. Filter by ***Activity Type;*** b. Filter by ***Priority;*** c. Filter by ***Proposed Start Date*** (including activities with future start dates); d. Filter by specific ***Province or Territory*** and ***Establishment Type*** within the specified ***Province(s) and Territory(s);*** e. Filter by ***Report Section.***	O	O
31.	**Close Modal Windows** For the User to close and cancel any modal windows at any time. For example, windows used to display information or help.	O	O
32.	**Move Modal Windows** For the User to move any modal windows so as not to obscure the data displayed in the parent screen. For example, windows used to display information or help.	O	O

33.	**Data Viewing Without An External Tool** For the User to access and view data related to activities and establishments wherever identified within the Prototype Solution without having to access an external tool. For example, all related activity data is viewable from within the establishment. The User is not required to view related activity data in a separate tool.	O	O
34.	**Prototype Solution Version** For the User to identify the current version of the Prototype Solution, for example, by version number.	O	O
35.	**Establishment "Tabbed Pane-like" Format and Components** To provide a tabbed pane-like format, for data input and viewing of all information relating to an establishment. The Establishment "tabbed pane" should be composed of the following components: a. Establishment Information; b. Concerns and Issues; c. Contacts (includes contact details); d. Associated Activities (includes compliance and enforcement history); e. Comments; f. Products and Brands (Establishments with ***Establishment Type*** value of "Manufacturers" only; includes counts); g. Industry Reporting History (Establishments with ***Establishment Type*** value of "Manufacturers" only).	O	O
36.	**Establishment "Establishment Information" Component** To provide the following field sets and related fields in the Establishment Information component of the Establishment "tabbed pane", for data input and viewing purposes: a. Establishment (Establishment Id, Establishment Name, Address); b. Mailing Address; c. Email; d. Phone; e. Ownership; f. Status; g. ***Establishment Assigned*** To; h. Establishment Type displayed in a multi-column list view format; i. Online Presence (for example: web site, social media) displayed in a multi-column list view format; j. As***sociated Establishments*** displayed in a multi-column list view format.	O	O
37.	**Establishment "Concerns and Issues" Component** **To provide the following field sets and related fields displayed in a multi-column list view format in the Concerns and Issues component of the Establishment "tabbed pane", for data input and viewing purposes:** **a. Concerns:** **i. Concern Id;** **ii. Date;** **iii. User Name;** **iv. Concern.** **b. Issues:** **i. Issue Id;** **ii. Date;** **iii. User Name;** **iv. Issue.**	O	O
38.	**Establishment "Contacts" Component**	O	O

	To provide the following field set and related fields displayed in a multi-column list view format in the Contacts component of the Establishment "tabbed pane", for data input and viewing purposes: a. Contacts: i. Contact Id; ii. Full Name; iii. Title; iv. Phone Descriptor; v. ***Phone Number;*** vi. ***Email Descriptor;*** vii. ***Email Address;*** viii. ***Language.***		
39.	**Establishment "Associated Activities" Component** To provide Activities associated with the establishment displayed in a multi-column list view format in the Activities component of the Establishment "tabbed pane", for data input and viewing purposes.	O	O
40.	**Establishment "Comments" Component** To provide the Comment History field set and related fields in the Comments component of the Establishment "tabbed pane", for data input and viewing purposes.	O	O
41.	**Establishment "Products and Brands" Component** To provide the following field sets and related fields displayed in a multi-column list view format in the Product and Brands component of the Establishment "tabbed pane" for data input and viewing purposes: a. Product; b. Brands.	O	O
42.	**Establishment "Industry Reporting History" Component** To provide the following field sets and related fields displayed in a multi-column list view format in the Industry Reporting History component of the Establishment "tabbed pane", for data input and viewing purposes: a. Overall Industry Report History; b. Industry Reports With No Associated Activity.	O	O
43.	**Activity Tabbed Pane-like Format and Components** To provide a tabbed pane -like format for data input and viewing of all information relating to an activity. The Activity "tabbed pane" should be composed of the following components and in the specified order: a. General Information; b. Scope Plan; c. Compliance Assessment; d. Enforcement Actions; e. Close.	O	O
44.	**Activity "General Information" Component** **To provide the following field sets and related fields in the General Information component of the Activity "tabbed pane", for data input and viewing purposes:** **a. Establishment related information field sets:** **i. Establishment (Est. Id, Establishment Name, Est. Status, Est. Type, location information, and Concerns and Issues, and Age Restricted Icons);** **ii. Establishment Contacts displayed in a multi-column list view format;** **iii. Associated Establishments displayed in a multi-column list view format;** **iv. Other Activities for this Establishment displayed in a multi-column list view** format.	O	O

	• Activity Timeline; • Sent To History displayed in a multi-column list view format; • Warrants (if applicable) displayed in a multi-column list view format; • Online Presence (for example: web site, social media) displayed in a multi-column list view format; • Links (to files) displayed in a multi-column list view format; • Comment History. c. ***Confirm When Completed*** (field).		
45.	**Activity "Scope Plan" Component Format** To provide the following field sets and related fields in the Scope Plan component of the Activity "tabbed pane", for data input and viewing purposes: a. ***Activity Scope Plan Type*** (field); b. Activity ***Scope*** Details; c. ***Confirm When Complete*** (field***).***	O	O
46.	**Activity "Compliance Assessment" Component** To provide the following field sets and related fields in the Compliance Assessment component of the Activity "tabbed pane", for data input and viewing purposes: a. Establishment Location Verification; b. Person Spoken To (displayed in a multi-column list view format); c. Add Scope; d. Compliance Results (displayed in a multi-column list view format; e. Artifacts Summary (displayed in a multi-column list view format); f. Responsible Party Summary (displayed in a multi-column list view format); g. ***Confirm When Completed*** (field).	O	O
47.	**Activity "Enforcement Actions" Component** To provide the following field sets and related fields in the Enforcement Actions component of the Activity "tabbed pane", for data input and viewing purposes: a. Recommended Enforcement Action, in a multi-column list view format: i. Warning Letter; ii. Warning Letter Links. b. A field set for each available enforcement action; c. ***Confirm When Completed*** (field).	O	O
48.	**Activity "Link/Close" Component Format** To provide the following field sets and related fields in the Link/Close component of the Activity "tabbed pane" for data input and viewing purposes: a. Recommended Next Steps; b. Justification; c. ***Activity Completed*** (field).	O	O
49.	**Activity "Compliance Assessment" Component Establishment Location Verification Format** To provide the following fields in the Establishment Location Verification field set in the Compliance Assessment component of the Activity "tabbed pane", for data input and viewing purposes: a. ***Activity Establishment Verification Code;*** b. ***Actual Start Date;*** c. ***Actual Start Time;*** d. ***Search Warrant Executed;*** e. C***onfirm When Completed.***	O	O
50.	**Activity "Compliance Assessment" Component Person Spoken To Format**	O	O

	To provide the following fields in the Person Spoken To field set in the Compliance Assessment component of the Activity "tabbed pane", for data entry and viewing purposes: a. ***Name of Person Spoken To;*** b. ***Title;*** c. ***Phone;*** d. ***Email;*** e. ***Establishment Profile Verified.***		
51.	**Activity "Compliance Assessment" Component Compliance Results Format** **To provide the following fields displayed in a multi-column list view format in the Compliance Results field set in the Compliance Assessment component of the Activity "tabbed pane" for data entry and viewing purposes:** **a. Legislation;** **b. Legislation Section Compliance Outcome, with the following selection values:** **i. "Not Inspected";** **ii. "Not Applicable";** **iii. "No Evidence of Non-Compliance";** **iv. "Non-Compliance".** d. ***Analysis Type;*** e. ***Artifacts Added;*** f. ***Number of Artifacts.***	O	O
52.	**Artifact "Tabbed Pane" like Format and Components** To provide an Artifact tabbed pane-like format for data input and viewing of all information relating to an artifact. The Artifact "tabbed pane" should be composed of the following components: a. Collection; b. Analysis; c. Links. The format of the Collection and Analysis components of the Artifact "tabbed pane" will depend on the selected ***Artifact Analysis Type*** value.	O	O
53.	**Artifact: Header Information Format** To provide a header field set in the Artifact "tabbed pane" for the display of artifact information that remains the same across all components of the Artifact "tabbed pane". For viewing purposes, the header section should be composed of the following fields: a. ***Establishment Name;*** b. ***Artifact Id;*** c. ***Legislative Section/Subsection;*** d. ***Artifact Analysis Type.***	O	O
54.	**Artifact: "Collection" Component Format** To provide the applicable artifact collection fields in the Collection component of the Artifact "tabbed pane", for data input and viewing purposes, according to the following values: a. The selected ***Artifact Analysis Type*** value; b. The selected ***Legislative Section/Subsection*** value.	O	O
55.	**Artifact: "Analysis" Component Format**	O	O

	To provide the application artifact analysis fields within the Analysis component of the Artifact "tabbed pane", for data input and viewing purposes, according to the following values: a. The selected Artifact Analysis Type value; b. The selected ***Legislative Section/Subsection*** value.		
56.	**Artifact: "Links" Component Format** To provide the following fields in a multi-column list view format within the Links component of the Artifact "tabbed pane", for data input and viewing purposes: a. ***Link Id Number;*** b. ***File name*** (of document being linked); c. ***Description*** (of the linked document); d. ***Linked By*** (User Name); e. ***Linke***d ***Date.***	O	O
57.	**Activity "Compliance Assessment" Component Artifact Summary** To provide the following fields displayed in a multi-column list view format in the Artifacts Summary field set in the Compliance Assessment component of the Activity "tabbed pane" for update and viewing purposes: a. ***Artifact Id;*** b. ***Legislation;*** c. ***Compliance Result;*** d. ***Description.***	O	O
58.	**Activity "Compliance Assessment" Component Responsible Party** To provide the following fields displayed in a multi-column list view format in the Responsible Party field set in the Compliance Assessment component of the Activity "tabbed pane" for update and viewing purposes: a. ***Name;*** b. ***Non-Compliant Legislation;*** c. ***Title;*** d. ***Language;*** e. ***Phone;*** f. ***Email.***	O	O
59.	**Industry Reports Compliance Assessment Component – Compliance Results Format Legislative Section/Subsection** **To provide the following fields displayed in Compliance Results field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes:** **a. In a multi-column list view format:** **i. Legislative Section/Subsection;** **ii. Legislation Section Compliance Outcome:** **1. Not Applicable;** **2. No Evidence of Non-Compliance;** **3. Non-Compliance;** **4. Compliance Outcome Level.** **iii. Number of Errors;** **iv. Non-Compliance History.** b. ***Total Number of Errors;*** c. ***View all Non-Compliance History.***	O	O
60.	**Industry Reports Compliance Assessment Component – Compliance Summary Format**	O	O

	To provide the following fields displayed in a multi-column list view format in the Compliance Summary field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. Activity Compliance Outcome (Displayed as State of Compliance): i. Not Applicable; ii. No Evidence of Non-Compliance; iii. Non-Compliance. b. Compliance Outcome Level (Displayed as Level of Compliance): i. Minor; ii. Major. c. Display the following in a summary multi-column list view format: i. Type by Non-Compliance Level; ii. Number of Non-compliances; iii. Number of errors; iv. The sum total of non-compliances; v. The sum total of errors.		
61.	**Industry Reports Compliance Assessment Component – Sections Overridden Format** To provide the following fields displayed in a multi-column list view format in the Sections Overridden field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. ***Legislative Section/Subsection;*** b. ***Reason.***	O	O
62.	**Industry Reports Compliance Assessment Component – Artifacts Summary Format** To provide the following fields displayed in a multi-column list view format in the Artifacts field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. ***Artifact Id;*** b. ***Legislation*** (Displayed as ***Applicable Legislation).***	O	O
63.	**Industry Reports - Artifact "Analysis" Component** For an ***Artifact Analysis Type*** value of "Industry Report Analysis", provide the following fields in the Artifact pane for viewing purposes: a. ***Artifact Id*** (Solution generated by concatenating Solution generated number + Legislation number + number of artifact for this ***Legislative Section/Subsection*** value, starting at the number 1); b. ***Establishment Name*** (for the activity); c. ***Legislation number and description*** (for which the artifact is being assessed); d. ***Artifact Information*** (Industry report data submitted).	O	O
64.	**Industry Reports Compliance Assessment Component – Compliance Results Format Errors Grouped by Legislative Section/Subsection View** To provide the following field sets and related fields in the "Errors Grouped by Legislative Section/Subsection" view for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. Errors for: [***Legislative Section/Subsection*** value and related text under which the error was identified]; b. Errors in Report (field set); i. System Identified Errors: [Total number of errors] with the following fields displayed in a multi-column list view:	O	O

	1. Brand Name (if applicable); 2. Dimension Field(s); 3. Measure Fields(s); 4. Error Name. ii. User Identified Errors: [Total number of errors] with the following fields displayed in a multi-column list view: 1. Brand Name (if applicable); 2. Dimension Field(s); 3. Measure Fields(s); 4. Error Name.		
Part 4: User Interface and Usability Assessment Total Score:			**/640**

PART 5: SEARCH ASSESSMENT

CAPABILITY AND USABILITY ASSESSMENT – PART 5: SEARCH ASSESSMENT			
Indicator #	**Search Indicators** **The Prototype Solution should have the functionality:**	**Not Demonstrated (0)**	**Demonstrated (10)**
1.	**Ad-hoc Search** To permit the User to search on specific record types and combinations of record types stored in the Prototype Solution as follows: a. Search for Establishment Profiles by Activities.	O	O
2.	**Establishment Profile Search** To provide a pre-defined Establishment Profile Search, with the following default values populated, for a User to search for an establishment: a. ***Establishment Status*** value is "Active"; b. ***Establishment Province*** value is the User profile province value; c. ***Establishment Region*** value is the User profile region value; d. ***Establishment Sub-Region*** value is the User profile sub-region value. Pre-defined Establishment Profile Search should consist of the following fields: a. ***Establishment Id;*** b. ***Establishment Name;*** c. ***Establishment Street;*** d. ***Establishment City;*** e. ***Establishment Province;*** f. ***Establishment Postal Code;*** g. ***Establishment Region;*** h. ***Establishment Sub-Region;*** i. ***Establishment Type;*** j. ***Establishment Sub-type;*** k. ***Establishment Status.***	O	O
3.	**Activity Search** To provide a pre-defined Activity Search, with the following default values populated, for the User to search for an activity: a. ***Establishment Province*** value is the User profile province value;	O	O

	b. ***Establishment Region*** value is the User profile region value; c. ***Establishment Sub-Region*** value is the User profile sub-region value. Pre-defined Activity Search should consist of the following fields: a. ***Activity Id;*** b. ***Activity Type;*** c. ***Activity Status;*** d. ***Compliance Status;*** e. ***Establishment Name;*** f. ***Establishment Street;*** g. ***Establishment City;*** h. ***Establishment Province;*** i. ***Establishment Postal Code;*** j. ***Establishment Region;*** k. ***Establishment Sub-Region;*** l. ***Establishment Type;*** m. ***Establishment Sub-type.***		
4.	**Industry Report Search** To provide a pre-defined Industry Report Search, with the following default values populated, for the User to search for an industry report: a. ***Report Status = "Registered";*** b. ***Submission Date = [Last 12 Months].*** Pre-defined Industry Report Search should consist of the following fields: a. ***Report Id;*** b. ***Report Section;*** c. ***Report Name;*** d. ***Report Period;*** e. ***Report Status;*** f. ***Submission Date;*** g. ***Manufacturer Id;*** h. ***Manufacturer Name;*** i. ***Submitter Name;*** j. ***Activity Number(s).***	O	O
5.	**Brand Search** To provide a pre-defined Brand Search, with the following default values populated, for the User to search for a brand: a. ***Brand Status = "Active".*** Pre-defined Brand Search should consist of the following fields: a. ***Brand Id;*** b. ***Brand Name;*** c. ***Brand Descriptor;*** d. ***Brand Status;*** e. ***Product Type;*** f. ***Product Size;*** g. ***Manufacturer Id;*** h. ***Manufacturer Name.***	O	O
6.	**User Profile Search** To provide a pre-defined User Profile Search, with the following default values populated, for the User to search for the profile: a. User Status = "Active". Pre-defined User Profile Search should consist of the following fields: a. ***User Id;*** b. ***User Name;***	O	O

	c. ***First Name;*** d. ***Last Name;*** e. ***Region.***		
7.	**Enter Search Values** For the User to enter search values.	O	O
8.	**Modify Search Values** For the User to modify the search values.	O	O
9.	**"Contains" Search** To use "contains" match searches, by default, to find items that contain the search value. For example: Search criteria: a. ***Province/Territory*** value is "Ontario" (exact). b. ***Establishment Sub-Type*** value is "Convenience store" (exact). c. ***Establishment Name*** value contains "**Bob"** (contains). Search results would include the following, where all 3 search values were found: Province/Territory | Establishment Sub-Type | Establishment. Name Ontario | Convenience store | **Bob**'s store Ontario | Convenience store | Ke**bob** Express Ontario | Convenience store | **Bob**cat Outdoor	O	O
10.	**"Exact" Search** To provide the User with the option to perform an exact search based on the search values entered. Search criteria example: a. ***Province/Territory*** value is "Ontario" (exact). b. ***Establishment Sub-Type*** value is "Convenience store" (exact).	O	O
11.	**"Case" Search** To provide the User with an option to change the search from case sensitive to case insensitive. For example, variations of the spelling of "Montreal" would appear in the search result list together, regardless of the case contained in the spelling when case insensitive is selected: a. montreal b. Montreal c. MONTREAL	O	O
12.	**"Diacritic" Search** To provide the User with an option to change the search from sensitive diacritic/accents to insensitive diacritic/accents, for example, à, é, ç. For example, variations of the spelling of "Montreal" would appear in the search result list together, regardless of the accented characters contained in the spelling: a. Montreal b. Montréal	O	O
13.	**Search Results Display** To display search results in a multi-column list view format (table/data grid), when a search is performed.	O	O
14.	**Search Result Page Navigation** To provide the User with a method to navigate the search result pages.	O	O

15.	**Result Set Position and Size** To display, in the search results, the following information: a. Total number of search results; b. Current search results range being displayed; c. Current Page; d. Total number of pages. For example, 1 to 20, of 500 results.	O	O
16.	**Preview** To permit the User to preview tombstone data for each search result without having to click through (open) the search result record for viewing and updating. For example, mouse over-like preview.	O	O
	Part 5: Search Assessment Total Score:		**/160**

PART 6: USER ACCOUNT ADMINISTRATION

CAPABILITY AND USABILITY ASSESSMENT – PART 6: USER ACCOUNT ADMINISTRATION			
Indicator #	**User Account Administration Indicators** **~~The Prototype Solution should provide the functionality:~~**	**Not Demonstrated (0)**	**Demonstrated (10)**
1.	**View User Profile Details** For the Account Administrator to view the following field values for a User Profile: a. ***Full Name;*** b. ***User Name;*** c. ***Job Title;*** d. ***User Role;*** e. ***User Level;*** f. ***User Status;*** g. ***Profile Region;*** h. ***Profile Sub-region;*** i. ***Profile Province/Territory;*** j. ***Profile City;*** k. ***Profile Street;*** l. ***Password;*** m. ***Phone Number;*** n. ***Email address;*** o. ***Language Preference.***	O	O
2.	**Create User Profile** For the Account Administrator to create a User Profile.	O	O
3.	**Update User Profile** For the following Users to update a User Profile: a. Account Administrator; b. User who owns the profile.	O	O

4.	**Create User Roles and Assign Privalleges** For the Account Administrator to create User roles and assign privileges to each role. Example, create a role of "Specialist", and set the privilege to "read-only" the ***Activity Type*** value fields within an activity.	O	O
5.	**Assign Rights and Roles** For the Account Administrator to assign rights and roles to a User profile. Example, assign the User profile the role of "Specialist".	O	O
6.	**Assign User Profile Status** For the Account Administrator to set a ***User Status*** value as follows: a. "Inactive" if the User Id is not associated with an activity or establishment. b. "Active" to activate the User account.	O	O
7.	**Delete the User Profile** For the Account Administrator to delete a User profile if the User Id is not associated with an activity or establishment.	O	O
8.	**Create User Groups** For the Account Administrator to create User Groups. Example, the Regional User Group should contain all regional supervisors and subordinates.	O	O
9.	**Assign the User to the User Group** For the Account Administrator to assign a User profile to a User Group.	O	O
10.	**Self-Management of User Preferences** For the User to set their User Profile Preferences for the following User Roles: a. Inspector; b. Supervisor.	O	O
11.	**User Notification Subscription Management** For the User to manage their User notification subscription (scheduled and event driven). Example, the User selects to receive email notifications weekly showing the number of open activities in their Workload Overview (dashboard).	O	O
12.	**Notification Via Email Management** For the User to set their preferred notification frequency for each type of solution-generated Email (only one email notification frequency for each solution-generated email notification type).	O	O
13.	**Notification Via Internal Notification Management** For the User to set their preferred notification frequency for each type of solution-generated internal notification.	O	O
14.	**User Preferences for Alerts** For the User to set their preference to show/hide system alerts. Example, for loss of unsaved data.	O	O
15.	**User Profile Management** For the User to update their User profile for the following fields: a. ***Full Name;*** b. ***Profile Region;*** c. ***Profile Sub-region;*** d. ***Profile Province/Territory;*** e. ***Profile City;*** f. ***Profile Street;*** g. ***Password;***	O	O

	h. ***Phone Number;*** i. ***Email address;*** j. ***Language Preference;***		
Part 6: User Account Administration Assessment Total Score:			**/150**

PART 7: SYSTEM USABILITY SCALE (SUS) ASSESSMENT

CAPABILITY AND USABILITY ASSESSMENT – PART 7: SYSTEM USABILITY SCALE (SUS) ASSESSMENT

Instructions: For each of the following statements, mark one box that best describes your reactions to the Prototype Solution.

Scenario #: _____ **Date:** _____/_____/_____

#	Indicator	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1.	I think that I would like to use this Prototype Solution frequently.	☐	☐	☐	☐	☐
2.	I found this Prototype Solution unnecessarily complex.	☐	☐	☐	☐	☐
3.	I thought this Prototype Solution was easy to use.	☐	☐	☐	☐	☐
4.	I think that I would need assistance to be able to use this Prototype Solution.	☐	☐	☐	☐	☐
5.	I found the various functions in this Prototype Solution were well integrated.	☐	☐	☐	☐	☐
6.	I thought there was too much inconsistency in this Prototype Solution.	☐	☐	☐	☐	☐
7.	I would imagine that most people would learn to use this Prototype Solution very quickly.	☐	☐	☐	☐	☐
8.	I found this Prototype Solution very cumbersome/awkward to use.	☐	☐	☐	☐	☐
9.	I felt very confident using this Prototype Solution.	☐	☐	☐	☐	☐
10.	I needed to learn many things before I could get going with this Prototype Solution.	☐	☐	☐	☐	☐
11.	I found navigating the Prototype Solution with a keyboard was easy.	☐	☐	☐	☐	☐
12.	I found the content was easily readable because the contrast was sufficient.	☐	☐	☐	☐	☐
13.	I found the content was easily readable because the font size was sufficient.	☐	☐	☐	☐	☐
14.	I found the language used was plain, clear, and simple to understand.	☐	☐	☐	☐	☐
15.	I found the pages were well labeled with a title.	☐	☐	☐	☐	☐

16.	I found the quantity of content on each page was reasonable.	☐	☐	☐	☐	☐
17.	I found moving through the workflow intuitive.	☐	☐	☐	☐	☐
18.	I found moving through the workflow frustrating.	☐	☐	☐	☐	☐
19.	Overall, I found the Prototype Solution provided a consistent, predictable, intuitive experience.	☐	☐	☐	☐	☐
20.	Overall, I found the Prototype Solution provided a consistent Graphical User Interface (GUI) that made it highly usable. For example, consistent labelling, field placement, input feedback, notifications, keyboard-friendly input and general behaviour.	☐	☐	☐	☐	☐
	Part 7: Total System Usability Scale Assessment Total Score:					**/ 200**

Note 1 - Scoring Calculations:

X = (Sum of Points for Questions 1, 3, 5, 7, 9, 11 to 17, 19 and 20) *(For each of the listed numbered questions, subtract 1 from the score)*

Y = (Sum of Points for Questions 2, 4, 6, 8, 10 and 18) *(For each of the listed numbered questions, subtract their value from 5)*

Total System Usability Scale Score = (X + Y) * 2.50

APPENDIX B - FULL SOLUTION REQUIREMENTS

A. General Specifications

#	Title	Requirement
A1.	Solution Modules	The Solution must have the functionality to provide the following modules: a. C&E i. Work Plan and Workload (Section B) ii. Establishment Profile (Section E) iii. Compliance and Enforcement (C&E) Activity (Sections F to O) iv. Reporting (Section R) v. Search (Section D) vi. User Management (Section U) vii. Application Management (Section U) b. Secure Portal i. Complaints, Enquiries, and Support Requests (Section P) ii. Electronic Data Submission (Section Q) c. Secure REST API i. Electronic Data Submission (Section Q) d. Off-Line (Section T) e. Business Intelligence and Data Analytics (Section S)
A2.	Single Sign On	The Solution must have the functionality for the User to log in through single sign-on (SSO).
A3.	Workflow Implementation	The Solution must have the functionality to configure all business process workflows. For example: a. Create New Establishment Profile (See Requirement E3) b. Create New Activity (See Requirement F3) c. Create New User d. Create User Group e. Create a Complaint (See Requirement P2) f. Create an Enquiry (See Requirement P9) g. Create a Support Request (See Requirement P17) h. Register a Submitted Industry Report (See Requirement Q8)
A4.	Documentation of Work	The Solution must have the functionality for the User to document all work performed in connection with a business process workflow.
A5.	Workflow – Move to Next Step	The Solution must have the functionality to move the User to the next step in the business process workflow upon completion of a step in the workflow. For example, the User must be moved from the "Scope Plan" step to the "Compliance Assessment" step in the business process workflow for C&E activities.
A6.	Workflow Information Update	The Solution must have the functionality for the User to navigate to a previously confirmed (that is, locked down) workflow step to view and update information that has not been set to read-only. For example, the User must be permitted to navigate to a previously confirmed General Information component of the Activity "tabbed pane" to update the ***Bring Forward Date*** value.
A7.	Resume Last Workflow Step	The Solution must have the functionality for the User to resume updating information at the last workflow step that was worked on previously, when returning to a business process workflow.
A8.	Confirm Workflow Step	The Solution must have the functionality to alert the User that choosing to continue will lock information (that is, set data to read-only) in the field set/component when the User indicates a workflow step is complete.

#	Title	Requirement
		The Solution must have the functionality to set the data in the field set/component that has been locked to read-only when the User confirms a workflow step is complete.
A9.	Save	The Solution must have the functionality for the User to save data entered at any point in a workflow and continue the workflow.
A10.	Loss of Unsaved Data	The Solution must have the functionality to provide the User with the option to cancel an action that would result in the loss of any data entered but not yet saved.
A11.	Business Rules	The Solution must have the functionality for the Solution Administrator to configure business rules without the need to modify the Solution code.
A12.	Fields	The Solution must have the functionality to configure fields and implement the rules associated with the fields.
A13.	Immediate Effect of Solution Changes	The Solution must have the functionality to ensure any changes to the Solution take immediate effect.
A14.	Linked Files List	The Solution must have the functionality to display a list of all files contextually associated with the item in the graphical user interface (GUI). For example, a list of all documents associated with a single activity record.
A15.	Preview Attached Files	The Solution must have the functionality to provide a preview pane for the User to view the attached file. For example, when the User selects an attached file, the User selects a preview option where the file viewer displays the file within the GUI. Files can be: a. Image files (jpg, png etc.); b. Word files version 2003 or higher; c. Excel files version 2003 or higher; d. PDF files.
A16.	Open Attached Files in Native Application	The Solution must have the functionality for the User to open attached files in the file's native software applications installed on Government of Canada computers. For example: a. a .jpg image file is opened using Windows Photos; b. a word document is opened using MS Word; c. an excel document is opened using MS Excel; d. a .pdf file is opened using Foxit PhantomPDF.
A17.	References to External Document Management Systems	The Solution must have the functionality for the User to enter read-across linkages across multiple platforms. For example, GC Docs.
A18.	Export Data	The Solution must have the functionality for the User to export any Solution data, including: a. Pre-defined reports. b. Results from a search. c. Workload view based on current filters and sorts. d. Originally submitted industry reports, including a bulk selection of originally submitted industry reports. e. Attached files. Export file formats must include: a. txt b. csv c. pdf
A19.	Exporting Industry Reports	The Solution must have the functionality to perform any necessary transformations to ensure that the industry report is readable in the format selected for export When exporting industry reports.

#	Title	Requirement
		For example, if a Section 13 Sales industry report is being exported in pdf format, the Solution must transform and arrange the sales data by market segment, brand, and province resembling the original Section 13 reporting template in order for it to be readable and viewable prior to being exported in pdf format.
A20.	Print	The Solution must have the functionality for the User to print. For example: a. search results b. complete establishment information c. complete activity information d. pre-defined reports e. forms f. templates g. workload h. linked files i. letters j. receipts k. industry reports
A21.	Print Preview and Print Quantity	The Solution must have the functionality for the User to: a. Preview the information to be printed b. Select the number of copies to be printed
A22.	Bulk Print Activities	The Solution must have the functionality for the User to bulk print selected activities.
A23.	Print Non Populated Forms	The Solution must have the functionality for the User to print blank (not pre-populated) forms.
A24.	Print Pre-populated Activity Forms	The Solution must have the functionality for the User to print a form for a selected activity, which includes details of a related promotional event (if applicable) and the description of any related linked file(s).
A25.	Print Pre-populated Artifact Forms	The Solution must have the functionality for the User to print forms relating to the collected Artifact. For example: a. Artifact Tracking form – Copy remains with artifact b. Artifact Receipt – Copy provided to Manufacturer / Retailer c. CIP Sample form
A26.	Notifications and Alerts	The Solution must have the functionality to: c. Display Notifications in a specific notification area of the Solution d. Display Alerts as triggered
A27.	Email Notification	The Solution must have the functionality to generate and send emails based upon events and triggers. For example, when an industry report is successfully submitted it triggers an email confirmation to be sent to the submitter with the ***Submission Confirmation Id*** value.
A28.	Email Notification Frequency	The Solution must have the functionality to provide a default value for email notification frequency. For example, the default value for email notification frequency is set to weekly.
A29.	Recurring Email Notification Based on User Action	The Solution must have the functionality to resend an email notification that requires User action at a set notification frequency, if the User defers the required action, until the User performs the required action.
A30.	Email Notifications For Specific Users	The Solution must have the functionality to send email notifications that are applicable only to the specified User.

#	Title	Requirement
A31.	Notification Area	The Solution must have the functionality to: a. Display notifications within a specific notification area of the Solution. b. Notify the User, using a visual indicator, of any new unread notifications in the notification area of the Solution. Examples of visual notification indicators would be: a. an icon on the GUI showing the number of unread notifications b. bolded unread notifications c. pop-up
A32.	Notification Receipt	The Solution must have the functionality to document the date a notification is accessed when either of the following occurs: a. When the User views the notification in the notification area of the Solution. b. When the User accesses the link within the email notification.
A33.	Email Notification Links	The Solution must have the functionality to support read-across linkages to the activity/establishment record so that the User may open the activity/establishment directly from the email when the activity/establishment information is included in an email notification.
A34.	Third Party Data Sources	The Solution must have the functionality to utilize results from APIs of third party data sources, such as: a. Canada Post Address Complete Service b. Chemical Abstract Service (CAS) Registry c. Global Location Number (GLN) d. Revenue Canada
A35.	Access to Audit Data	The Solution must have the functionality for the User to access audit data.

B. Work Plan/Work Load

#	Title	Requirement
B1.	Workload Planning	The Solution must have the functionality for the Users to define their workload plan by creating activities and defining the activity scope and future start date.
B2.	Default Workload Overview	The Solution must have the functionality to provide up to date Workload Overview (dashboard) for the following Users: a. For Supervisor: Activities (and core information including assigned User) grouped by a region or sub-region within a chosen period b. For Subordinate: Activities the User has, or has had, control of within a chosen period c. For Dual Role (Supervisor and Subordinate): i. Activities (and core information including assigned User) grouped by a region or sub-region within a chosen period ii. Activities the User has, or has had, control of within a chosen period For example: a. Supervisor – see own work and that of their subordinates b. Subordinate – see own work only
B3.	Default Workload Overview Display	The Solution must have the functionality to provide the default Workload Overview (dashboard) that is applicable to the User type (for example, Supervisor, Subordinate), grouped by ***Activity Status***, ***Activity Type*** values in the following separate Workload Overview field sets and displayed in the following order: a. My Workload – activities, complaints, and requests for information the User currently has control of, including newly assigned and created activities. b. Activity Sent for Review - activities, complaints, and requests for information sent to another User for action and that are not closed. c. Activities No Longer Assigned to me – activities, complaints, and requests for information in which the User has interacted with, but no longer has control of. d. My Region – activities, complaints, and requests for information modified or created within the User's region. e. Anticipated Workload – (specific to ***Designated User***) submission schedule of anticipated industry reports.
B4.	Anticipated Workload Display	The Solution must have the functionality to display, in the ***Designated User***'s Anticipated Workload field set of the Workload Overview (dashboard), a schedule of industry reports for the ***Designated User*** based on the submission frequency for a specified period by specified manufacturer(s) in various User-selected display formats, for example, calendar, list, etc.
B5.	Establishment Profile Information	The Solution must have the functionality to provide a direct link via the Establishment Name value to the establishment information of each activity listed in the User's Workload Overview (dashboard). The following rules apply: a. For Establishments in the User's region/sub-region, the update interface for the Establishment information related to an activity is accessible from the following Workload Overview field sets: i. My Workload ii. Activities Sent for Review iii. Activities No Longer Assigned to me b. For Establishments outside the User's region/sub-region, the read-only view of the Establishment information related to an activity is accessible from the following Workload Overview field sets: i. Activities of Sent for Review ii. Activities No Longer Assigned to me

#	Title	Requirement
B6.	Workload Overview - Assigned Activities	The Solution must have the functionality to provide the following: a. Up to date Workload Overview (dashboard) field sets displaying all activities assigned to the User including newly assigned activities. b. For the User to select and open an activity from My Workload field set to view and edit activity details.
B7.	Workload Overview Display Functionality	The Solution must have the functionality for the User to configure the Workload Overview (dashboard) Display to: a. Define and save their own custom Workload Overviews (dashboards), for example, define the columns and sort order in a multi-column list view format (table/data grid) for all open inspections assigned to the User. b. Select their default custom Workload Overview(s) (dashboard) to display their workload c. Filter activities on attributes d. Sort activities
B8.	Workload Overview Add New Activity	The Solution must have the functionality to update the My Workload field set in the Workload Overview (dashboard) with new activities when the User creates and saves an activity.

C. User Interface and Usability

#	Title	Requirement
C1.	Consistent Graphical User Interface (GUI)	The Solution must have the functionality to provide a Graphical User Interface (GUI) with consistent look and feel to ensure high usability, which includes: a. colors, shapes, layout, and typefaces b. consistent behaviour of dynamic elements such as buttons, boxes, and menus c. consistent labelling and field placement d. data entry format display, that is, indicates the required format in the label or placeholder text of the field that require specially formatted input (for example, for dates, times, postal codes). e. keyboard-friendly input, for example, the User should be able to easily tab through the fields and make necessary edits, all without lifting their fingers off the keyboard f. workflow sequences g. field focus h. messages i. consistent navigation and orientation
C2.	Responsive Design Principles	The Solution must have the functionality to maximise the screen space and layout based on screen sizes, for example, desktop screens, tablets.
C3.	Organization of Data Entry Fields	The Solution must have the functionality to provide the User with a logical organization of fields that share the same space. For example: a. grouping related fields into field sets b. grouping related field sets into components c. grouping related components into a tabbed pane
C4.	Show and Hide Relevant Fields, Field Sets, and Components	The Solution must have the functionality to show and hide fields, field sets, and components in the GUI based on: a. The relevance of that field, field set, and component.

#	Title	Requirement
		b. The context of data previously entered. For example, display fields for input of additional information where the value in another field is "Yes".
C5.	Input control	The Solution must have the functionality to use input controls to ensure valid data is entered. For example: a. pick lists b. multi-select pick lists c. check boxes d. radio buttons e. dropdown lists f. list boxes g. toggles h. date picker i. form data validation
C6.	Context Relevant Data Options	The Solution must have the functionality to display, for selection purposes, only the list of input options that apply based on the context of the data previously entered. For example: a. A city list would be restricted to the values associated with the previously selected province/territory value. b. A brand list would be restricted to the values associated with the previously selected establishment value.
C7.	Data Entry Format Display	The Solution must have the functionality to indicate in the GUI the required data entry format in the label and placeholder text for the field that requires specially formatted input. For example: a. dates b. times c. postal codes
C8.	Mandatory Data Fields: Indication, Validation, Notification	The Solution must have the functionality to control mandatory fields in the following way: a. Visually indicate to the User mandatory fields in a consistent manner on all data input screens. b. Visually indicate to the User invalid data upon entry, for example, non-numeric characters in a numeric field. c. Alert the User of any of the following when the User attempts to confirm completion of a data entry step (for example, submitting an industry report via the guided form-based submission process): i. any field value requiring validation that has not passed data validation. ii. any mandatory field missing a value. d. Navigate the User directly to the first instance of any of the following: i. invalid data in a field. ii. missing mandatory data. e. Permit the User to complete or correct the input for all fields. f. Permit the User to repeat the confirmation of completing the data entry. g. Set validated and confirmed fields to read-only.

#	Title	Requirement
C9.	Conditionally Mandatory Fields	The Solution must have the functionality to configure conditionally mandatory fields.
C10.	Undefined and Unselected Field Values	The Solution must have the functionality to indicate when a field has not been populated with a value by the User and has not been populated with a value by the Solution. For example: a. Default value for a pick list is "Select". b. Default value for a check box is not selected.
C11.	Clear Values	The Solution must have the functionality for the User to clear an existing value from a User editable field where the User cannot delete the value. For example: a. Click an eraser icon to clear: i. a date field ii. a radio button set b. Click an "x" to clear a filter or search term.
C12.	Reset Data Entry Forms	The Solution must have the functionality for the User to clear all User entered values from a form and reset any defaults values.
C13.	Read-only Fields	The Solution must have the functionality to visually indicate read-only fields. For example: a. Grey out. b. Prevent data input.
C14.	Null Field Values	The Solution must have the functionality to visually indicate an empty or null field value and set the field to read-only. Example of a visual indicator: a. "n/a"' b. "-"
C15.	Data Validation	The Solution must have the functionality to enforce data validation rules.
C16.	Real-Time Updates	The Solution must have the functionality to refresh the value of a field displayed in the GUI as soon as that value is updated.
C17.	Calculated and Derived Data Values	The Solution must have the functionality to calculate, derive, and display values based on user-entered and Solution-stored information. Upon entry of the field values, the Solution must generate calculated and derived values and update the GUI with the values in real-time. For example: a. The User enters data into numeric fields A and B. The Solution displays the sum in a third calculated numeric field C. b. The User enters data into four numeric fields. The Solution displays the standard deviation in a fifth, calculated numeric field. c. The User sets two ***Legislation Section Compliance Outcome*** values as "No Evidence of Non-Compliance", and one ***Legislation Section Compliance Outcome*** value as "Non-Compliance". The Solution uses logic on the text values to derive and display the ***Activity Compliance Outcome*** text value as "Non-Compliance".
C18.	Time Format	The Solution must have the functionality to store all times in Coordinated Universal Time (UTC) format with offset for the time zone.
C19.	User-Entered Time Zone	The Solution must have the functionality for the User to select the time zone for any time entered.

#	Title	Requirement
C20.	Default Offset Time Zone	The Solution must have the functionality to set the default-offset time zone to that of the User's time zone.
C21.	User-Entered Time Display	The Solution must have the functionality to display all user-entered times in the time zone of the User who entered the time.
C22.	System-Generated Time Display	The Solution must have the functionality to display all system-generated times in the User's time zone.
C23.	Large Data Values	The Solution must have the functionality for the User to view the entire value of a field when the length of the value is larger than the display width of the field (for example, in a multi-column list view (table/data grid), or dropdown lists), for example, mouse-over display or in a manner that does not disrupt the layout.
C24.	Bilingual Interface (English and French)	The Solution must have the functionality to provide the GUI in each of Canada's official languages (French and English).
C25.	Language Preference	The Solution must have the functionality to use the ***Language Preference*** value in the User profile settings when the User logs on as the default language display value for: a. The Solution GUI. b. Selection values. c. Alerts and notifications. d. Context specific help.
C26.	Language – Free Text	The Solution must have the functionality to display free-text field values in the language in which the text is entered.
C27.	Diacritic and Special Characters	The Solution must have the functionality to display diacritic and special characters correctly.
C28.	Display of Context Specific Help	The Solution must have the functionality to display the context specific Help information in such that it will minimally affect the current work of the User. For example, in a: a. new window b. pop up c. tooltip
C29.	User On-line help Documentation	The Solution must have the functionality for the User to access an on-line help manual that must be available at any time.
C30.	Default Sort Order	The Solution must have the functionality to default all sorts using standard sort parameters unless explicitly identified. For example, alphabetical (a to z), numerical (0 to 9), and reverse chronological dates.
C31.	Legislative Display Order	The Solution must have the functionality to display contextually relevant Legislative Section/Subsection values sorted by Parts, Sections (within parts), and Regulations (within Sections) in ascending order, that is, using natural sort order where multi-digit numbers are treated atomically. For example: a. Part I – Tobacco Products i. 5 – Product Standards ii. 5.1 Prohibition – Manufacture iii. 5.2 Prohibition – Sale iv. 6(1) – Information required v. 6(2) – Supplementary Information vi. 6.1 – Disclosure b. Part II Access

#	Title	Requirement
		i. 8(1) – Furnishing to Youth ii. 9(1) – Sending and Delivering iii. 9.1(1) – Interprovincial Sending and Delivering iv. 9.1(2) – Advertising
C32.	Default Case Insensitive Sort	The Solution must have the functionality to default all sorts to be case insensitive. For example, variations of the spelling of "Montreal" would appear in the sorted list together, regardless of the case contained in the spelling when case insensitive is selected: a. montreal b. Montreal c. MONTREAL
C33.	"Case" Sort	The Solution must have the functionality for the User to select the option to change the sort from sensitive to insensitive to case.
C34.	"Diacritic" Sort	The Solution must have the functionality for the User to select the option to change the sort from sensitive to insensitive to diacritic/accents, for example, à, é, ç. For example, variations of the spelling of "Montreal" would appear in the sorted list together, regardless of the accented characters contained in the spelling: a. Montreal b. Montréal
C35.	Multi-Column List View (table/data grid) Sort	The Solution must have the functionality for all multi-column list views (table/ data grid) to be sortable by any column using standard sort parameters, for example, lowest to highest, highest to lowest, a-z, z-a.
C36.	Updating and Viewing a Record in a Multi-Column List View (table/data grid)	The Solution must have the functionality for the User to select a record in any multi-column list view (table/data grid) to access it directly for updating or viewing, and return to the multi-column list view after the action on the record is completed. For example: a. The User can select an activity from the Workload multi-column list view to update compliance assessment information for a selected ***Legislative Section/Subsection*** value. Once updating is complete, the User is returned to the Workload multi-column list view. b. The User can select an establishment profile from the Establishment Profile Search results multi-column list view. Once viewing is complete, the User is returned to the Establishment Profile Search results multi-column list view.
C37.	Filtering in a Multi-Column List View (table/data grid)	The Solution must have the functionality for the User to filter any multi-column list view (table/data grid) by any criteria or combination of criteria. For example: a. filter by ***Activity Type*** b. filter by ***Priority*** c. filter by ***Proposed Start Date*** (including activities with future start dates) d. filter by specific ***Province/Territory*** and ***Establishment Type*** within the specified ***Province(s)/Territory(s)*** e. filter by ***Report Section***

#	Title	Requirement
C38.	Close Modal windows	The Solution must have the functionality for the User to close and cancel any modal windows at any time. For example, windows used to display information or help.
C39.	Move Modal windows	The Solution must have the functionality for the User to move any modal windows so as not to obscure the data displayed in the parent window. For example, windows used to display information or help.
C40.	Data Viewing Without An External Tool	The Solution must have the functionality for the User to access and view data related to activities and establishments wherever identified within the Solution without having to access an external tool. For example, all related activity data is viewable from within the establishment. The User is not required to view related activity data in a separate tool.
C41.	Industry Report Submission via Portal and API	The Solution must have the functionality for the External User to electronically submit structured data (for example, industry reports, laboratory analyses results reports) via the following interfaces: a. A secure Portal User Interface. b. A secure REST API.
C42.	Portal User Interface	The Solution must have the functionality for the User who is required to submit industry reports to perform the following via the Portal User Interface: a. Industry Report Submission Interface b. Submit Laboratory Analysis Results Reports c. Submit a Complaint d. Submit an Enquiry e. Request an Industry Report Submission account f. Request a Laboratory Submission Account
C43.	Solution version	The Solution must have the functionality for the User to identify the current version of the Solution, for example, by version number.
C44.	Support Request, Complaint, and Enquiry "Tabbed Pane-like" Format and Components	The Solution must have the functionality to provide a format for the collection of all information relating to processing a Support Request, Complaint, or Enquiry such that the information is arranged logically in sections where the User can intuitively move from one section to another. For example, for data input and viewing purposes, the format can be composed of the following sections for each Support Request, Complaint, or Enquiry: a. Support Request, Complaint, or Enquiry information b. Links c. Sent To
C45.	Submit Support Request	The Solution must have the functionality to provide the following field sets and related fields in the Support Request, for data input and viewing purposes: a. Submitter Details, for example i. Name ii. Email iii. Phone Number b. Support Request Issue Category (a selected value) c. Support Request Details (description of the request submitted) d. Date of Request

#	Title	Requirement
C46.	Internal Facing - Processing a Support Request-Fields	The Solution must have the functionality to provide the following additional fields in the Support Request component for the processing of the Support Request, for data input and viewing purposes: a. Actions Taken (description of the actions taken) b. Date of Action c. Support Request Status (a selected value)
C47.	Industry Report Submission Interface -Components	The Solution must have the functionality to provide the following components in a tabbed pane-like format in the Industry Report Submission Interface for data input and viewing purposes: a. Home (Dashboard) b. Contact (Contact Management) c. Reports (Submit and View) d. Settings (User Profile and Preferences) e. Support Request
C48.	Industry Report Submission Interface - Home Component Field Sets	The Solution must have the functionality to provide the following field sets and related fields in the Home component of the Industry Report Submission Interface, for data input and viewing purposes: a. Submission Status, (for the last 2 quarters), of reports due, overdue, submitted late or submitted on prior to or on the submission date; b. Report Filter.
C49.	Industry Report Submission Interface - Contact Component Field Sets	The Solution must have the functionality to provide the following field sets in the Contact component of the Industry Report Submission Interface for data input and viewing purposes. a. Establishment Profile Management b. Contact Management
C50.	Industry Report Submission Interface - Reports Component Field Sets	The Solution must have the functionality to provide the following field sets and related fields in the Reports component of the Industry Report Submission Interface for data input and viewing purposes: a. Saved Reports in Progress b. Overdue Reports View c. Industry reporting History View d. Submit a New Industry Report (field)
C51.	Industry Report Submission Interface - Settings Component Field Sets	The Solution must have the functionality to provide User Profile and Preferences field sets in the Settings component of the Industry Report Submission Interface for data input and viewing purposes. a. User Profile b. Preferences
C52.	Industry Report Submission Interface - User Profile Fields	The Solution must provide the following fields in the User Profile field set in the Settings component of the Industry Report Submission Interface for data input and viewing purposes: a. ***Profile Id*** (read-only) b. ***Full Name*** c. ***User Name*** (read-only) d. ***Profile Province/Territory*** e. ***Profile City*** f. ***Profile Street*** g. ***Profile Area*** h. ***Profile Time Zone*** i. ***Account Type*** j. ***Password*** k. ***Phone Number*** l. ***Email address***

#	Title	Requirement
		m. ***Language Preference***
C53.	Establishment "Tabbed Pane-like" Format and Components	The Solution must have the functionality to provide a tabbed pane-like format, for data input and viewing of all information relating to an establishment. The Establishment "tabbed pane" must be composed of the following components: a. Establishment Information b. Concerns and Issues c. Contacts (includes contact details) d. Associated Activities (includes compliance and enforcement history) e. Comments f. Products and Brands (only displayed when the ***Establishment Type*** value is "Manufacturer"; includes counts) g. Industry Reports (only displayed when the ***Establishment Type*** value is "Manufacturer") h. Promotional Events (only displayed when the ***Establishment Type*** value is "Other" and the ***Establishment Subtype*** value is "Promotor")
C54.	Establishment "Establishment Information" Component	The Solution must have the functionality to provide the following field sets and related fields in the Establishment Information component of the Establishment "tabbed pane", for data input and viewing purposes: a. Establishment (***Establishment Id, Establishment Name, Address, etc.***) b. Mailing Address c. Email d. Phone e. Ownership f. Status g. ***Establishment Assigned To*** h. Establishment Type displayed in a multi-column list view format i. Online Presence (for example: web site, social media) displayed in a multi-column list view format j. Associated Establishments displayed in a multi-column list view format k. Promotional Events displayed in a multi-column list view format (only when the ***Establishment Type*** value is "Other" and ***Establishment Subtype*** value is "Promotor")
C55.	Establishment "Concerns and Issues" Component	The Solution must have the functionality to provide the following field sets and related fields displayed in a multi-column list view format in the Concerns and Issues component of the Establishment "tabbed pane", for data input and viewing purposes: a. Concerns i. Concern Id ii. Date iii. User Name iv. Concern b. Issues i. Issue Id ii. Date iii. User Name iv. Issue
C56.	Establishment "Contacts" Component	The Solution must have the functionality to provide the following field set and related fields displayed in a multi-column list view format in the Contacts component of the Establishment "tabbed pane", for data input and viewing purposes: a. Contacts i. ***Contact Id***

#	Title	Requirement
		ii. Full Name ***iii. Title*** ***iv. Phone Descriptor*** v. ***Phone Number*** vi. ***Email Descriptor*** vii. ***Email Address*** viii. ***Language***
C57.	Establishment "Associated Activities" Component	The Solution must have the functionality to provide Activities associated with the establishment displayed in a multi-column list view format in the Activities component of the Establishment "tabbed pane", for data input and viewing purposes.
C58.	Establishment "Comments" Component	The Solution must have the functionality to provide the Comment History field set and related fields in the Comments component of the Establishment "tabbed pane", for data input and viewing purposes.
C59.	Establishment "Products and Brands" Component	The Solution must have the functionality to provide the following field sets and related fields displayed in a multi-column list view format in the Products and Brands component of the Establishment "tabbed pane", for data input and viewing purposes: a. Product b. Brands
C60.	Establishment "Industry Reporting History" Component	The Solution must have the functionality to provide the following field sets and related fields displayed in a multi-column list view format in the Industry Reporting History component of the Establishment "tabbed pane", for data input and viewing purposes: • Overall Industry Report History • Industry Reports With No Associated Activity
C61.	Activity "Tabbed Pane-like" Format and Components	The Solution must have the functionality to provide a "tabbed pane" like format for data input and viewing of all information relating to an activity. The Activity "tabbed pane" must be composed of the following components and in the specified order: a. General Information b. Scope Plan c. Compliance Assessment d. Enforcement Actions e. Link/Close f. Sent To
C62.	Activity "General Information" Component Format	The Solution must have the functionality to provide the following field sets and related fields in the General Information component of the Activity "tabbed pane", for data input and viewing purposes: a. Establishment related information field sets: i. Establishment (Establishment Id, Establishment Name, Establishment Status, Establishment Type, location information, and Concerns and Issues, and Age Restricted Icons) ii. Establishment Contacts displayed in a multi-column list view format iii. Associated Establishments displayed in a multi-column list view format iv. Other Activities for this Establishment displayed in a multi-column list view format b. Specific activity related information field sets: i. Core Information ii. Activity Timeline

#	Title	Requirement
		iii. Sent To History displayed in a multi-column list view format iv. Warrants (if applicable) displayed in a multi-column list view format v. Online Presence (for example: web site, social media) displayed in a multi-column list view format vi. Links (to files) displayed in a multi-column list view format vii. Comment History c. ***Confirm When Complete*** (field)
C63.	Activity "Scope Plan" Component Format	The Solution must the functionality to provide the following field sets and related fields in the Scope Plan component of the Activity "tabbed pane", for data input and viewing purposes: e. ***Activity Scope Plan Type*** (field) f. Activity Scope Details g. ***Confirm When Complete*** (field) h. ***Audit Plan*** (field) (if applicable)
C64.	Activity "Compliance Assessment" Component Format	The Solution must provide the following field sets and related fields in the Compliance Assessment component of the Activity "tabbed pane", for data input and viewing purposes: a. Establishment Location Verification b. Person Spoken To displayed in a multi-column list view format c. Add Scope d. Compliance Results displayed in a multi-column list view format e. Artifacts Summary displayed in a multi-column list view format f. Responsible Party displayed in a multi-column list view format g. ***Confirm When Complete***
C65.	Activity "Compliance Assessment" Component - Establishment Location Verification Format	The Solution must have the functionality to provide the following fields in the Establishment Location Verification field set in the Compliance Assessment component of the Activity "tabbed pane", for data input and viewing purposes: a. ***Activity Establishment Verification Code*** b. ***Actual Start Date*** c. ***Actual Start Time*** d. ***Warrant Executed*** e. ***Confirm When Complete***
C66.	Activity "Compliance Assessment" Component - Person Spoken To Format	The Solution must have the functionality to provide the following fields in the Person Spoken To field set in the Compliance Assessment component of the Activity "tabbed pane", for data entry and viewing purposes: a. ***Name of Person Spoken To*** b. ***Title*** c. ***Phone*** d. ***Email*** e. ***Establishment Profile Verified***
C67.	Activity "Compliance Assessment" Component - Compliance Results Format	The Solution must have the functionality to provide the following fields displayed in a multi-column list view format in the Compliance Results field set in the Compliance Assessment component of the Activity "tabbed pane", for data entry and viewing purposes: a. Legislation b. Legislation Section Compliance Outcome, with the following selection values: i. "Not Inspected" ii. "Not Applicable" iii. "No Evidence of Non-Compliance" iv. "Non-Compliance"

#	Title	Requirement
		c. ***Analysis Type*** d. ***Add Artifacts*** e. ***Number of Artifacts***
C68.	Artifact "Tabbed Pane-like" - Format and Components	The Solution must have the functionality to provide an Artifact tabbed pane-like format for data input and viewing of all information relating to an artifact. The Artifact "tabbed pane" must be composed of the following components: a. Collection b. Analysis c. Links The format of the Collection and Analysis components of the Artifact "tabbed pane" will depend on the selected ***Artifact Analysis Type*** value.
C69.	Artifact: Header Information Format	The Solution must have the functionality to provide a header field set in the Artifact "tabbed pane" for the display of artifact information that remains the same across all components of the Artifact "tabbed pane". For viewing purposes, the header section must be composed of the following fields: a. ***Establishment Name*** b. ***Artifact Id*** (Solution generated value) c. ***Legislative Section/Subsection*** d. ***Artifact Analysis Type*** The ***Artifact Analysis Type*** values are as follows: a. "Industry Report Analysis" b. "TPLR Analysis" c. "TPIR Analysis" d. "Weight Analysis" e. "Promotion of PA Analysis" f. "Prohibited Additives Analysis" g. "Cigarette Ignition Propensity Analysis" h. "TPR(PSP) Analysis" i. "Nicotine Quantification Analysis" j. "Health Benefits Analysis" k. "Observation Analysis" l. "Pre-Benchmark Analysis" m. "Benchmark Analysis" n. "VPLPR Analysis"
C70.	Artifact: "Collection" Component Format	The Solution must have the functionality to provide the applicable artifact collection fields in the Collection component of the Artifact "tabbed pane", for data input and viewing purposes, according to the following values: a. the selected ***Artifact Analysis Type*** value; b. the selected ***Legislative Section/Subsection*** value.
C71.	Artifact: "Analysis" Component Format	The Solution must have the functionality to provide the applicable artifact analysis fields, within the Analysis component of the Artifact "tabbed pane", for data input and viewing purposes, according to the following values: a. the selected ***Artifact Analysis Type*** value; b. the selected ***Legislative Section/Subsection*** value.
C72.	Artifact: "Shipping" Component	The Solution must have the functionality to provide the applicable fields and field sets for data input and viewing purposes, according to the ***Artifact Analysis Type*** value, for the Shipping component of the Artifact "tabbed pane".

#	Title	Requirement
C73.	Artifact: "Analysis" Component: Industry Reports	The Solution must have the functionality to provide the following field sets and related data in the Artifact pane for viewing purposes, for an activity whose ***Artifact Analysis Type*** value is "Industry Report Analysis": a. ***Artifact Id*** (Solution generated by concatenating Solution generated number + Legislation number + number of artifact for this ***Legislative Section/Subsection*** value, starting at the number 1) b. ***Establishment Name*** (for the activity) c. ***Legislation number and description*** (for which the artifact is being assessed) d. ***Artifact Information*** (Industry report data submitted (also includes files attached in the industry report submission))
C74.	Artifact: "Links" Component Format	The Solution must have the functionality to provide the following fields in a multi-column list view format within the Links component of the Artifact "tabbed pane", for data input and viewing purposes: a. ***Link Id Number*** b. ***File name*** (of document being linked) c. ***Description*** (of the linked document) d. ***Linked By*** (User name) e. ***Linke***d ***Date***
C75.	Activity "Compliance Assessment" Component - Artifact Summary	The Solution must have the functionality to provide the following fields displayed in a multi-column list view format in the Artifacts Summary field set in the Compliance Assessment component of the Activity "tabbed pane", for update and viewing purposes: a. ***Artifact Id*** b. ***Legislation*** c. ***Compliance Result*** d. ***Description***
C76.	Activity "Compliance Assessment" Component - Responsible Party	The Solution must have the functionality to provide the following fields displayed in a multi-column list view format in the Responsible Party field set in the Compliance Assessment component of the Activity "tabbed pane", for update and viewing purposes: a. ***Name*** b. ***Non-Compliance Legislation*** c. ***Title*** d. ***Language*** e. ***Phone*** f. ***Email***
C77.	Activity "Enforcement Actions" Component	The Solution must have the functionality to provide the following field sets in the Enforcement Actions component of the Activity "tabbed pane", for data input and viewing purposes: a. Recommended Enforcement Action b. A field set for each selected enforcement action c. A field set for the links for each selected enforcement action d. ***Confirm When Complete*** (field)
C78.	Activity "Link/Close" Component Format	The Solution must have the functionality to provide the following field sets and related fields in the Link/Close component (See Requirement C61) of the Activity "tabbed pane", for data input and viewing purposes: a. Recommended Next Steps b. Justification c. ***Confirm When Complete*** (field)
C79.	Industry Reports Compliance Assessment Component –	The Solution must have the functionality to provide the following fields displayed in the Compliance Results field set in the Compliance

#	Title	Requirement
	Compliance Results Format Legislative Section/Subsection	Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. in a multi-column list view format: i. Legislative Section/Subsection ii. Legislation Section Compliance Outcome 1. Not Applicable 2. No Evidence of Non-Compliance 3. Non-Compliance 4. Compliance Outcome Level iii. No. of Errors iv. Non-Compliance History b. ***Total No. of Errors*** ***c. View all Non-Compliance History***
C80.	Industry Reports Compliance Assessment Component – Compliance Summary Format	The Solution must have the functionality to provide the following fields displayed in a multi-column list view format in the Compliance Summary field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. Activity Compliance Outcome (Displayed as State of Compliance) i. Not Applicable ii. No Evidence of Non-Compliance iii. Non-Compliance b. Compliance Outcome Level (Displayed as Level of Compliance) i. Minor ii. Major c. Display the following in a summary multi-column list view format: i. Type by Non-Compliance Level ii. Number of Non-compliances iii. Number of errors iv. The sum total of non-compliances v. The sum total of errors
C81.	Industry Reports Compliance Assessment Component – Sections Overridden Format	The Solution must have the functionality to provide the following fields displayed in a multi-column list view format in the Sections Overridden field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. ***Legislative Section/Subsection*** b. ***Reason***
C82.	Industry Reports Compliance Assessment Component – Artifacts Summary Format	The Solution must have the functionality to provide the following fields displayed in a multi-column list view format in the Artifacts field set in the Compliance Assessment component of the Activity "tabbed pane" for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. ***Artifact Id*** b. ***Legislation*** (Displayed as ***Applicable Legislation)***
C83.	Industry Reports Compliance Assessment Component – Compliance Results Format Errors Grouped by Legislative Section/Subsection View	The Solution must have the functionality to provide the following field sets and related fields in the "Errors Grouped by Legislative Section/Subsection" view for any Activity where an industry report has been submitted, for data entry and viewing purposes: a. Errors for: [***Legislative Section/Subsection*** value and related text under with the error was identified] b. Errors in Report (field set)

#	Title	Requirement
		i. System Identified Errors: [Total number of errors] with the following fields displayed in a multi-column list view: 1. Brand Name (if applicable) 2. Dimension Field(s) 3. Measure Fields(s) 4. Error Name ii. User Identified Errors: [Total number of errors] with the following fields displayed in a multi-column list view: 1. Brand Name (if applicable) 2. Dimension Field(s) 3. Measure Fields(s) 4. Error Name c. Outstanding Errors Not Corrected from Previous Report Versions: [Total number of errors] a. Brand Name (if applicable) b. Dimension Field(s) c. Measure Fields(s) d. Error Name e. Report Version f. Date of Report (linked to Activity)
C84.	Public Facing - Enquiry	The Solution must have the functionality to provide the following field sets and related fields in the Enquiry, for data input and viewing purposes: a. Submitter Details, for example i. Name ii. Email iii. Phone Number b. Enquiry Details (description of the Enquiry submitted) c. Date of Enquiry
C85.	Internal Facing - Processing an Enquiry - Fields	The Solution must have the functionality to provide additional fields for the processing of the Enquiry. For example: a. ***Actions Taken*** (description of the actions taken) ***b. Date of Action*** c. ***Enquiry Status*** (a selected value)
C86.	Public Facing - Complaint	The Solution must have the functionality to provide the following field sets and related fields in the Complaint, for data input and viewing purposes: a. Submitter Details, for example: i. Name ii. Email iii. Phone Number b. ***Complaint Details*** (description of the complaint submitted) ***c. Date of Complaint***
C87.	Internal Facing - Processing a Complaint-Fields	The Solution must have the functionality to provide additional fields for the processing of the Complaint. For example: a. ***Actions Taken*** (description of the actions taken) b. ***Date of Action*** c. ***Complaint Status*** (a selected value)
C88.	Landing Page	The Solution must have the functionality to provide a landing page where the User can access modules of the application via menus applicable for the type of User.

#	Title	Requirement
C89.	"Establishment Create/Update Reason" Fields	The Solution must have the functionality to provide the following fields for data input and viewing purposes, when the User saves a new establishment profile and updates an establishment profile: a. ***Reason for establishment create/update*** b. ***Background*** (description of reason for create/update)
C90.	Warrant Executed	The Solution must have the functionality to provide the following fields for data input and viewing purposes, when a warrant is indicated as executed: a. ***Served to*** b. ***Served by*** c. ***Executed date*** d. ***Executed time***
C91.	Activity "Sent To" Component Format	The Solution must have the functionality to provide the following field set and related fields in the Sent To component of the Activity "tabbed pane", for data input and viewing purposes: a. Send Activity For Action b. Approval Required c. Sent To History (displayed in a multi-column list view format) i. Sent By ii. Sent To iii. Sent Date as the activity Date Created and time for initial entry, and Sent Date and time for subsequent entries iv. Activity Send To Action v. ***Activity Send To Reason*** d. Sent To Comments History
C92.	Industry Reports Compliance Assessment Component – Compliance Results Format Non-Compliance History View	The Solution must have the functionality to provide the following fields in the "Non-Compliance History" view for any Activity where an industry report has been submitted, for viewing purposes for the last three ***Report Period*** values: a. ***Brand Name*** (if applicable) b. Dimension Field(s) c. Measure Fields(s) d. ***Error Name*** e. ***Period Year*** of the report f. ***Report Period*** g. ***Report Version*** h. ***Date of Report*** (linked to Activity) i. ***Corrected*** (values "Yes" and "No") j. ***Date of Report Corrected*** (linked to activity)
C93.	Industry Report Pre-Benchmark -Assessment of Compliance	The Solution must have the functionality to provide the following field sets and related fields in the Compliance Assessment view for ***Report Section*** values of "14(13)" for updating and viewing purposes when the ***Activity Reason Type*** value is any of "Industry Reports" values: a. Assessment of Exemption b. Reason c. ***Compliance Status***
C94.	Industry Report Benchmark - Assessment of Compliance	The Solution must have the functionality to provide the following field sets and related fields in the Compliance Assessment view for ***Report Section*** values of "14(11)" for updating and viewing purposes when the ***Activity Reason Type*** value is any of "Industry Reports" values: a. Assessment of Exemption b. Reason ***c. Compliance Status***

D. Search

#	Title	Requirement
D1.	Search	The Solution must have the functionality for the User to search on specific record types and combinations of record types stored in the Solution. For example: a. Establishment Profiles b. Activities c. Complaints d. Enquiry e. Support Request f. Industry Reports g. Industry Report Audit h. Brands i. Product types j. Linked files (that is, linked file meta data) k. Attached Files l. User Profiles
D2.	Establishment Profile Search	The Solution must have the functionality to provide a pre-defined Establishment Profile Search, with the following default values populated, for the User to search for an establishment: a. ***Establishment Status*** value is "Active" b. ***Establishment Province*** value is the User profile province value c. ***Establishment Region*** value is the User profile region value d. ***Establishment Sub-Region*** value is the User profile sub-region value Pre-defined Establishment Profile Search must consist of the following fields: a. ***Establishment Id*** b. ***Establishment Name*** c. ***Establishment Street*** d. ***Establishment City*** e. ***Establishment Province*** f. ***Establishment Postal Code*** g. ***Establishment Region*** h. ***Establishment Sub-Region*** i. ***Establishment Type*** j. ***Establishment Sub-type*** k. ***Establishment Status***
D3.	Activity Search	The Solution must have the functionality to provide a pre-defined Activity Search, with the following default values populated, for the User to search for an activity: a. ***Establishment Province*** value is the User profile province value b. ***Establishment Region*** value is the User profile region value c. ***Establishment Sub-Region*** value is the User profile sub-region value The Activity Search criteria must also provide the same establishment fields as provided in the pre-defined Establishment Profile Search Criteria. Pre-defined Activity Search must consist of the following fields: a. ***Activity Id*** b. ***Activity Type*** c. ***Activity Status*** d. ***Compliance Status*** e. ***Establishment Name*** f. ***Establishment Street*** g. ***Establishment City***

#	Title	Requirement
		h. ***Establishment Province*** i. ***Establishment Postal Code*** j. ***Establishment Region*** k. ***Establishment Sub-Region*** l. ***Establishment Type*** m. ***Establishment Sub-type***
D4.	Complaint Search	The Solution must have the functionality to provide a pre-defined Complaint Search, with the following default values populated, for the User to search for a complaint: a. ***Complaint Status*** value is "Open" b. ***Province*** value is [User profile's ***Province*** value] c. ***Region*** value is [User profile's ***Region*** value] d. ***Sub-Region*** value is [User profile's ***Sub-Region*** value] Pre-defined Complaint Search must consist of the following fields: a. ***Compliant Id*** b. ***Complaint Status*** c. ***Province*** d. ***Region*** e. ***Sub-Region***
D5.	Enquiry Search	The Solution must have the functionality to provide a pre-defined Enquiry Search, with the following default values populated, for the User to search for an enquiry: a. ***Enquiry Status*** value is "Open" b. ***Province*** value is [User profile's ***Province*** value] c. ***Region*** value is [User profile's ***Region*** value] d. ***Sub-Region*** value is [User profile's ***Sub-Region*** value] Pre-defined Enquiry Search must consist of the following fields: a. ***Enquiry Id*** b. ***Enquiry Status*** c. ***Province*** d. ***Region*** e. ***Sub-Region***
D6.	Support Request Search	The Solution must have the functionality to provide a pre-defined Support Request Search, with the following default values populated, for the User to search for a support request: The default populated values must be: a. ***Support Request Status*** value is "Open***"*** b. ***Province*** value is [User profile's ***Province*** value] c. ***Region*** value is [User profile's ***Region*** value] d. ***Sub-Region*** value is [User profile ***Sub-Region*** value] Pre-defined Support Request Search must consist of the following fields: a. ***Support Request Id*** b. ***Support Request Status*** c. ***Province*** d. ***Region*** e. ***Sub-Region***
D7.	Industry Report Search	The Solution must have the functionality to provide a pre-defined Industry Report Search, with the following default values populated, for the User to search for an industry report: c. ***Report Status*** value is "Registered" d. ***Submission Date*** value is [Last 12 Months] Pre-defined Industry Report Search must consist of the following fields: a. ***Report Id***

#	Title	Requirement
		b. ***Report Section*** c. ***Report name*** d. ***Report Period*** e. ***Report Status*** f. ***Submission Date*** g. ***Manufacturer Id*** h. ***Manufacturer Name*** i. ***Submitter Name*** j. ***Activity Number(s)***
D8.	Brand Search	The Solution must have the functionality to provide a pre-defined Brand Search, with the following default values populated, for the User to search for the brand: b. ***Brand Status*** value is ***"Active"*** Pre-defined Brand Search must consist of the following fields: a. ***Brand Id*** b. ***Brand Name*** c. ***Brand Descriptor*** d. ***Brand Status*** e. ***Product Type*** f. ***Product Size*** g. ***Manufacturer Id*** h. ***Manufacturer Name***
D9.	Linked File Search	The Solution must have the functionality to provide a Linked Files Search.
D10.	User Profile Search	The Solution must have the functionality to provide a pre-defined User Profile Search, with the following default values populated, for the User to search for the profile: a. ***User Status*** value is "Active" Pre-defined User Profile Search must consist of the following fields: a. ***User Id*** b. ***User name*** c. ***First Name*** d. ***Last Name*** e. ***Region***
D11.	Enter Search Values	The Solution must have the functionality for the User to enter and modify search values.
D12.	"Contains" Search	The Solution must have the functionality to use "contains" match searches, by default, to find items that contain the search value. For example: Search criteria: a. ***Province/Territory*** value is "Ontario" (exact) b. ***Establishment Sub-Type*** value is "Convenience store" (exact) c. ***Establishment Name*** value contains "**Bob"** (contains) Search results would include the following, where all 3 search values were found: Province/Territory | Establishment Sub-Type | Establishment Name Ontario | Convenience store | **Bob**'s store Ontario | Convenience store | Ke**bob** Express Ontario | Convenience store | **Bob**cat Outdoor
D13.	"Exact" Search	The Solution must have the functionality to provide the User with the option to perform an exact search based on the search values entered.

#	Title	Requirement
		Search criteria example: c. ***Province/Territory*** value is "Ontario" (exact) d. ***Establishment Sub-Type*** value is "Convenience store" (exact)
D14.	"Case" Search	The Solution must have the functionality to provide the User with an option to change the search from case sensitive to case insensitive. For example, variations of the spelling of "Montreal" must appear in the search result list together, regardless of the case contained in the spelling when case insensitive is selected: a. montreal b. Montreal c. MONTREAL
D15.	"Diacritic" Search	The Solution must have the functionality to provide the User with an option to change the search from sensitive diacritic/accents to insensitive diacritic/accents, for example, à, é, ç. For example, variations of the spelling of "Montreal" must appear in the search result list together, regardless of the accented characters contained in the spelling: a. Montreal b. Montréal
D16.	Search Results Display	The Solution must have the functionality to display search results in a multi-column list view format (table/data grid) when a search is performed.
D17.	Search Result Page Navigation	The Solution must have the functionality to navigate the search result pages.
D18.	Result Set Position and Size	The Solution must have the functionality to display, in the search results, the following information: e. Total number of search results f. Current search results range being displayed g. Current Page h. Total number of pages For example, 1 to 20 of 500 results
D19.	Preview	The Solution must have the functionality for the User to preview tombstone data for each search result without having to click through (open) the search result record for viewing and updating. For example, mouse over-like preview.
D20.	Existing Establishment Verification Search	The Solution must have the functionality to perform an Existing Establishment Verification Search of existing establishment profiles using the new establishment profile information as the search values, to determine if the new establishment profile is either of the following, when the User selects to verify the establishment information: a. matches b. is similar to an existing establishment profile
D21.	Bulk Create Activities Search	The Solution must have the functionality to provide a pre-defined Bulk Create Activities Search, with the following default values populated, for the User to search for establishments: a. ***Establishment Status*** value is "Active" b. ***Establishment Province*** value is [the User profile province value] c. ***Establishment Region*** value is [the User profile region value] d. ***Establishment Sub-Region*** value is [the User profile sub-region value] e. ***Establishment Type*** value is "Retailer" Pre-defined Establishment Profile Search must consist of the following fields:

#	Title	Requirement
		a. ***Establishment Id*** b. ***Establishment Name*** c. ***Establishment Street*** d. ***Establishment City*** e. ***Establishment Province*** f. ***Establishment Postal Code*** g. ***Establishment Region*** h. ***Establishment Sub-Region*** i. ***Establishment Type*** j. ***Establishment Sub-type*** k. ***Establishment Status***
D22.	Ad-hoc Search	The Solution must have the functionality for the User to perform the following: a. Select ad-hoc search parameter values. b. Create, save, share, retrieve, and delete ad-hoc search criteria. c. Cancel ad-hoc searches that are being executed. d. View the results of an ad-hoc search once the search has completed its execution.

E. Establishments

#	Title	Requirement
E1.	Create New Establishment Profile	The Solution must have the functionality for the User to: a. Create a new establishment profile record. b. Update and save an existing establishment profile record.
E2.	Establishment: Create and Update Profile – Role based	The Solution must have the functionality for the User to create and update an establishment profile based on the ***User Role*** value and ***Establishment Type*** value. For example: A User with a ***User Role*** value of "Industry Report Reviewer" is the only User that can create and update an establishment profile when the ***Establishment Type*** value is "Manufacturer".
E3.	Workflow Steps – Create a New Establishment Profile	The Solution must have the functionality to move the User through the following business process workflow steps to create a new establishment profile record: a. Enter establishment information for the fields in the Establishment field set and related fields, including all mandatory information. b. Validation of the establishment's physical address. c. Correct validated address (as required). d. Confirm validated address. e. Existing Establishment Verification. f. Continue to enter the establishment profile information.
E4.	Establishment Information Component	The Solution must have the functionality for the User to enter, update, and view all data in the Establishment Information component of the Establishment "tabbed pane".
E5.	New Establishment Information	The Solution must have the functionality to prevent the User from entering additional establishment information for a physical address until the following processes have been completed: a. Validation of the establishment's physical address. b. Existing Establishment Verification.
E6.	Validation of the Establishment's Physical Address	The Solution must have the functionality to limit the User from moving to the next workflow step until the User confirms the physical address has been validated.
E7.	Geographic Coordinates for Establishment location	The Solution must have the functionality to use an address validation service to provide global positioning coordinates for all addresses upon validation.
E8.	Address Validation – Establishment address and postal code	The Solution must have the functionality to validate an establishment's address (physical, mailing) using an updated address validation service (for example, Canada Post Address Complete service) before the establishment address can be saved to the database. Address validation service used must be kept up to date.
E9.	Address Validation – Establishment address and postal code	The Solution must have the functionality, when the address validation service determines the address is not valid, such as "postal code does not match street address/city", to: a. List the address validation results and problems with the address. b. Provide the option for the User to correct the address.
E10.	Address Validation – Establishment address and postal code	The Solution must have the functionality to display a list of alternative addresses, when the address validation service determines an address is not valid.
E11.	Address Validation – Establishment address and postal code	The Solution must have the functionality for the User to select an address from a list of alternative addresses provided by the address validation service to replace the address that is determined to be invalid (instead of manually entering the address).

#	Title	Requirement
E12.	Address Validation – Establishment address and postal code	The Solution must have the functionality for the User to use the address as entered, even if the address validation service has determined the address to be invalid.
E13.	Address Validation and Existing Establishment Verification	The Solution must have the functionality for the User to perform the following processes when the address has been updated for an existing establishment: a. Validation of the establishment's physical address b. Existing establishment verification
E14.	New Establishment - Existing Establishment Verification	The Solution must have the functionality for the User to perform the Existing Establishment Verification Search (See Requirement D20) on the existing establishment profiles to verify the uniqueness of the new establishment profile and avoid data entry of duplicate information, before the User can indicate a new establishment profile has been verified.
E15.	Existing Establishment View	The Solution must have the functionality for the User to select an existing establishment profile from the search results and view all establishment profile information, without losing the current establishment profile information.
E16.	New establishment at existing establishment address	The Solution must have the functionality, when the User enters a new establishment profile for an address currently used by an existing establishment in the Solution, to: a. alert the User that there is an existing establishment profile at the address entered b. provide the following options in the alert: i. Update the address of the existing establishment. ii. New Establishment at this address iii. New owner for the existing establishment iv. Multiple establishments at this address.
E17.	New establishment at existing establishment address - Action	The Solution must have the functionality to perform the following actions, when the User selects the option of "New Establishment at this address": a. Change the existing ***Establishment Location Verification*** value to "Establishment Relocated – Address Unknown - New Establishment at Specified Location". b. Set the existing ***Establishment Status*** value to "Inactive" as of the current date, when the existing ***Establishment Status*** value is "Active", to permit the User to continue entering the new establishment profile using the address.
E18.	New establishment at existing establishment address - Action	The Solution must have the functionality to prompt the User through the New Owner process to change the ownership for the existing establishment profile, when the User selects the option of "New owner for the existing establishment" (See Requirement E45).
E19.	Establishment – Existing: Use, Discard, or Cancel	The Solution must have the functionality to prompt the User to choose from one of the following options when an existing similar establishment profile has been identified via the Existing Establishment Verification Search: a. Discard the new establishment profile and select an identified existing similar establishment profile for updating as required. b. Cancel the establishment verification, un-confirm "verify establishment information", and use the new establishment profile as entered.
E20.	Establishment – Potential Duplicate Identified	The Solution must have the functionality for the User to change the ***Establishment Status*** values to "Inactive: Potential Duplicate", when the User identifies 2 or more establishment profiles as being identical.
E21.	Validation of the Establishment's Updated Physical Address	The Solution must have the functionality to validate the physical address before permitting the User to continue entering establishment profile information, when a User has updated the physical address.

#	Title	Requirement
E22.	Establishment Verification – Next Components	The Solution must have the functionality for the User to enter, update, and view all data in the components of the Establishment "tabbed pane", when the establishment has been verified as unique.
E23.	Associate an Establishment	The Solution must have the functionality for the User to associate (link) an existing establishment to the selected establishment.
E24.	Remove Associated Establishment	The Solution must have the functionality for the User to remove an associated (linked) establishment from the selected establishment.
E25.	Concerns and Issues Component	The Solution must have the functionality for the User to enter, update, and view all data in the Concerns and Issues component of the Establishment "tabbed pane".
E26.	Contacts Component	The Solution must have the functionality for the User to enter, update, and view all data in the Contacts component of the Establishment "tabbed pane".
E27.	Associated Activities Component	The Solution must have the functionality for the User to view all data in the Associated Activities component of the Establishment "tabbed pane".
E28.	Comments Component	The Solution must have the functionality for the User to enter, update, and view all data in the Comments component of the Establishment "tabbed pane".
E29.	Product and Brands Component	The Solution must have the functionality for the User to enter, update, and view all data in the Product and Brands component of the Establishment "tabbed pane".
E30.	Establishment – Brand information	The Solution must have the functionality to display the brand information in a list view (table/data grid) format, when the User views the brands associated with an establishment in the Product and Brands component of the Establishment "tabbed pane".
E31.	Establishment – Brand information	The Solution must display the total count of brands for the establishment, when the User views the brands associated with an establishment.
E32.	Industry Reporting History Component	The Solution must have the functionality for the User to enter, update, and view all data in the Industry Reporting History component of the Establishment "tabbed pane".
E33.	Establishment Promotional Events	The Solution must have the functionality for the User to enter, update, and view all data in the Promotional Events field set in the Establishment component, when the ***Establishment Type*** value is "Other" and ***Establishment Subtype*** value is "Promoter".
E34.	Establishment Create/Update Reason	The Solution must have the functionality for the User to perform the following actions when prompted by the Solution: a. Select the ***Reason for Establishment Create/Update*** value. b. Enter the ***Background*** value (description of reason for create/update)
E35.	Establishment: Manufacturer	The Solution must have the functionality to default the ***Establishment Status*** to "Pending Validation", when the User creates an establishment with the ***Establishment Type*** of "Manufacturer".
E36.	Establishment - Update	The Solution must have the functionality to prevent the User from changing the ***Establishment Status*** of a Manufacturer from "Pending Validation" to another value.
E37.	Confirm Establishment Profile is Complete	The Solution must have the functionality for the User to confirm an Establishment Profile as complete.
E38.	Create New Establishment Profile Record	The Solution must have the functionality to create a new Establishment Profile record when the User confirms the Establishment Profile is complete.
E39.	Create New Activity Associated with New Establishment Profile	The Solution must have the functionality to perform the following when a new Establishment Profile record is created: a. Create a new activity record. b. Associate the activity record with the new establishment profile record. c. Populate the fields in the Activity Core Information field set.

#	Title	Requirement
E40.	Create New Activity Associated with Updated Establishment Profile	The Solution must have the functionality to perform the following actions when an existing establishment profile is updated: a. Create a new activity, b. Associate the new activity record with the existing establishment profile record, c. Populate the fields in the Activity Core Information field set.
E41.	New Establishment Comments Copy to Activity	The Solution must have the functionality to copy values entered into the ***Establishment Comments*** field during the creation of a new establishment profile record into the ***Activity Comments History*** field upon the creation of the new activity.
E42.	Populate Physical Address Search Values in New Establishment	The Solution must have the functionality to populate the fields for a new establishment profile with the establishment name, street, city, province, and postal code values when the option has been selected to use the values entered during an Establishment Profile Search.
E43.	Establishment - Update	The Solution must have the functionality to prevent the User from updating the profile of an establishment if the ***Establishment Status*** value is any of the following: a. Inactive b. Inactive: DNS c. Inactive: Potential Duplicate
E44.	Product/Brand	The Solution must have the functionality to set the ***Brand Status*** value to "Inactive" for all active brands associated with the establishment, when the Establishment Status value of an establishment with the ***Establishment Type*** of "Manufacturer" is set to "Inactive".
E45.	Establishment – Create New Owner Function	The Solution must have the functionality for the User to create a new limited copy of an existing establishment profile to accommodate a change in ownership, as follows: a. The limited establishment copy must comprise the following: i. the existing establishment profile information ii. associated establishments iii. contact and contact details, with exception of the former owner b. The following conditions must be met prior to creating the new limited establishment and new owner: i. the ***Establishment Status*** value of the existing establishment must be "Inactive" or Inactive: DNS" ii. the ***Activity Status*** value of all activities associated with the existing establishment is "Closed" c. The limited establishment copy must not include: i. the compliance and enforcement history (includes activities) of the establishment under the former owner(s) (remains with the inactive establishment) ii. Contact details of the former owner (remains with the inactive establishment)
E46.	Compliance and Enforcement History	The Solution must have the functionality to maintain an establishment's compliance and enforcement history of activities throughout all ownerships, which will consist of a rollup of all compliance and enforcement histories relating to the establishment and the establishment's contacts.
E47.	New Establishment not in User's region/sub-region and new activity – Alert User	The Solution must have the functionality to alert the User that the establishment is not from the User's region/sub-region, when the User creates a new establishment profile for an establishment that is outside of the User's region and sub-region.

#	Title	Requirement
E48.	New Establishment not in User's region/sub-region and new activity – "Establishment Status"	The Solution must have the functionality to set the ***Establishment Status*** value to "Pending Validation", when the User creates a new establishment profile for an establishment that is outside of the User's region and sub-region.
E49.	New Establishment not in User's region/sub-region and new activity – Prevent User from Updating	The Solution must have the functionality to prevent the User from updating establishment profile information, other than to provide comments, for an establishment that is outside of the User's region and sub-region.
E50.	New Establishment not in User's region/sub-region and new activity – Send New Activity	The Solution must have the functionality for a User to send the new activity, populated with core information, to the Supervisor/ Supervisor Group in the User's region/sub-region, when the User creates a new establishment profile for an establishment that is outside of the User's region and sub-region.
E51.	Link an Activity to Another Establishment	The Solution must have the functionality to change the link for an activity from one establishment to another.

F. Activity

#	Title	Requirement
F1.	Activity – General Functionality	The Solution must have the functionality for the User to: a. Create a new activity record associated with an existing establishment with an ***Establishment Status*** value of "Active". b. Update and save an existing activity record.
F2.	Activity Tabbed Pane-like Format and Components	The Solution must have the functionality for the User enter, update, and view all information relating to an activity in a tabbed pane-like format (See Requirement C61).
F3.	New Activity Workflow Steps	The Solution must have the functionality to move the User through the following workflow steps to create a new activity: a. when the Activity Type value is "Inspection", "Investigation", or "Internal Quality Assurance" and the Activity Reason Type value is not any of "Industry Reports", the workflow steps are: i. Search for an establishment (See Requirement F4) ii. Select an establishment (See Requirement F5) iii. Create new activity iv. Create activity scope plan v. Document compliance analysis and assessment results vi. Document enforcement action(s) (as required) vii. Close activity or viii. Close with Linked Activity b. when the Activity Type value is "Compliance Promotion" the workflow steps are: i. Search for an establishment ii. Select an establishment iii. Create new activity iv. Create activity scope plan v. Verify establishment location vi. Add to scope (optional) vii. Document compliance promotion results viii. Close activity or ix. Close with Linked Activity
F4.	Activity Workflow Step: Search for an Establishment	The Solution must have the functionality for the User to perform a pre-defined Establishment Profile Search (See Requirement D2) to find an establishment to connect to a new activity.
F5.	Activity Workflow Step: Select an Establishment	The Solution must have the functionality to perform the following: a. For the User to select an establishment from the pre-defined Establishment Profile Search results list to connect with a new activity. b. For the Solution to create a new activity and add it to the User's My Workload field set.
F6.	Activity Tabbed Pane-like Format: General Information component	The Solution must have the functionality for the User to enter, update, and view all data in the General Information component of the Activity "tabbed pane" (See Requirement C62).
F7.	Activity Workflow Step: Enter New Activity Information	The Solution must have the functionality to move the User through the following workflow steps to enter information for a new activity: a. View detailed profile information for the selected establishment. (See Requirement F8) b. Update concerns and issues. (See Requirement C62) c. Update establishment contact information. (See Requirement C62)

#	Title	Requirement
		d. Confirm the review of establishment information is complete. (See Requirement C62) e. View detailed information about an establishment associated with the selected establishment (if any). (See Requirement F13) f. View detailed information about an activity connected to the selected establishment (if any). (See Requirement C62 and F13) g. Confirm the review of the associated establishments and the review of the establishment activity history information is complete. (See Requirement F14) h. Enter activity information into the Core Information and remaining field sets. (See Requirement C62 and F16) i. Confirm the activity information is complete. (See Requirement C62)
F8.	Activity: Establishment Profile View	The Solution must have the functionality for the User to view from the Establishment field set the entire establishment profile information for the selected establishment (See Requirement C62).
F9.	Activity: Establishment - Concerns and Issues	The Solution must have the functionality for the User to update the concerns and issues connected with the selected establishment profile in the Establishment field set in the General Information component (See Requirement C63).
F10.	Activity: Establishment Contacts	The Solution must have the functionality for the User to update contact information connected with the selected establishment profile, in the Establishment Contacts field set in the General Information component (See Requirement C63).
F11.	Activity: Establishment and Contacts Information - Confirm Review	The Solution must have the functionality to require the User to confirm the review of the selected establishment and establishment contacts information is complete in the General Information component (See Requirement C63).
F12.	Activity: Associated Establishments and Other Activities for this Establishment	The Solution must have the functionality for the User to view the following information in the Associated Establishments field set and in the Other Activities for this Establishment field set in the General Information component, when the review of the establishment and establishment contacts information has been confirmed as complete by the User (See Requirement C63): a. All establishments associated with the selected establishment, if any. b. All activities connected to the selected establishment, if any.
F13.	Activity: Associated Establishments and Other Activities for this Establishment - View	The Solution must have the functionality for the User to select and view the following information in the Associated Establishments field set and in the Other Activities for this Establishment field set in the General Information component, (See Requirement C63) the following information: a. An establishment associated with the selected establishment, if any. b. An activity connected to the selected establishment, if any.
F14.	Activity: Associated Establishments and Other Activities for this Establishment - Confirm Review	The Solution must have the functionality to limit the User from moving to the next workflow step until the User confirms the review of the information in the Associated Establishments and Other Activities for this Establishment field sets in the General Information component (See Requirement C63) is complete.
F15.	Activity: Promotional Event	The Solution must have the functionality for the User to select the establishment's existing promotional event and add details for a new promotional event to be connected with a new activity, when the ***Establishment Subtype*** value is "Promoter" (See Requirement C63).
F16.	Activity: Core Information and Other General Information Field Sets	The Solution must have the functionality for the User to input and view the following activity related information field sets and fields in the General Information component, when the review of the information in the Associated Establishments field set and the Other Activities for this Establishment field set has been confirmed as complete by the User (See Requirement C63): a. Core Information

#	Title	Requirement
		i. Activity Reason Type ii. Activity Type iii. Priority b. ***Act***ivity Timeline i. ***Proposed Start Date*** ii. ***Bring Forward Date*** c. Sent To History (viewing only) d. Online Presence e. Links f. Comment History g. Warrants (only if ***Warrant Required*** value is "Yes")
F17.	Activity: Core Information and Other General Information Field Sets – Data Capture	The Solution must have the functionality for the User to enter activity values into the following field sets and fields in the General Information component (See Requirement C63): a. Core Information i. Activity Reason Type (mandatory) ii. Activity Type (mandatory) iii. Priority (mandatory, default value is "Normal") b. ***Act***ivity Timeline i. ***Proposed Start Date*** [any date value] (mandatory) c. Online Presence d. Links e. Comment History f. Warrants (only if ***Warrant Required*** value is "Yes")
F18.	Warrant not issued - Generic	The Solution must have the functionality to set the ***Activity Close Reason*** value to "Not completed, absence of warrant", and the ***Activity Status*** value to "Pending Closure" when the User selects either of the following values: a. ***Supervisor Approval*** value for the warrant request is set to "Rejected" b. ***JP Approval*** value for the warrant request is set to "Rejected"
F19.	Industry Report - New Activity Workflow Steps	The Solution must have the functionality to move the User through the following workflow steps to view/update a new activity: a. View submitted industry report data from the Artifacts Summary field set b. Review compliance assessment results by ***Legislative Section/Subsection*** value c. Review non-compliance history by ***Legislative Section/Subsection*** value d. View grouped errors e. Manually identify and document errors (as required) f. Override a ***Compliance Outcome*** value for a ***Legislative Section/Subsection*** value (as required) g. Review overall compliance summary h. View and update details of a responsible party from the Responsible Party Summary field set i. View/remove brands under Stop Sale (as required) j. Confirm Compliance Assessment information is complete k. Document enforcement action(s) (as required) l. Close activity or m. Close with Linked Activity when the ***Activity Reason Type*** value is any of the following: 1. "Scheduled Industry Report" 2. "Unscheduled Industry Report" 3. "Scheduled Industry Report-Audit"

#	Title	Requirement
		4. "Unscheduled Industry Report-Audit"
F20.	Industry Report – Activity Association of Expected Reports	The Solution must have the functionality to connect the industry report with the open linked activity as soon as an industry ***Report Status*** value is set to "Registered", and the following conditions have occurred: a. the ***Establishment Name, Report Section, and Report Period*** values of incoming industry report match with the same values in an open linked activity b. the ***Report Status*** value of the industry report in the open, linked activity is one of the following: i. "Not due" ii. "Absent-Grace Period"
F21.	Industry Reports - Report Status: Absent - Action Required and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions: a. Set the Report Status value for the required industry report to "Absent-Action Required". b. Create an activity for the establishment connected to the industry report after the grace period date. c. Set the following industry report information values for the activity based on the expected report information values: i. Report Section Number ii. Report Period iii. Report Version iv. ***Report Type*** (if applicable) v. ***Report Due Date*** d. Set the ***Activity Reason Type*** value to "Scheduled: Industry Report". e. Set the ***Activity Type*** value to "Inspection". f. Set the ***Proposed Start Date*** value to the ***Grace Period Due Date*** value. g. Set the ***Activity Scope Plan Type*** value to the ***Report Section Name*** value. h. Set the ***Legislative Section/Subsection*** values applicable for the ***Activity Scope Plan Type***. i. Confirm the Scope Plan is complete. j. Set the ***Activity Status*** value to "Compliance in Progress". k. Set the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** values to "Non-Compliance". l. Set the ***Overall Assessment of Compliance*** value in the Compliance Assessment component to "Non-Compliance-Major". m. Enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane". n. Add the new activity to the ***Designated User's*** My Workload field set in the Workload Overview. when an industry report, based on either of the following, has not been received prior to or on the due date and the ***Grace Period*** has expired: 1. submission frequency 2. request from Health Canada
F22.	Industry Report – Create Activity for a Registered Report - Workflow Steps and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions when an industry ***Report Status*** value is "Registered", and an open activity has not been found for that ***Report Section, Report Period,*** and ***Establishment Name*** values: a. Create an activity for the establishment connected to the industry report based on the industry report information values (for example, ***Report Section***) b. Update the establishment contact information with the ***Author of The Report*** information if the contact information of the Author is not already found

#	Title	Requirement
		c. Set the value to indicate the review of establishment information is confirmed as complete d. Set the value to indicate the review of the associated establishments and the establishment activity history information is confirmed as complete e. Set the ***Activity Type*** value to "Inspection" f. Set the ***Activity Reason Type*** value to one of the following values: i. Scheduled: Industry Report ii. Unscheduled: Industry Report g. Set the ***Proposed Start Date*** value to the ***Report Status Effective Date*** value h. Set the value to indicate the activity initialization information is confirmed as complete i. Set the mandatory field values to read-only j. Set the ***Activity Scope Plan Type*** value to the ***Report Section Name*** value k. Set the ***Legislative Section/Subsection*** values applicable for the ***Activity Scope Plan Type*** value l. Confirm the Scope Plan is complete m. Set the ***Activity Status*** value to "Compliance in Progress" n. enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane" o. Add the new activity to the ***Designated User's*** My Workload field set in the Workload Overview
F23.	Industry Report - Status Changes when Industry Report Connected to Open Activity	The Solution must have the functionality to change the ***Report Status*** value to "Registered" when an industry report is connected to an open industry report activity, where the ***Repor*t *Status*** value is one of the following: a. Not Due b. Absent-Grace Period
F24.	Industry Report Status – Absent-Grace Period	The Solution must have the functionality to set the ***Report Status*** value to "Absent-Grace Period", when a linked, open Activity for which no industry report has been "Registered" has passed its start date.
F25.	Industry Report – Absent Open Activity	The Solution must have the functionality to perform the following actions when a linked, open Activity for which no industry report has been received has passed its ***Grace Period***: a. Set the ***Report Status*** value to "Absent-Action Required". b. Set the ***Legislation Section Compliance Outcome*** value to "Non-Compliance" for each ***Legislative Section/Subsection*** value. c. Set the ***Overall Assessment of Compliance*** value in the Compliance Assessment component to "Non-Compliance-Major".
F26.	Industry Report Audit of a Closed Report Activity	The Solution must have the functionality for the ***Assigned User*** to search for and select an already closed activity with an industry report as an artifact for use in the new activity when an ***Assigned User*** creates an activity in one of the following conditions: a. "Internal Quality Assurance" has been selected as the ***Activity Type*** b. "Inspection" has been selected as the ***Activity Type*** and one of the following ***Activity Reason Type*** values has been selected: i. Scheduled: Industry Report-Audit ii. Unscheduled: Industry Report-Audit
F27.	Industry Report- Activity Created for Audit and Enable Next Components in Workflow	The Solution must have the functionality, when an ***Assigned User*** has selected an already closed activity with an industry report as an artifact for use in the new activity, to perform the following actions: a. Display the fields for the User to enter the Audit Information when the ***Activity Type*** value is "Inspection"

#	Title	Requirement
		b. Set the Activity Reason Type value to the same Activity Reason Type value as in the previously closed activity when the Activity Type value is "Internal Quality Assurance" c. Use the industry report from the closed activity as the artifact in the new activity d. Capture and display in the Artifacts field set the Activity Id value of the closed activity e. Populate the following industry report information for the activity with the industry report artifact information from the previously closed activity: i. Report Section ii. Report Period iii. Report Version iv. ***Report Id*** v. ***Report Type (if applicable)*** vi. ***Report Due Date*** f. Set the ***Activity Scope Plan*** value according to the ***Report Section*** value g. Set the ***Legislative Section/Subsection*** value(s) applicable for the ***Activity Scope Plan Type*** value h. Confirm the Scope Plan is complete i. Set the Activity Status value to "Compliance in Progress" j. Apply the applicable analysis and compliance assessment rules to evaluate the industry report k. Enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane" l. Add the new activity to the My Workload field set in the Workload Overview of the User indicated in the ***Activity Send To*** field
F28.	New Activity: General Information - Confirm Completion of Data Entry	The Solution must have the functionality to limit the User from moving to the next workflow step until the User confirms that the entry of the initial information for a new activity in the General Information component is complete.
F29.	New Activity: Set Values and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions when the information in the General Information component of the new activity has been confirmed by the User, and successfully verified as complete: a. Set the following mandatory fields to the following values: i. Activity Status value to "Planning in Progress" ii. Activity Plan Status Type value to "Draft Plan" b. Set the mandatory field values to read-only c. Add the new activity to the User's "Activities" list in the My Workload field set of the Workload Overview (dashboard) d. Enable for input and viewing the following components of the Activity "tabbed pane": i. Scope Plan ii. Link/Close iii. Send To
F30.	Bulk Create Activities Process	The Solution must have the functionality for the User to bulk create new activities for selected establishments.
F31.	Bulk Create Activities Process: Search for an Establishment	The Solution must have the functionality for the User to perform a pre-defined Bulk Create Activities Search (See Requirement D21) to find establishments to connect to a new activity.
F32.	Bulk Create Activities Search Criteria	The Solution must have the functionality to apply the following search criteria to the Bulk Create Activities Search. a. The selected establishments must not have any of the following: i. ***Activity Scope Plan Type*** value of "Youth Access"

#	Title	Requirement
		ii. Any concerns iii. Any issues iv. Any previous non compliances in the past 12 months v. Any open activities
F33.	Bulk Create Activities: Details	The Solution must have the functionality to perform the following actions when the User initiates the Bulk Create Activities process: a. Permit the User to select the values for the following fields: i. Activity Type ii. Activity Scope Plan Type iii. Proposed Start Date b. Populate each activity with the User selected values c. Populate the following fields in each activity with the following values: i. Activity Status value: "Pending Compliance" ii. Activity Reason Type value: "Scheduled: Workplan" iii. Activity Send To value: [current User's name] iv. ***Activity Plan Status Type*** value: "Approved" v. ***Activity Priority*** value: "Normal"
F34.	Bulk Create Audit Industry Report Activities	The Solution must have the functionality for the User to create bulk audit activities for Establishment Manufacturer(s) by ***Report Section*** and ***Report Period*** values and enter Audit Information that will be populated in each of the activities created.
F35.	Bulk Create Audit Industry Report Activities: Details	The Solution must have the functionality to perform the following actions in the following order when the User initiates the Bulk Create Activities process for Activity Reason Type value of "Scheduled Industry Report-Audit": a. Permit the User to select the values for the following fields: i. Activity Type ii. Activity Scope Plan Type iii. Audit Wave iv. Proposed Start Date v. Report Section Name vi. Report Period vii. Consumer Product Type b. Prompt and permit the User to link documents in the Audit Plan Documentation field set that will be in each activity created by the Bulk Create Activities process. c. Populate the following fields in each activity with the following values: i. Activity Type value: "Inspection" ii. Activity Status value: "Pending Compliance" iii. Activity Reason Type value: "Scheduled Industry Report-Audit" iv. ***Activity Send To*** value***:*** [current User's name] v. ***Activity Plan Status Type*** value***:*** "Approved" vi. ***Activity Priority*** value***:*** "Normal" d. Create the required number of activities with the above information based on the number of establishments and the number of reports that would be reported for the selected ***Report Section*** and ***Report Period*** values***.*** For example, the User wants to create bulk activities for establishment A, B, and C who manufacturer cigarettes that would have a ***Report Section*** value of "13" and cover a ***Report Period*** of 2018-01-01 to 2018-12-31. Since those establishments, all submitted monthly the "Section 13-Report on Sales of Consumer Tobacco Products," for that stated report period, the Solution must therefore create 36 activities with an ***Activity Reason Type value*** of "Scheduled

#	Title	Requirement
		Industry Report-Audit" with an ***Audit Wave*** number specified by the ***Assigned User***.
F36.	Open Activity from "My Workload" (Dashboard) – Industry Report	The Solution must have the functionality to open the activity at the Compliance Results field set of the Compliance Assessment component of the Activity "tabbed pane" when the User accesses an activity from their My Workload field set in the Workload Overview (dashboard), when the ***Activity Reason Type*** is any "Industry Report", and no changes have been made to the activity.

G. Activity: Scope Plan

#	Title	Requirement
G1.	Activity Tabbed Pane-like Format: Scope Plan component	The Solution must have the functionality for the User to enter, update, and view all data in the Scope Plan component of the Activity "tabbed pane" (See Requirement C64).
G2.	Activity Workflow Step: Create Scope Plan	The Solution must have the functionality for the User to select an ***Activity Scope Plan Type*** value in the Scope Plan component to create a scope plan.
G3.	Activity Scope Plan: Applicable Legislation Values List	The Solution must have the functionality to display in the Activity Scope Details field set the ***Legislative Section/Subsection*** values depending on the values previously populated in the following activity fields when the User selects an ***Activity Scope Plan Type*** value: a. ***Activity Scope Plan Type*** b. ***Establishment Type*** c. ***Activity Reason Type*** d. ***Proposed Start Date***
G4.	Activity Scope Plan: Legislative Values - Default Selected	The Solution must have the functionality to set all ***Legislative Section/Subsection*** value(s) associated with the selected ***Activity Scope Plan Type*** value to a "selected" state when the ***Activity Type*** value is any of the following: a. "Inspection" b. "Compliance Promotion".
G5.	Activity Scope Plan: Legislative Sections - Default Unselected	The Solution must have the functionality to set all ***Legislative Section/Subsection*** value(s) associated with the selected ***Activity Scope Plan Type*** value of "General" as "unselected" when the ***Activity Type*** value is "Investigation".
G6.	Activity Scope Plan Type: Modify	The Solution must have the functionality for the User to modify the ***Activity Scope Plan Type*** value within the Scope Plan component at any time prior to the User confirming the Scope Plan is complete.
G7.	Activity Scope Plan: Select Legislation Values	The Solution must have the functionality for the User to select and de-select any available ***Legislative Section/Subsection*** values listed in the Activity Scope Details field set at any time prior to the User confirming the information in the Scope Plan is complete.
G8.	Linked Activity Scope Plan	The Solution must have the functionality to perform the following actions when a linked activity is created: a. Set the ***Scope Plan Type*** value of the linked activity to the ***Scope Plan Type*** value of the original activity b. Select ***Legislative Section/Subsection*** value(s) where the ***Legislation Section Compliance Outcome*** value in the original activity is "Non-Compliance"

#	Title	Requirement
		c. Set the selected ***Legislative Section/Subsection*** value(s) selected by the Solution to read-only d. Permit the User to select additional ***Legislative Section/Subsection*** value(s)
G9.	Activity Scope Plan – Supervisor confirmed scope	The Solution must have the functionality for Supervisors to set the ***Activity Scope Plan*** value in the Activity Scope Details field set of the Scope Plan component.
G10.	Activity Scope Details	The Solution must have the functionality for the assigned Subordinate to select or de-select any ***Legislative Section/Subsection*** value in the Activity Scope Details field set of the Scope Plan component that was set by a Supervisor for the ***Activity Scope Plan*** value.
G11.	Activity Scope Plan: Minimum Scope Selected	The Solution must have the functionality to verify a minimum of one ***Legislative Section/Subsection*** value has been selected before the User can confirm that the Scope Plan is complete.
G12.	Activity Scope Plan – confirmed/ unconfirmed	The Solution must have the functionality to perform the following actions when a Supervisor sets the ***Activity Scope Plan*** value, and the assigned Subordinate selects or de-selects any ***Legislative Section/Subsection*** value in the Activity Scope Details field set: a. Prevent the Subordinate User from confirming the scope plan as complete. b. Prompt the Subordinate User to send the activity to a Supervisor for action.
G13.	Confirm Selected Legislative Section/Subsections	The Solution must have the functionality to limit the User from moving to the next workflow step until the User confirms the information in the Scope Plan component is complete.
G14.	Activity – Scope Plan Confirm and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions when the information in the Scope Plan component has been confirmed by the User, and successfully validated and verified as complete: a. Set the ***Activity Status*** value to "Pending Compliance". b. Set the Ac***tivity Plan Status Type*** value to "Approved". c. Set all Scope Plan field values to read-only. d. Enable for input and viewing the Compliance Assessment component of the Activity "tabbed pane" and the fields in the Establishment Location Verification field set.

H. Activity: Compliance Assessment – Establishment Location Verification

#	Title	Requirement
H1.	Activity Tabbed Pane-like Format: Compliance Assessment component	The Solution must have the functionality for the User to enter, update, and view all information in the Compliance Assessment component of the Activity "tabbed pane" (See Requirement C65).
H2.	Compliance Assessment	The Solution must have the functionality to move the User through the following workflow steps to document compliance assessment: a. Verify establishment location b. Confirm establishment location verification is complete c. Document person spoken to d. Confirm establishment profile information was verified e. Document Compliance Results for each artifact: i. Document Artifact Collection ii. Document Artifact Analysis results for each Legislative Section/Subsection value for the artifact iii. Document Linked files iv. Document the Responsible Party for each ***Legislative Section/Subsection*** value in the artifact analysis where non-compliance is indicated f. Update Compliance Result field set g. View and update details of an artifact from Artifact Summary field set h. View and update details of a responsible party from Responsible Party Summary field set i. Confirm Compliance Assessment information is complete
H3.	Activity Workflow Step: Compliance Assessment component – Establishment Location	The Solution must have the functionality for the User to enter the required values in the Establishment Location Verification field set in the Compliance Assessment component (See Requirement C66).
H4.	Activity Workflow Step: Compliance Assessment component – Actual Date and Time	The Solution must have the functionality for the User to enter the ***Actual Start Date*** and ***Actual Start Time*** values in the Establishment Location Verification field set in the Compliance Assessment component (See Requirement C66).
H5.	Establishment Location Verification	The Solution must have the functionality to limit the User from moving to the next workflow step until the User confirms when finished entering information in the Establishment Location Verification field set in the Compliance Assessment component (See Requirement C66).
H6.	Establishment Location Verification – By Portal and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions when the Activity Reason Type value is any of "Industry Reports": a. Set Activity Establishment Verification Code value to "Verified by Portal". b. Set the Actual Start Date value to the system date value. c. Set the Actual Start Time value to the system time value. d. Confirm the information in the Establishment Location Verification field set is complete. e. Set all field values in the Establishment Location Verification field set to read-only. f. Set the following fields to the following values: i. Activity Status value to "Compliance In Progress" ii. Activity Plan Status Type value to "Approved" iii. confirm the establishment profile information is verified g. Enable for input and viewing the following field sets of the Compliance Assessment component: i. Compliance Results ii. Artifacts Summary iii. Responsible Party Summary

#	Title	Requirement
H7.	Establishment Location Verification - Confirm location is verified and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions: a. set all field values in the Establishment Location Verification field set to read-only b. set the following fields to the following values: i. Activity Status value to "Compliance In Progress" ii. Activity Plan Status Type value to "Approved" c. enable for input and viewing the following field sets and fields of the Compliance Assessment component: i. Person Spoken To ii. Add Person Spoken To iii. Establishment Profile Verified (field) when the entry of information in the Establishment Location Verification field set of the Compliance Assessment component is confirmed as complete by the User with any of the following values: 1. "Verified by Portal" 2. "Establishment Verified at Specified Location" 3. "New Address Updated-Verified at New Address"
H8.	Establishment Location Verification - Address Unknown	The Solution must have the functionality to perform the following actions when the information in the Establishment Location Verification field set of the Compliance Assessment component is confirmed as complete by the User and validated with "Address unknown": a. prevent previously confirmed fields to be edited b. set the following fields to the following values: i. Activity Status value to "Closed" ii. Activity Plan Status Type value to "Approved" c. close the activity with the following values: i. set Linked To value to "N/A" ii. set Activity Close Reason value to "Activity completed with/without enforcement action" iii. set Close Activity Now value to "Yes" d. set the ***Establishment Status*** value to "Inactive" in the establishment profile for the establishment identified as the ***Location of the Activity***
H9.	Establishment Location Verification - Location DNS	The Solution must have the functionality to perform the following actions when the information in the Establishment Location Verification field set of the Compliance Assessment component is confirmed as complete and validated with "Establishment no longer selling, manufacturing, or importing tobacco products": a. Prevent previously confirmed fields to be edited b. Set the following fields to the following values: i. Activity Status value to "Closed" ii. Activity Plan Status Type value to "Approved" c. Close the activity with the following values: iii. Set Linked To value to "N/A" iv. Set ***Activity Close Reason*** value to "Activity completed with/without enforcement action" v. Set ***Close Activity Now*** value to "Yes" d. Set the ***Establishment Status*** value to "DNS" in the establishment profile for the establishment identified as the ***Location of the Activity***
H10.	Establishment Location Verification - Location Out of Business	The Solution must have the functionality to perform the following actions when the information in the Establishment Location Verification field set of the Compliance Assessment component is confirmed as complete and validated with "Establishment out of business": a. Prevent previously confirmed fields to be updated

#	Title	Requirement
		b. Set the following fields to the following values: i. Activity Status value to "Closed" ii. Activity Plan Status Type value to "Approved" c. Close the activity with the following values: i. Set Linked To value to "N/A" ii. Set Activity Close Reason value to "Activity completed with/without enforcement action" iii. Set Close Activity Now value to "Yes" d. Set the ***Establishment Status*** value to "Inactive" in the establishment profile for the establishment identified as the ***Location of the Activity***
H11.	Warrant Executed – Generic	The Solution must have the functionality for the User to perform the following, in the Establishment Location Verification field set of the Compliance Assessment component: a. Confirm when a warrant has been executed b. Enter the required values for the warrant (See Requirement C90)

I. Activity: Compliance Assessment – Person Spoken To/Verify Establishment Profile/Add Scope

#	Title	Requirement
I1.	Activity Workflow Step: Compliance Assessment component - Person Spoken To	The Solution must have the functionality for the User to perform the following actions in the Person Spoken To field set (See Requirement C66) and the Add Scope field set (See Requirement C64) within the Compliance Assessment component: a. Select a minimum of one person spoken to as the contact. b. Select multiple "Person Spoken To" contacts. c. Add a new establishment contact to the contact list connected to the establishment profile. d. View, update, delete contact information connected with the establishment profile.
I2.	Activity Workflow Step: Compliance Assessment component – Verify Establishment Profile	The Solution must have the functionality to limit the User from moving to the next workflow step in the Compliance Assessment component until the User confirms that the establishment profile information has been verified and updated.
I3.	Compliance Assessment component – Field Sets	The Solution must have the functionality to enter, update, and view the following field sets in the Compliance Assessment component when the establishment profile information is confirmed as verified by the User: a. Add Scope b. Compliance Results (if Activity Type value is not "Compliance Promotion") c. Compliance Promotion Results (if Activity Type value is "Compliance Promotion") d. Artifacts Summary e. Responsible Party Summary f. Test Shopper (if Scope Plan Type value is "Youth Access") g. Total Number of CIP Samples (if applicable)
I4.	Activity Tabbed Pane-like Format: Compliance Assessment component – Add Scope	The Solution must have the functionality for the User to add ***Legislative Section/Subsection*** value(s) to the list of previously selected ***Legislative Section/Subsection*** value(s) in the Compliance Results field set of the Compliance Assessment component. (See Requirement C68).
I5.	Legislation Currently Not In Scope	The Solution must have the functionality for the User to select from a list of available ***Legislative Section/Subsection*** value(s) that have not previously been selected in the Scope Plan and are applicable to the selected ***Activity Scope Type***.

J. Activity: Compliance Assessment – Results

#	Title	Requirement
J1.	Activity Workflow Step: Compliance Assessment component – Compliance Results	The Solution must have the functionality for the User to enter, update, and view all information in the Compliance Results field set in the Compliance Assessment component (See Requirement C68).
J2.	Compliance Results	The Solution must have the functionality to populate the ***Legislation*** field in the Compliance Results field set with all ***Legislative Section/Subsection*** values selected previously in the Scope Plan component.
J3.	Assessment of Compliance for each legislative section/subsection – Inspection / Investigation	The Solution must have the functionality for the User to select one of the following ***Legislation Section Compliance Outcome*** values for a ***Legislative Section/Subsection*** value listed in the Compliance Results field set when compliance assessment is not required: a. "Not Inspected" b. "Not Applicable"
J4.	Artifact: Select Analysis Type Workflow	The Solution must have the functionality for the User to select the ***Artifact Analysis Type*** value for the ***Legislative Section/Subsection*** value when compliance assessment is required for a ***Legislative Section/Subsection*** value listed in the Compliance Results field set.
J5.	Artifact: Add for Select Legislation	The Solution must have the functionality for the User to select to add an artifact for the ***Legislative Section/Subsection*** value that has the ***Artifact Analysis Type*** value selected.
J6.	Compliance Assessment Outcome - Artifact	The Solution must have the functionality to set the ***Legislation Section Compliance Outcome*** value for the legislative section/subsection in the Compliance Results field set as read-only when an artifact has been added.
J7.	Display Count of Artifacts for each Legislative Section/Subsection	The Solution must have the functionality to display the total number of artifacts added to each ***Legislative Section/Subsection*** value in the Compliance Results field set.
J8.	Display Derived Legislation Section Compliance Outcome Value – One or More Artifacts Added	The Solution must have the functionality to derive and display in the Compliance Results field set the ***Legislation Section Compliance Outcome*** value or each ***Legislative Section/Subsection*** value derived from the ***Overall Artifact Compliance Outcome*** value of each artifact added to the ***Legislative Section/Subsection*** value, as follows: a. If the ***Overall Artifact Compliance Outcome*** value for any artifact is "Non-Compliance", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "Non-Compliance" b. If no artifact has an ***Overall Artifact Compliance Outcome*** value of "Non-Compliance" and the ***Overall Artifact Compliance Outcome*** value for at least one artifact is "No Evidence of Non-Compliance", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "No Evidence of Non-Compliance" c. If the ***Overall Artifact Compliance Outcome*** value for all artifacts is "Not Applicable", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "Not Applicable" d. If the ***Overall Artifact Compliance Outcome*** value for all artifacts is "Not Inspected", the ***Legislation Section Compliance Outcome*** value for the ***Legislative Section/Subsection*** value is derived as "Not Inspected".
J9.	Industry Reports - Compliance Assessment by Legislative Section/Subsection - Grouping Requirements	The Solution must have the functionality to group the error reasons, including their related errors, by the ***Legislative Section/Subsection*** value based on values set by the Solution Administrator, when the ***Activity Reason Type*** value is any of "Industry Reports".

#	Title	Requirement
J10.	Industry Reports - Compliance Assessment by Legislative Section/Subsection - Error Display Requirements	The Solution must have the functionality to display the following in the Compliance Results field set, when the ***Activity Reason Type*** value is any of "Industry Reports": a. ***Number of Errors*** by ***Legislative Section/Subsection*** value b. ***Total Number of Errors*** for all ***Legislative Sections/Subsections***
J11.	Industry Reports - Compliance Assessment by Legislative Section/Subsection - Errors Grouping Requirements	The Solution must have the functionality for the User to view a summary of the errors grouped by ***Legislative Section/Subsection*** value displayed in a view titled "Errors Grouped by Legislative Section/Subsection" (See Requirement C79), when the following conditions are met: a. the ***Activity Reason Type*** value is any of "Industry Reports" b. the ***Assigned User*** selects either of the following: i. the ***Number of Errors*** value beside any ***Legislative Section/Subsection*** value ii. the ***Total Number of Errors*** value (See Requirement C79)
J12.	Industry Reports - Errors Identified by the User	The Solution must have the functionality for the ***Assigned Use***r to manually identify and document errors related to the artifact that were not flagged by the Solution's validation (See Requirement C81) when the ***Activity Reason Type*** value is any of "Industry Reports".
J13.	Industry Reports - Compliance Assessment by Legislative Section/Subsection - User Override Prompt	The Solution must have the functionality to limit the User from moving to the next workflow step until the User confirms the change in value when the User changes the ***Compliance Outcome*** value set by the Solution for a ***Legislative Section/Subsection*** value and the ***Activity Reason Type*** value is any of "Industry Reports". The Solution must have the functionality to update the ***Compliance Outcome*** value with the changed value after the User has: a. Confirmed the change in the value. b. Entered a reason for the override in the Sections Overridden field set.
J14.	Industry Report Audit-Differences in Compliance Assessment Values for two activities with the same report as the artifact	The Solution must have the functionality to visually indicate any differences between the compliance assessment values of two industry report activities, when the following conditions occur: a. One of the following Activity Reason Type values has been selected: ii. Scheduled: Industry Report-Audit iii. Unscheduled: Industry Report-Audit iv. Internal Quality Assurance b. The User has selected a compliance assessment value for a ***Legislative Section/Subsection*** value. For example: a. Highlight the selected compliance assessment value if it differs from the previous industry report b. Display (for example, a mouse-over) the original compliance assessment value
J15.	Industry Report Audit-Differences in Compliance Assessment Values for two activities with the same industry report	The Solution must have the functionality to prompt the User, when a compliance assessment value differs from the compliance assessment value of the original industry report, to enter a reason, in the comment box, for the difference in the values.
J16.	Industry Reports - Legislative Section/Subsection Refresh After Update	The Solution must have the functionality to update the ***Compliance Outcome*** value based on the actions of the User in real time, when the ***Activity Reason***

#	Title	Requirement
		Type value is any of "Industry Reports" and the User manually identifies an error or overrides the ***Compliance Outcome*** value set by the Solution.
J17.	Assessment of Compliance – Early Completion	The Solution must have the functionality to perform the following actions, when the User selects the ***Establishment Location Verification*** value "Unable to Verify Establishment – Entry Refuse: a. Set the ***Legislative Section Compliance Assessment Value*** for Section 38(2) of the ***Tobacco and Vaping Products Act*** to "Non-Compliance". b. Permit the User to select the responsible establishment/party for Section 38(2). c. Require the User to confirm the Assessment of Compliance for the activity (locks it down).
J18.	Assessment of Compliance for each legislative section/subsection – Compliance Promotion	The Solution must have the functionality for the User to document the results of a Compliance Promotion activity by selecting the ***Compliance Outcome*** value for each selected ***Legislative Section/Subsection*** value.
J19.	Industry Reports - Overall Assessment of Compliance	The Solution must have the functionality to perform the following actions, when the Activity Reason Type value is any of "Industry Reports": a. Display the State of Compliance and Level of Compliance values for the activity in the "Compliance Summary" field set and related fields. b. Derive and populate the Activity Compliance Outcome value by setting the State of Compliance and Level of Compliance values in the Compliance Summary field set to one of the following values: i. "Non-Compliance-Minor" if the Legislative Section/Subsection value(s) found to be "Non-Compliance" were set to "Minor" Compliance Level in a maximum of 5 instances. ii. "Non-Compliance-Major" if the Legislative Section/Subsection value(s) found to be "Non-Compliance" had at least one where a "Major" Compliance Level was set. iii. "No Evidence of Non-Compliance" if at least one Legislative Section/Subsection value was found to be "No Evidence of Non-compliance", but no Legislative Section/Subsection values were found to be "Non-Compliance". iv. "Not assessed" if all Legislative Section/Subsection values were found to be "Not assessed". v. "Not Applicable" if all ***Legislative Section/Subsection*** values were found to be "Not Applicable".
J20.	Industry Reports - Overall Assessment of Compliance - Totals of Non-Compliances and Errors	The Solution must have the functionality to perform the following actions, when the ***Activity Reason Type*** value is any of "Industry Reports": a. Calculate the total number of ***Legislative Section/Subsection*** values with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Minor". b. Calculate the total number of ***Legislative Section/Subsection*** values with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Major". c. Calculate the number of errors for ***Legislative Section/Subsection*** values with the ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Minor". d. Calculate the number of errors for ***Legislative Section/Subsection*** values with the ***Legislation Section Compliance Outcome*** value of "Non-Compliance-Major".
J21.	Industry Reports - Overall Assessment of Compliance -	The Solution must have the functionality to display the following values in the summary table of the non-compliances in the Compliance Summary field set

#	Title	Requirement
	Display Requirements in a Industry Report Activity	in the following manner, when the ***Activity Reason Type*** value is any of "Industry Reports": a. The number of non-compliances by ***Compliance Outcome Level***, Major and Minor. b. The Number of errors by ***Compliance Outcome Level***, Major and Minor. c. The sum total of the number of non-compliances. d. The sum total of the number of errors.
J22.	Industry Reports - Overall Assessment of Compliance-Automatic Selection	The Solution must have the functionality to limit the User from overriding the selected value in the Overall Assessment of Compliance Section when the ***Activity Reason Type*** value is any of "Industry Reports".
J23.	Industry Reports - Stop Sale Removal	The Solution must have the functionality for the User to enter, update, and view information in the Compliance Assessment component when a ***Stop Sale*** value is set to "No" (designation is removed), when the ***Activity Reason Type*** value is any of "Industry Reports".
J24.	Industry Reports – Stop Sale Effective Date	The Solution must have the functionality to set the ***Effective Start Date*** value to the system date value when the ***Stop Sale*** value is "Yes" (designation is added).
J25.	Industry Reports - Stop Sale Removal Display Requirements	The Solution must have the functionality to display the ***Brand Name*** value(s) with a ***Stop Sale*** value of "Yes" designation in the Compliance Assessment component.
J26.	Industry Reports - Stop Sale Removal	The Solution must have the functionality for the User to select the ***Brand Name*** value where a ***Stop Sale*** designation value needs to be set to "No" when the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports". b. The ***Stop Sale*** designation has a value of "Yes" for a ***Brand Name*** value. c. That ***Brand Name*** value is included in a submitted industry report that: i. Has a ***Report Version*** value of "Revision" or "Revision and Addendum" ii. Linked to a closed activity in which the ***Stop Sale*** designation value is "Yes".
J27.	Industry Reports - Stop Sale Removal Requirements	The Solution must have the functionality for the User to perform the following actions, when the ***Activity Reason Type*** value is any of "Industry Reports": a. Document the decision for the Stop Sale removal b. Document the links for letters related to the Stop Sale Removal
J28.	Industry Reports - Stop Sale Removal Link	The Solution must have the functionality to display a list of the activity numbers linked to the establishment, where the brand is under a Stop Sale designation value of "Yes", when the following conditions occur: a. the ***Activity Reason Type*** value is any of "Industry Reports" b. the ***Activity Start Date*** value is greater than the ***Actual Start Date*** designation for the brand

K. Activity: Compliance Assessment – Documentation of Artifacts

#	Title	Requirement
K1.	Artifact "Tabbed pane": Documentation	The Solution must have the functionality for the User to enter, update, and view all data for an artifact for a selected ***Legislative Section/Subsection*** value and for a selected ***Artifact Analysis Type*** value in the Artifact "tabbed pane" (See Requirement C68).
K2.	Artifact "Tabbed pane": Header Information	The Solution must have the functionality to populate the following artifact field values in the header field set of the Artifact "tabbed pane" (See Requirement C69): a. ***Establishment Name*** value is "[***Establishment Name*** value for the activity]" b. ***Artifact Id*** value is "[***Artifact Id*** value]" c. ***Legislative Section/Subsection*** value is "[value previously selected in the Compliance Assessment field set for which the artifact is being assessed]" d. ***Artifact Analysis Type*** value is "[value previously selected by the User in the Compliance Assessment field set]"
K3.	Artifact "Tabbed pane": Collection Component	The Solution must have the functionality for the User to enter, update, and view the artifact collection information values for the fields in the Collection component of the Artifact "tabbed pane" (See Requirement C70).
K4.	Artifact "Tabbed pane": Analysis Component	The Solution must have the functionality for the User to enter, update, and view the analysis information values for the artifact fields in the Analysis component of the Artifact "tabbed pane" (See Requirement C71).
K5.	Artifact – Perform Calculations	The Solution must have the functionality to perform calculations according to the ***Artifact Analysis Type*** value. Examples: a. Calculate the labelling area based on the User-entered height and width and set the ***Legislation Section Compliance Assessment*** value for the applicable ***Legislative Section/Subsection*** value to "Non-Compliance" when the labelling area is determined to be less than a predefined value. b. Set the ***Activity Compliance Assessment*** value for Part III Labelling to "Non-Compliance" when one or more TPIR ***Legislation Section Compliance Assessment*** values has a value of "Non-Compliance". c. Notify the User of the applicable Excise Stamp coverage measurements to record based on the TPLR artifact. d. Determine if a "Heath Warning Message" is on the correct side of a cigarette package based on the size of the "Health Warning Message" compared to the size of display area of the cigarette package. e. When the ***Report Section*** value is "11", sum the ***Ingredient Amount*** values for each ***Brand*** value and compare it against the reported ***Product Weight*** value. If the sum is greater than ± a specified range of the ***Product Weight*** value, flag this error and set the ***Legislation Section Compliance Assessment*** value for the ***Legislative Section/Subsection*** value of "11(1)(d)" to "Non-Compliance". f. When the ***Report Section*** value is "13", verify the ***Total Volume Sold*** value for each ***Brand*** value. If the validation fails, then the Solution must flag this error and set the ***Legislation Section Compliance Assessment*** value for the ***Legislative Section/Subsection*** value of "13(2)" to "Non-Compliance". Perform the validation in the following manner: i. If the ***Unit of Measure of Package*** value is "g", then the ***Total Volume Sold*** value must equal the value from the following calculation: ***Amount Per Package*** * ***Total Packs Sold***/1000

#	Title	Requirement
		ii. If the ***Unit of Measure of Package*** value is not "g", then the ***Total Volume Sold*** value must equal the value from the following calculation: ***Amount Per Package*** * ***Total Packs Sold*** g. Identify missing, incomplete, and incorrect data submitted for an industry report.
K6.	Industry Report - Consolidate Industry Report Data from a previous R***eport Period***	The Solution must have the functionality to create a consolidated industry report data set by combining the most recent data derived from multiple submissions of a specified industry report for a specified ***Report Period*** value. The consolidated industry report data set would be used for viewing, comparison, and identification of changes between ***Report Period*** values. For example: if some industry report data are revised in a later submission for the specified ***Report P***eriod value, the consolidated industry report data set will include the latest data submitted rather than the original data submitted.
K7.	Industry Report - Compare Consolidated Industry Report Data from a previous R***eport Period***	The Solution must have the functionality to: a. Compare data of the industry report against the industry report with the same Report Section value from a previous period. b. Use the most up to date industry data consolidated from the submissions of the previous period. c. Identify any changes in the data that exceeds the High Variance Threshold value. When all the following conditions occur: 1. The Activity Reason Type value is any of "Industry Reports". 2. The industry report has been submitted with any of the following Report Section values: i. "11" ii. "12" iii. "14.1" 3. an industry report with the same ***Report Section*** value has been submitted in the previous ***Report Period*** value. Example of a comparison between ***Report Period*** values that identifies a change in value beyond a specific High Variance Threshold value: Event 1. An industry report with a ***Report Section*** value of "12" and a ***Report Version*** value of "Original" was submitted with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is "Cigee" c. ***Constituent Name*** value is "Myosmine" d. ***Constituent Mean*** value is "0". Event 2. An industry report with a ***Report Section*** value of "12" and a ***Report Version*** value of "Revision" was later submitted with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is ***"***Cigee" c. ***Constituent Name*** value is "Myosmine" d. ***Constituent Mean*** value is "15". Event 3.

#	Title	Requirement
		For the next ***Report Period*** value, an industry report with a ***Report Section*** value of "12" and a ***Report Version*** value of "Original" was submitted with the following information: a. ***Report Period*** value is "20200101-20201231" b. ***Brand*** value is "Cigee" c. ***Constituent Name*** value is "Myosmine" d. ***Constituent Mean*** value is "12". Expected result for the above example: For the ***Brand*** value of "Cigee" and the ***Constituent Name*** value of "Myosmine" the Solution must: a. compare the ***Constituent Mean*** values of "12" and "15" b. identify that the change of 25% greater than or equal to the High Variance Threshold value of 20%
K8.	Industry Report – Compare to Identify Duplicate Data	The Solution must have the functionality to compare industry report data to identify duplicate data, using the following comparison types: a. the industry report data is compared between the most recently received version of an industry report and the previously received version of the industry report when all the following conditions are met: i. The Activity Reason Type value is any of "Industry Reports". ii. The Report Status value is "Registered". iii. The Report Period value for both industry reports are the same. Example: Event 1. An industry report with a ***Report Section*** value of "11" and a ***Report Version*** value of "Original" was submitted with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is "Smokee" c. ***Ingredient Name*** value is "Methyl Cellulose" d. A***mount*** value is "11". Event 2. An industry report with a ***Report Section*** value of "11" and a ***Report Version*** value of "Replacement" was later submitted with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is "Smokee" c. ***Ingredient Name*** value is "Methyl Cellulose" d. A***mount*** value is "11". Expected result based on the above Example: For the ***Brand*** value of "Smokee" the Solution must identify that the ***Ingredient Name*** value of "Methly Cellulose" is a duplicate in the industry report with the ***Report Version*** value of "Replacement". b. The consolidated industry report data of the submitted ***Report Period*** value is compared with the consolidated industry report data of the previous ***Report Period*** value when all the following conditions are met: 1. The ***Activity Reason Type*** value is any of "Industry Reports". 2. The ***Report Period*** value for the industry reports are different. Example 2: Event 1.

#	Title	Requirement
		An industry report with a ***Report Section*** value of "12" and a ***Report Version*** value of "Original" was submitted with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is "Smothee" c. ***Constituent Name*** value is "Anatabine" d. ***Constituent Mean*** value is "0". Event 2. An industry report with a ***Report Section*** value of "12" and a ***Report Version*** value of "Revision" was later submitted with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is ***"***Smothee" c. ***Constituent Name*** value is Anatabine" d. ***Constituent Mean*** value is "15". Event 3. For the next ***Report Period*** value, an industry report with a ***Report Section*** value of "12" and a ***Report Version*** value of "Original" was submitted with the following information: a. ***Report Period*** value is "20200101-20201231" b. ***Brand*** value is ***"***Smothee" c. ***Constituent Name*** value is "Anatabine" d. ***Constituent Mean*** value is "15". Expected results for the above example: For the ***Brand*** value of "Smothee" and ***Constituent Name*** value of "Anatabine" the Solution must identify that a duplicate record exists as the ***Constituent Mean*** values are both "15" in the industry report with the ***Report Version*** value of "Revision".
K9.	Industry Report-Rebuttal Brand Validation Check	The Solution must have the functionality to not perform a Brand Validation Check on a submitted industry report when the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" b. The ***Report Type*** value is "Rebuttal"
K10.	Industry Report- Brand Validation Check	The Solution must have the functionality to perform a Brand Validation Check on a submitted industry report for any of the following ***Report Section*** values: a. "10" b. "11" c. "12" d. "13" e. "14" f. "14.1" g. "14.2" h. "20" When the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values. b. The ***Report Status*** value is "Registered".
K11.	Industry Report-General Validation	The Solution must have the functionality to identify any validation errors within the industry report.
K12.	Artifact "Tabbed Pane": Analysis Component – User	The Solution must have the functionality for the User to select the ***Overall Artifact Compliance Assessment Outcome*** value for the artifact when the artifact is assessed against only one ***Legislative Section/Subsection*** value.

#	Title	Requirement
	Selected ***Overall Artifact Compliance Outcome***	
K13.	Artifact "Tabbed Pane": Analysis Component - ***Overall Artifact Compliance Outcome*** Value Read-only	The Solution must have the functionality to set the ***Overall Artifact Compliance Outcome*** value for the artifact in the Overall Compliance Assessment field set of the Analysis component as read-only when the following conditions occur: a. The artifact is assessed against multiple ***Legislative Sections/Subsection*** values. b. The ***Overall Artifact Compliance Outcome*** value has been derived by the Solution.
K14.	Solution Derived ***Overall Artifact Compliance Outcome*** Value - Override	The Solution must have the functionality for the User to override the ***Compliance Outcome*** value for a ***Legislative Section/Subsection*** value derived by the Solution when the ***Artifact Analysis Type*** value is "Industry Report Analysis".
K15.	Solution Derived ***Overall Artifact Compliance Outcome*** Value - More Than One Legislative Section/Subsection for the Artifact	The Solution must have the functionality to derive the ***Overall Artifact Compliance Outcome*** value of the artifact as follows when more than one Legislative Section/Section value is used in the analysis of an artifact: a. If the ***Legislation Section Compliance Outcome*** value for any ***Legislative Section/Subsection*** value is "Non-Compliance", the ***Overall Artifact Compliance Outcome*** value for the artifact is derived as "Non-Compliance". b. If no ***Legislative Section/Subsection*** value has a ***Legislation Section Compliance Outcome*** value of "Non-Compliance" and the ***Legislation Section Compliance Outcome*** value for at least one ***Legislative Section/ Subsection*** value is "No Evidence of Non-Compliance", the ***Overall Artifact Compliance Outcome*** value for the artifact is derived as "No Evidence of Non-Compliance". c. If the ***Legislation Section Compliance Outcome*** value for all ***Legislative Section/Subsection*** values is "Not Applicable", the ***Overall Artifact Compliance Outcome*** value for the artifact is derived as "Not Applicable". d. If the ***Legislation Section Compliance Outcome*** value for all ***Legislative Section/Subsection*** values is "Not Inspected", the ***Overall Artifact Compliance Outcome*** value for the artifact is derived as "Not Inspected". For example: One value of "Non-Compliance" and three values of "No Evidence of Non-Compliance" will result in an ***Overall Artifact Compliance Outcome*** value of "Non-Compliance".
K16.	Select Responsible Party	The Solution must have the functionality for the User to select a ***Full Name*** value from the list of contacts associated with the establishment profile as the ***Responsible Party*** value for each ***Legislative Section/Subsection*** value listed in the Analysis component where non-compliance is indicated (See Requirement C57).
K17.	New Responsible Party	The Solution must have the functionality for the User to create a new establishment contact associated with an establishment profile to use as the ***Responsible Party*** value for each ***Legislative Section/Subsection*** value listed in the Analysis component where non-compliance is indicated (See Requirement C57).
K18.	Artifact "Tabbed Pane" : Links Component	The Solution must have the functionality for the User to enter, update, and view the linked document information values for the fields in the Linked component of the Artifact "tabbed pane" (See Requirement C74).

#	Title	Requirement
K19.	Industry Report Artifact Analysis	The Solution must have the functionality to perform Artifact Analysis against the applicable legislation when the ***Activity Reason Type*** value is any of "Industry Reports" values.
K20.	Industry Report Artifact Verification	The Solution must have the functionality to verify all industry report artifacts based on the applicable legislation and populate errors according to the legislated submission requirements when the ***Activity Reason Type*** value is any of "Industry Reports" values. For example: a. Identify information required in the submission but not provided (Brand Validation Check). b. Identify information missing in the submission but found in the Solution. c. Identify information found in the submission but missing in the Solution (Brand Validation Check). d. Identify information found in the submission but not recognized in a managed list, for example, CAS. e. Identify changes to tombstone data, such as company name and address. f. Incorrect unit of measures. g. Values outside of a range. h. Incorrect Totals. i. High Variance of measures compared to previous submission. j. Incorrect or misspelled terms (for example, chemicals, constituents, etc.).
K21.	Add Industry Report to Activity Artifact	The Solution must have the functionality to copy the industry report submission into the data collected for the activity artifact when the ***Activity Reason Type*** value is any of "Industry Reports" values.
K22.	Industry Report - Error Identification and Display Requirements	The Solution must have the functionality, when the ***Activity Reason Type*** value is any of "Industry Reports" values, to: a. identify errors and variances b. display the errors and variances error messages
K23.	Industry Report - View Consolidated Industry Report	The Solution must have the functionality for the User to view a consolidated industry report showing all the most up to date data cumulatively submitted at the time of the creation of the activity for an industry report of a given ***Report Section*** and ***Report Period*** values when the ***Activity Reason Type*** value is any of "Industry Reports" values.
K24.	Industry Report Version: Carry-Over of Errors	The Solution must have the functionality to display any uncorrected errors in the revised industry report that were identified in the previously submitted industry report of the same ***Report Period*** value in the Errors Grouped by Legislative Section/Subsection view (See Requirement C83) of the Compliance Assessment when the following conditions occur: a. the ***Activity Reason Type*** value is any of "Industry Reports" values b. the ***Report Version*** value is "Revision"
K25.	Industry Report History of Non-Compliances	The Solution must have the functionality to display the Non-Compliance History view (See Requirement C92) for the selected ***Legislative Section/ Subsection*** value in the Compliance Results field set of the Compliance Assessment component, when the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values. b. The User selects ***Non-Compliance History.***
K26.	Industry Report History of Non-Compliances-Overall	The Solution must have the functionality to display the Overall Non-Compliance History consolidated view of all the ***Legislative Sections/Subsection*** values with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance" for that ***Report Section*** value in the Compliance

#	Title	Requirement
		Results field set of the Compliance Assessment component when the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values. b. The User selects ***Overall Non-Compliance History*** consolidate view.
K27.	Artifact – Laboratory Shipment Component	The Solution must have the functionality for the User to enter, update, and view all information in the Shipping component of the Artifact "tabbed pane".
K28.	Responsible Party-Industry Reports	The Solution must have the functionality for the User to select a ***Full Name*** value from the list of contacts associated with the establishment profile as the ***Responsible Party*** value for the ***Legislative Sections/Subsection*** value of the industry report where non-compliance is indicated when the ***Activity Reason Type*** value is any of "Industry Reports" values.

L. Activity: Compliance Assessment – Test Shopper/Complete Assessment

#	Title	Requirement
L1.	Test Shopper	The Solution must have the functionality to require a minimum of one test shopper to be connected to an activity when the ***Activity Scope Plan Type*** is "Youth Access".
L2.	Test Shopper – Select	The Solution must have the functionality for the User to select an existing ***Test Shopper Name*** value(s) in the User's region/sub-region when the ***Activity Scope Plan Type*** value is "Youth Access".
L3.	Test Shopper -Indicate need to input new	The Solution must have the functionality to visually indicate the need to enter the test shopper details when the ***Activity Scope Plan Type*** is "Youth Access".
L4.	Test Shopper - create new	The Solution must have the functionality for the User to create a new ***Test Shopper Name*** value if the User cannot find the ***Test Shopper Name*** value in the search results list after performing a search for the ***Test Shopper Name*** value.
L5.	Activity Tabbed Pane-like Format: Compliance Assessment Component – Artifact Summary	The Solution must have the functionality to populate and display details of each added artifact in the Artifact Summary field set (See Requirement C75).
L6.	Artifact Summary - Update/View	The Solution must have the functionality for the User to select to update or view a previously documented artifact from the Artifacts Summary field set.
L7.	Artifact Viewing: Industry Report	The Solution must have the functionality to populate and display the industry report submission data in the Artifact Analysis component of the Artifact pane in a structured, readable, and viewable format.
L8.	Artifact Summary - Delete	The Solution must have the functionality for the User to select and delete a previously documented Artifact and all related artifact information from the Artifacts Summary field set.
L9.	Activity Tabbed Pane-like Format: Compliance Assessment Component – Responsible Party Summary	The Solution must have the functionality to populate and display details of each added responsible party in the Responsible Party Summary field set (See Requirements C75).
L10.	Responsible Party Summary - Update/View	The Solution must have the functionality for the User to select to update or view a previously documented Responsible Party from the Responsible Party Summary field set.
L11.	Responsible Party Summary - Delete	The Solution must have the functionality for the User to select and delete a previously documented Responsible Party and all related artifact information from the Responsible Party Summary field set.
L12.	Compliance Assessment - Confirm	The Solution must have the functionality to require the User to confirm that the information in the Compliance Assessment component is complete after the following conditions have been met: a. Each ***Legislative Section/Subsection*** value has a ***Legislation Section Compliance Outcome*** value indicated in the Compliance Result field set. b. For each artifact: i. All required artifact information has been completed. ii. An ***Overall Artifact Compliance Outcome*** value has been selected. iii. A minimum of one ***Contact Name*** has been selected as the Responsible Party for each ***Legislative Section/Subsection*** value with an ***Overall Artifact Compliance Outcome*** value of "Non-Compliance". c. Where the ***Activity Scope Plan Type*** value is "Youth Access": i. A minimum of one Test Shopper has been selected.

#	Title	Requirement
		ii. The transaction results, if the Transaction C***ompleted*** value is "Yes", has been documented.
L13.	Activity –-Confirmation - Non-Compliance Identified and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions: a. Set the following fields to the following values: i. Activity Status value to "Enforcement Action Plan Required" ii. Compliance Assessment Completion Date value to the system date value iii. Compliance Assessment Completion Time value to the system time value b. Set all fields to read-only. c. Enable for input and viewing the Enforcement Action component of the Activity "tabbed pane". When the information in the Compliance Assessment component is confirmed by the User, and successfully validated and verified as complete, and there is a ***Legislative Section/Subsection*** value with a ***Legislation Section Compliance Outcome*** value of one of the following: a. "Non-Compliance" b. "Non-Compliance – Minor" c. "Non-Compliance – Major"
L14.	Activity - Confirmation - No Non-Compliance Identified – No Enforcement Action Required and Enable Next Components in Workflow	The Solution must have the functionality to perform the following actions: a. Set the following fields to the following values: i. Activity Status value to "Pending Closure" ii. Compliance Assessment Completion Date value to the system date value iii. Compliance Assessment Completion Time value to the system time value b. Set previously confirmed fields to read-only. c. Enable for input and viewing the Link/Close component of the Activity "tabbed pane" When the information in the Compliance Assessment component is confirmed by the User, and successfully validated and verified as complete, and no ***Legislative Section/Subsection*** value has a ***Legislation Section Compliance Outcome*** value of any of the following: d. "Non-Compliance" e. "Non-Compliance – Minor" f. "Non-Compliance – Major"

M. Activity: Enforcement Actions

#	Title	Requirement
M1.	Enforcement Actions Component	The Solution must have the functionality for the User to enter, update, and view all data in the Enforcement Action component in the Activity "tabbed pane" (See Requirement C77) as follows: a. Data in the Recommended Enforcement Action field set. b. Data in the applicable enforcement action field sets for each ***Enforcement Action Type*** value selected in the Recommended Enforcement Action field set.
M2.	Enforcement Actions Workflow Steps	The Solution must have the functionality to move the User through the following workflow steps to document enforcement actions when the ***Activity Type*** value is "Inspection": a. Select the applicable ***Enforcement Action Type*** values for each ***Legislative Section/Subsection*** value. b. Complete the information for each selected ***Enforcement Action Type*** value. c. Confirm Enforcement Actions information is complete.
M3.	Recommended Enforcement Action	The Solution must have the functionality to display in the Recommended Enforcement Action field set all applicable ***Enforcement Action Type*** value(s) for each ***Legislative Section/Subsection*** value with a ***Legislation Section Compliance Outcome*** value of "Non-Compliance", when the ***Activity Type*** value is one of the following: a. "Inspection" b. "Investigation" c. "Internal Quality Assurance"
M4.	Industry Reports - Recommend Enforcement Action	The Solution must have the functionality to select the applicable default ***Enforcement Action Type*** value in the Recommended Enforcement Action field set for the Enforcement Action component when the ***Activity Reason Type*** value is any of "Industry Reports" values.
M5.	Industry Reports - Benchmark - Enforcement Action	The Solution must have the functionality for the User to use standard letter generation to generate Benchmark documents in the Enforcement Action component when the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values. b. The ***Enforcement Action Type*** value is "Benchmark". c. The ***Report Section*** value is "14(11)".
M6.	Enforcement Action Plan	The Solution must have the functionality for the User to select an ***Enforcement Action Type*** value for each responsible party and ***Legislative Section/Subsection*** value where non-compliance is indicated.
M7.	Industry Reports - Enforcement Action Override	The Solution must have the functionality to prompt the User to document a reason for the override when the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values b. The User has overridden the Solution recommended ***Enforcement Action Type*** value for a ***Legislative Section/Subsection*** value
M8.	Industry Report Audit - Differences in Enforcement Actions for two activities with the same report as the artifact	The Solution must have the functionality to visually indicate any differences between the Activity Enforcement Action Type values of the two industry report activities when the following conditions occur: a. One of the following Activity Reason Type values has been selected: i. Scheduled: Industry Report-Audit ii. Unscheduled: Industry Report-Audit iii. Internal Quality Assurance b. The User has selected an ***Activity Enforcement Action Type*** value for a ***Legislative Section/Subsection*** value, For example:

#	Title	Requirement
		a. Highlight the selected compliance assessment value if it differs from the compliance assessment value of the previous industry report b. Display (for example, a mouse-over) the original compliance assessment value
M9.	Industry Report - Audit - Enforcement Action Reason for Difference	The Solution must have the functionality to prompt the User to document a reason for the difference when the following conditions occur: a. ***Activity Reason Type*** value is any of "Industry Reports" values. b. The User selects an ***Activity Enforcement Action Type*** value that differs from the ***Activity Enforcement Action Type*** value of the previously closed activity.
M10.	Industry Reports - Stop Sale Brand Candidates	The Solution must have the functionality to: a. Identify Brand values with outstanding non-compliances where the Brand value has an error in at least two industry report activities where the ***Activity Compliance Outcome*** value is "Non-Compliance" for the same ***Establishment Name*** value of the same ***Report Section*** value submitted in the last two ***Report Period*** value***s.*** b. List the Brand values and associated ***Activity Id*** values as possible candidates for a stop sale designation. When the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values. b. The ***Enforcement Action Type*** value of "Stop Sale" is selected.
M11.	Industry Reports - Stop Sale Display Requirements	The Solution must have the functionality to: a. Prevent the User from selecting a ***Brand Name*** value for a stop sale designation (for example, the "Stop Sale" value is greyed out). b. Display the ***Activity Id*** value of the activity in which the ***Brand*** value was initially selected for stop sale designation. When the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values. b. When a ***Brand*** value has: i. Already been selected or approved for a stop sale designation in another activity. ii. Is identified as a possible candidate for a stop sale designation in the activity in which the User is working.
M12.	Industry Reports - Permit Approval for Stop Sale	The Solution must have the functionality for the User to approve a stop sale designation for selected ***Brand*** values within the enforcement action phase of the activity when the ***Activity Reason Type*** value is any of "Industry Reports" values.
M13.	Industry Reports - Stop Sale Designation Requirements	The Solution must have the functionality for the User to perform the following actions: a. Document the decision for the Stop Sale designation b. Document the links for letters related to the Stop Sale designation When the following conditions occur: a. The ***Activity Reason Type*** value is any of "Industry Reports" values b. The ***Enforcement Action Type*** value of "Stop Sale" is selected
M14.	Industry Report Versioning: Enforcement Action Component Unavailable Due to New Industry Report	The Solution must have the functionality to make unavailable the Enforcement Action component for the activity of the original industry report when the ***Activity Reason Type*** value is any of "Industry Reports" values and when the following conditions occur: ***a.*** An industry report activity for a given ***Report Section*** value and ***Report Period*** value has any of the following ***Activity Status*** values: i. "Pending Compliance" ii. "Compliance in Progress"

#	Title	Requirement
		iii. "Artifact Analysis in Progress" b. Another industry report is submitted with the same ***Report Section*** value and ***Report Period*** value and one of the following ***Report Version*** values: i. "Update-Addendum" ii. "Update-Replacement"
M15.	Industry Report Versioning: Enforcement Action Locked Down Due to New Industry Report	The Solution must have the functionality to prevent the User from entering data in the Enforcement Action component (lock it down) for the activity of the original industry report when the ***Activity Reason Type*** value is any of "Industry Reports" values and when the following conditions occur: a. An industry report activity for a given ***Report Section*** value and ***Report Period*** value has any of the following ***Activity Status*** values: i. "Pending Enforcement" ii. "Enforcement in Progress" b. Another industry report is submitted with the same ***Report Section*** value and ***Report Period*** value and one of the following ***Report Version*** values: i. "Update-Addendum" ii. "Update-Replacement"
M16.	Enforcement Comments	The Solution must have the functionality to append the data in the ***Comments*** field to the data in the ***Comments History*** field for each Enforcement Action in the General Information component.
M17.	Enforcement Action - Counts	The Solution must have the functionality to display the total count for each type of enforcement action, as well as each type of enforcement action applicable to the activity, (for example, 1 No Action, 3 Warning Letters), in the Enforcement Summary column of the following components: a. Work Load b. Establishment "tabbed pane": Activities c. Activity "tabbed pane": General Information – Other Activities for the Establishment
M18.	Information on Enforcement Action	The Solution must have the functionality for the User to enter, update, and view information for all enforcement actions and links connected to the enforcement action, as required for the activity, in its own field set within the Enforcement Action component.
M19.	Visually Differentiate Changes	The Solution must have the functionality to visually indicate any changes to an ***Enforcement Action Type*** value made by any User other than the User who initially selected the ***Enforcement Action Type*** value.
M20.	Industry Report: One Letter Generated for Multiple Activities	The Solution must have the functionality for the User to include ***Legislative Sections/Subsection*** value(s) from multiple activities where non-compliance is indicated into one letter when the ***Activity Reason Type*** value is any of "Industry Reports" values. In such cases, the information regarding the industry report can be selected by the User and imported into the letter.
M21.	Enforcement Action Validation	The Solution must have the functionality to ensure the following conditions have been completed for each ***Legislative Section/Subsection*** value where non-compliance is indicated before the Enforcement Action component can be confirmed as complete: a. A responsible party is assigned. b. An enforcement action is selected. c. The enforcement action is in a completed state.
M22.	Enforcement Action Confirmation	The Solution must have the functionality to perform the following actions: a. Set the ***Activity Status*** value to "Pending Closure". b. Set all the values in the Enforcement Action field set to read-only. When the information in the Enforcement Action component is: c. Confirmed by the User as complete.

#	Title	Requirement
		d. Successfully validated and verified as complete.

N. Activity: Close, or Link and Close

#	Title	Requirement
N1.	Activity - Tabbed Pane-like Format: Link/Close Component	The Solution must have the functionality for the User to enter, update, and view all data in the Link/Close component of the Activity "tabbed pane" at any time after the activity plan information in the General Information component has been confirmed as complete (See Requirement C77).
N2.	Activity Workflow Step: Close Activity	The Solution must have the functionality for the User to close an activity with no linked activity in the Link/Close component by performing the following workflow steps: a. Within the Recommended Next Steps field set: i. Select "No linked activity required at this time" as the value for Linked To ii. Select a value for Activity Close Reason iii. Select "Yes" as the value for Close Activity Now b. Within the Justification field set, provide a justification for closing the activity
N3.	Activity Workflow Step: Close with Linked Activity	The Solution must have the functionality for the User to close an activity with a linked activity in the Link/Close component by performing the following workflow steps: a. Within the Recommended Next Steps field set: i. Select the applicable Activity Type value for Linked To ii. Select a date value for the Proposed Start Date iii. Select a value for Activity Close Reason iv. Select "Yes" as the value for ***Close Activity Now*** b. Within the Justification field set, provide a justification for closing the activity
N4.	New Linked Activity	The Solution must have the functionality to: a. Create a new linked activity, populated with the following values, when the values in the originating activity are "Yes" for Has Linked Activity and "Closed" for the Activity Status value: i. Activity Type value to the Linked Activity Type value ii. Proposed Start Date value to the Linked Proposed Start Date value. iii. Activity Reason Type value to "Unscheduled: Linked Activity". iv. ***Activity Id*** value of the originating activity to the ***Linked from Activity Id*** value. v. ***Activity Scope Plan Type*** value will be locked and unchangeable from the originating activity for the following ***Activity Type*** values: 1. "Inspection" to "Inspection" with all ***Legislative Sections/Subsection*** value(s) selected by default 2. "Inspection" to "Investigation" with ***Legislative Sections/Subsection*** value(s) where non-compliance is indicated of the originating activity selected by default and locked 3. "Investigation" to "Investigation" with all ***Legislative Sections/Subsection*** value(s) where non-compliance is indicated of the originating activity selected by default and locked 4. "Investigation" to "Inspection" with all ***Legislative Sections/Subsection*** value(s) selected by default vi. ***Activity Scope Plan Type*** value will be unlocked and changeable from the originating activity for the following ***Activity Type*** values: 1. "Compliance Promotion" to "Inspection" 2. "Compliance Promotion" to "Investigation"

#	Title	Requirement
		vii. Activity Scope Plan Type value must contain all Legislative Sections/Subsection value(s) selected by default for Activity Type values of "Compliance Promotion" to "Compliance Promotion" b. Store the following information in the originating and linked activity Comments field: i. "Linked activity" ii. Linked Activity Id value iii. "Originating activity" iv. ***Originating Activity Id*** value v. The justification for creating a linked activity c. Add the new linked activity to the User's My Workload field set in the Workload Overview d. Never create a linked activity from an activity with ***Activity Scope Plan Type*** value of "CIP"
N5.	Industry Report - Request an Industry Report Creating an Open Linked Activity With Pre-Populated Industry Report Data	The Solution must have the functionality to: a. Create a linked activity populated with the following values when the Has Linked Activity value is "Yes" and the Activity Status value of the originating activity is "Closed": i. Activity Type value to the Linked Activity Type value. ii. Proposed Start Date value to the Linked Proposed Start Date value. iii. Proposed Start Date value to the Report Due Date value. iv. Activity Reason Type value to any of the following: 1. "Unscheduled: Industry Report" when the Activity Reason Type of the originating activity is either of the following values: (i) "Scheduled: Industry Report" (ii) "Unscheduled: Industry Report" 2. "Unscheduled: Industry Report-Audit" when the Activity Reason Type of the originating activity is either of the following values: (i) "Scheduled: Industry Report-Audit" (ii) "Unscheduled: Industry Report-Audit" v. Activity Id value of the originating activity to the Linked from Activity Id value. vi. Activity Scope Plan Type value will be unlocked and changeable from the originating activity. vii. Populate the activity with the following information of the expected industry report using the same values as the originating activity: 1. Report Section 2. Report Period 3. Report Type viii. Report Status value to "Not due" b. Store the following information in the originating and linked activity Comments field: i. "Linked activity" ii. Linked Activity Id value iii. "Originating activity" iv. ***Originating Activity Id*** value v. The justification for creating a linked activity c. Add the new linked activity to the User's My Workload field set in the Workload Overview When the ***Activity Reason Type*** value is any of the following: a. Any of "Industry Reports" values

#	Title	Requirement
		b. "Scheduled: Industry Report-Audit" c. "Unscheduled: Industry Report-Audit"
N6.	Activity - Bulk Close	The Solution must have the functionality for the User to select and close multiple activities at once.
N7.	Activity - Bulk Close	The Solution must have the functionality to ensure that the following criteria is met before an activity can be selected for the bulk activity close feature: a. Activity Type value is either of the following: i. "Inspection" ii. "Compliance Promotion" b. Activity Reason Type value is: "Scheduled: Workplan" c. Activity Status value is any of the following: i. "Pending" ii. "Planning in Progress" iii. "Pending Compliance" iv. "Pending Compliance Promotion" v. "Pending Closure" d. ***Has Linked Activity*** value is "No" e. ***Supervisor Approval Required*** value is "No" f. ***Supervisor Approval Required*** value is "Yes" and ***Supervisor Approval Granted*** value is "Yes"
N8.	Activity Complete	The Solution must have the functionality to require the User to confirm that the information in the activity is complete when the ***Close Activity Now*** value is "Yes".
N9.	Activity - Complete and Close	The Solution must have the functionality to perform the following actions in the specified order when the User confirms the information in the activity is complete: a. Set the ***Activity Completed*** value to "yes". b. Set the ***Activity Close Date*** value to the current system date value. c. Set the Act***ivity Status*** value to "Closed". d. Append the ***Activity Close Reason*** value and the ***Activity Close Justification*** value to the activity's ***Comments*** value. e. Set all the activity field values to read-only to prevent further updating to the closed activity. f. Add the closed activity to the "Activities No Longer Assigned to me" list in the User's workload view.
N10.	Benchmark-Closing Activity	The Solution must have the functionality to set the following legislated submission requirement values for each Band Name values approved benchmark activity: a. ***Report Section*** value to "14(11)" b. ***Brand Status*** value to "Exempted" c. ***Notification Start Date*** value to the ***Activity Close Date*** value d. ***Effective Date*** value to the ***Activity Close Date*** value When the ***Activity Reason Type*** value is any of "Industry Reports" values and when the following conditions occur: a. The User closes an industry report activity with a ***Report Section*** value of "14(11)" b. The ***Benchmark 14 15 Response*** value is either "Yes" or "Yes, But With Errors"
N11.	Close Referred Activity	The Solution must have the functionality for the User in the role of "Regional Supervisor" to close activities sent to them from a User with a ***Region/Sub-region*** value different from their own ***Region/Sub-region*** value without having to send the activity for action to the User in the role of "Regional Subordinate".

O. Send To

#	Title	Requirement
O1.	Send Activity to Another User	The Solution must have the functionality for the User to send an activity to another User for various reasons actions.
O2.	Sent To Component	The Solution must have the functionality for the User to enter, update, and view all data in the Sent To component of the Activity "tabbed pane".
O3.	Send to Supervisor	The Solution must have the functionality for the User with a ***Profile Level*** of "Subordinate" to send for action activity the User currently has control of, to either of the following in the User's region/sub-region: a. Any Supervisor b. Any Supervisor Group
O4.	Send to Subordinate	The Solution must have the functionality for the User with a ***Profile Level*** value of "Supervisor" to send a response to the User with a ***Profile Level*** value of "Subordinate" within their Subordinate Group with a decisio action as required.
O5.	Send to Supervisor	The Solution must have the functionality to send to the User's Supervisor group for approval any activity with ***Activity Reason Type*** value of "Unscheduled" that is created by the User with a ***Profile Level*** value of "Subordinate".
O6.	Send for Action	The Solution must have the functionality for the User with a ***Profile Level*** value of "Supervisor" to send activi for action to the User with a ***Profile Level*** value of "Subordinate" in the Supervisor's region/sub-region.
O7.	Send to Supervisor	The Solution must have the functionality for the User with a ***Profile Level*** value of "Supervisor" to send activi for action to any User with a ***Profile Level*** value of "Supervisor" and Supervisor group in any region/sub-regio
O8.	Assume Control of Activity	The Solution must have the functionality to perform the following actions when the User with a ***Profile Level*** v of "Supervisor" assumes control of any activity sent for action to their Supervisor group: a. Remove the activity from the Supervisor Group workload b. Add the activity to the Supervisor's workload
O9.	Activity Approval	The Solution must have the functionality to prevent the User with a ***Profile Role*** value of "Specialist" and Use ***Profile Level*** value of "Supervisor", who is acting in a ***Profile Role*** value of "Inspector" with the User ***Profile L*** value of "Subordinate", from approving their own activities requiring approval from a User with a ***Profile Leve*** value of "Supervisor".
O10.	Send To Action and Recipients	The Solution must have the functionality to display the following information in the Sent To component of the Activity "tabbed pane": a. The applicable ***Activity Send To Action*** values based on: i. The User's ***Profile Level*** value ii. The ***Profile Role*** value b. The list of potential ***Activity Send To*** recipients based on: i. The User's ***Profile Level*** value ii. The User's ***Profile Role*** value iii. The selected ***Activity Send To Action*** value
O11.	Workflow – Activity Sent To	The Solution must have the functionality to update the information in the Sent To History field set of the Gen Information component whenever an activity is sent to another User for action.
O12.	Activity Sent To History	The Solution must have the functionality to display, in a multi-column list view format in the Sent To History f set of the Sent To component, the following fields and values: a. ***Sent By*** value as the User's ***Name*** value b. ***Sent To*** value as the ***Activity Send To*** value c. ***Sent Date*** value as the activity ***Date Created*** and time values for initial entry, and ***the system date*** and t values for subsequent entries d. ***Action and Reason*** value (***Activity Send To Action*** value + ***Activity Send To Reason*** value)
O13.	Sent To Comment History	The Solution must have the functionality to append the ***Sent To Comments*** to the Sent To Comments Histor field set of the Sent To component.
O14.	Update Sent To History	The Solution must have the functionality to update the following information in the Sent To History field set o General Information component whenever a "Sent To" action is performed on an activity (that is send to, approve, assume control of, etc.): a. ***Sent By*** value as the User's ***Name*** value b. ***Sent To*** value as the ***Activity Send To*** value

#	Title	Requirement
		c. ***Sent Date*** value as the system date value and time d. ***Action and Reason*** value (***Activity Send To Action*** value + ***Activity Send To Reason*** value)

P. Complaints, Enquiries, and Support Request

#	Title	Requirement
P1.	Complaint/Enquiry /Support Request: New	The Solution must have the functionality to create any of the following records: a. A Complaint. b. An Enquiry. c. A Support Request.
P2.	Workflow: Complaint	The Solution must have the functionality for the User to be moved through the following default workflow to create a Complaint record: a. Initialization of a Complaint. b. Enter Complaint information details. c. Provide a Recommended Action. d. Option to create an activity linked to the complaint. e. Option to send the complaint to another User. f. Close.
P3.	Complaint: Recommended Action	The Solution must have the functionality for the User to create an activity linked to the Complaint when the ***Recommended Action*** value for a Complaint is any of the following: a. Inspection b. Refer to Other Authority c. Compliance Promotion
P4.	Complaint: Linked Activity Type	The Solution must have the functionality to set the ***Activity Type*** value in the new linked activity to the ***Recommended Action*** value when the User creates an activity linked to a Complaint.
P5.	Complaint: Linked Activities	The Solution must have the functionality to display the linked activities in a multi-column list view format in the Linked Activities field set of the Complaint/Request component, when linked activities exist for previous complaints related to the same Alleged Offender.
P6.	Complaint: Completed	The Solution must have the functionality to set the Complaint field values to read-only, when the ***Complaint Status*** value is set to "Completed".
P7.	Complaint: Update	The Solution must have the functionality to update an existing Complaint record.
P8.	Complaint from External User	The Solution must have the functionality to perform the following actions when the Complaint is created by an External User: a. Set the ***Complaint Status*** value to "Open" b. Set the ***Recommended Action*** value to "To Be Determined" c. Set the ***Date Received*** value to the date the Complaint was entered d. Send the complaint to the Regional Supervisor group for action.
P9.	Workflow: Enquiry	The Solution must have the functionality to move the User through the following default workflow to create an Enquiry record: a. Initialization of an Enquiry b. Enter Enquiry details c. Provide a Recommended Action

#	Title	Requirement
		d. Option to create an activity linked to the Enquiry e. Option to send the Enquiry to another User f. Close
P10.	Enquiry: Recommended Action	The Solution must have the functionality for the User to create an activity linked to the Enquiry when the ***Recommended Action*** value for an Enquiry is any of the following: a. Inspection b. Refer to Other Authority c. Compliance Promotion
P11.	Enquiry: Linked Activity Type	The Solution must have the functionality to set the ***Activity Type*** value in the new linked activity to the ***Recommended Action*** value when the User creates of an activity linked to an Enquiry.
P12.	Enquiry: Linked Activities	The Solution must have the functionality to display the linked activities in a multi-column list view format in the Linked Activities field set of the Complaint/Enquiry component, where linked activities exist for previous Enquiries related to the same person requesting the information.
P13.	Enquiry: Completed	The Solution must have the functionality to set the Enquiry field values to read-only when the ***Enquiry Status*** value is set to "Completed".
P14.	Enquiry: Update	The Solution must have the functionality to update an existing Enquiry record.
P15.	Enquiry from External User	The Solution must have the functionality where the Enquiry is created by an External User to: a. Set the ***Enquiry Status*** value to "Open" b. Set the ***Recommended Action*** value to "To Be Determined" c. Set the ***Date Received*** value to the date the Enquiry was entered. d. Send the Enquiry to the Supervisor group for action.
P16.	Support Request: New	The Solution must have the functionality for the User to create and submit the Support Request to the Solution via either of the following: a. An external public facing interface b. Within the Solution
P17.	Workflow: Support Request	The Solution must have the functionality to move the User through the following default workflow to create a Support Request record: a. Initialization of an Support Request b. Enter Support Request details including selection the applicable issue category c. Submit the support request.
P18.	Support Request: Closed	The Solution must have the functionality to set the Support Request field values to read-only when the ***Support Request Status*** is set to "Closed".
P19.	Support Request: Update	The Solution must have the functionality for the User to update an existing Support Request record. For example: a. Document the Actions Taken and Date of Action b. Update the Support Request Issue Category as required c. Set the ***Support Request Status*** to "Closed"
P20.	Support Request from External User	The Solution must have the functionality, when the Support Request is created by an External User, to: a. Set the Support Request ***Status*** value to "Open". b. Set the ***Recommended Action*** value to "To Be Determined". c. Set the ***Date Received*** value to the date the Support Request was entered. d. Send the Support Request to the Solution Administrator for action.

Q. Electronic Data Submission

#	Title	Requirement
Q1.	Portal and API-Based Submissions	The Solution must have the functionality to capture and process electronically submitted data via the following methods: a. Guided form-based submissions via a portal b. API-based electronic data submissions.
Q2.	Electronic Submission of Data	The Solution must have the functionality for the following External Users to electronically submit data: a. Industry to electronically submit structured industry report data in a prescribed form and manner for each legislated type of industry data. b. Third parties (for example, laboratories) to electronically submit data, for example laboratory analysis results reports c. Third parties (that is, the general public) to electronically submit information, for example Complaints.
Q3.	Industry Report Submission – Internal User Guided Form Submission	The Solution must have the functionality for the User to perform a manual data entry of an industry report for a selected establishment using the same guided form-based submission process used by External Users.
Q4.	Industry Report Submission – Guided Form Submission Pre-populate Data or Paste Data	The Solution must have the functionality for the User to do the following in the Guided form-based submission: a. Select the option to have the guided form pre-populated with data stored in the Solution. For example, if a guided form asks for brand information such as Brand Name and Unit of Measure that is stored in the Solution, the User has the option to have those fields populated with the data. b. Copy and Paste data into the guided form. For example, if the guided form asks for ingredients, the Solution must permit the User to copy and paste the ingredients into that guided form. c. Enter data into the fields via the keyboard.
Q5.	Update Industry Report Submission Interface	The Solution must have the functionality to update values in the Industry Report Submission Interface based on events occurring in the Solution in real time.
Q6.	Update Views: Absent-Grace Period	The Solution must have the functionality to perform the following actions when an expected industry report, based on the submission frequency or based on a request from Health Canada, has not been received prior to or on the due date but the ***Grace Period*** has not expired: a. set the ***Report Status*** value for the required industry report to "Absent-Grace Period" b. add the industry report to the ***Designated User***'s Anticipated Workload Overview Display c. update the ***Submission Display Status*** to "Overdue" in the Home component of the Industry Report Submission Interface d. update the Industry Report Submission Interface by adding the industry report to the Overdue Reports View
Q7.	Update Views: Registered Industry Report Past Due Date	The Solution must have the functionality to perform the following actions when an expected industry report, based on the submission frequency or based on a request from Health Canada, has been received after the due date but the ***Grace Period*** has not expired: a. create an activity for the establishment associated with the industry report with ***Activity Type*** value of "Inspection" and ***Activity Reason Type*** value of "Scheduled: Industry Report" b. add the industry report data as the artifact c. set the ***Report Status*** value to "Registered" in the General Information component of the Activity "tabbed pane" d. set the ***Submission Timing Status*** value to "Post-submission date" in the General Information component of the Activity "tabbed pane"

#	Title	Requirement
		e. add activity to the ***Designated User***'s workload f. update the ***Submission Display Status*** to "Submitted-Late" in the Home component of the Industry Report Submission Interface g. update the Industry Report Submission Interface by: i. Adding the industry report to the Industry Reporting History View ii. Removing the industry report from the Overdue Reports View
Q8.	Update Views: Registered	The Solution must have the functionality to perform the following actions when an expected industry report, based on the submission frequency, has been received prior to or on the due date: a. Set the ***Report Status*** value to "Registered" and display it in the General Information component of the Activity "tabbed pane" b. Add the industry report data as the artifact c. Set the ***Submission Timing Status*** value to "Prior to or on the submission date" and display it in the General Information component of the Activity "tabbed pane" d. Set the ***Submission Display Status*** value to "Submitted" in the Home component of the Industry Report Submission Interface e. Update the Industry Report Submission Interface by adding the industry report to the Industry Reporting History View
Q9.	Update Submit Industry Reports View: Absent - Action Required	The Solution must have the functionality to perform the following actions when an expected industry report, based on the submission frequency, has been received prior to or on the due date and the ***Report Status*** value for the required industry report is "Absent-Grace Period": a. Update the ***Submission Display Status*** value to "Overdue" in the Home component Industry Report Submission Interface b. Update the Industry Report Submission Interface by adding the industry report to the Industry Reporting History View
Q10.	Submit Industry Reports: Supplier Account Manufacturer Selection	The Solution must have the functionality, when a ***Supplier User*** submits industry report data via Reports component of the Industry Report Submission Interface, to: a. Permit the ***Supplier User*** to select the name of the Manufacturer-Importer on behalf of which the industry report data is being submitted b. Limit the list of Manufacturer-Importer values to those who have authorized the ***Supplier User*** to submit on their behalf
Q11.	Industry Reporting History View	The Solution must have the functionality for the User to view and search in the Industry Reporting History view for previously submitted industry reports.
Q12.	Submit Industry Reports View	The Solution must have the functionality for the User to do the following in the Reports component: a. View, search and update industry reports that are saved in progress b. View confirmation that industry reports have been submitted by the supplier and awaiting confirmation by the manufacturer to submit the complete industry report c. View confirmation that industry reports have been submitted by the ***Delegated User*** on behalf of the ***Primary User*** d. View and search a summary of industry reports where the ***Submission Display Status*** value is "Overdue" or "Due Soon" e. Submit a new industry report
Q13.	Industry Report Update/View Screen of Tombstone Information	The Solution must have the following functionality when the User initiates the guided form-based submission process in the Industry Report Submission Interface for any industry report: a. To provide an update/view screen of the fields reflecting mandatory tombstone information as stipulated by S.3 (2) and S.3 (3) of the TRR pre-populated with the Establishment Profile information stored in the Solution. b. For the User to update and confirm the tombstone information.
Q14.	Product/Brand	The Solution must have the functionality to capture identical product sold under different brand names (as reference brand) for each of the following ***Report Sections:*** a. "10"

#	Title	Requirement
		b. "12" c. "14" d. "14.1" e. "14.2"
Q15.	Industry Report Submission Interface - Update Previously Saved Fields	The Solution must have the functionality for the User to update any previously saved data in the guided form associated with that industry report, when an industry report submission has not been completed but saved in progress.
Q16.	Industry Report Submission - Save	The Solution must have the functionality for the User to save a copy of the submitted data, when an industry report has been successfully submitted.
Q17.	Industry Report Version - Original	The Solution must have the functionality to set the ***Report Version*** value to "Original" of the industry report when a ***Report Status*** value is set to "Registered" for a given ***Report Section*** and ***Report Period (if applicable)*** values where no industry report has been previously submitted***.***
Q18.	Industry Report Version: Revision	The Solution must have the functionality to perform the following actions when the User attempts to submit an industry report that has been requested by Health Canada for the Report Section and Report Period values entered: a. Notify the User that the data submitted will be considered part of the revised industry report data requested by Health Canada b. Provide the User the option to: i. Proceed with the submission ii. Save the industry report in progress iii. Cancel the submission
Q19.	Industry Report Version: Update - Revision	The Solution must have the functionality to set the ***Report Version*** value to "Update-Revision" when all the following conditions are met: a. An industry report has been submitted and its ***Report Status*** value has been successfully set to "Registered" in response to a request for revision by Health Canada for the ***Report Section*** and ***Report Period*** values provided. b. An industry report has previously been submitted for the same ***Report Section*** and ***Report Period*** values. c. Values have been revised only. Example: Event 1: ***Report Section 11*** was submitted originally with the following information: a. ***Report Period*** value is "20190101-20191231". b. ***Brand*** value is "Smoky". c. ***Ingredient Chemical Name*** value is "triacetin". d. ***Amount*** value is "5". Event 2: ***Report Section 11*** was later submitted with a change to the following information: a. ***Report Period*** value is "20190101-20191231". b. ***Brand*** value is "Smoky". c. ***Ingredient Chemical Name*** value is "triacetin". d. ***Amount*** value is "7". Expected Result: Since this is an update to existing values only and not an addition of new values, the Solution must have the functionality to set the ***Report Version*** value to "Update-Revision".

#	Title	Requirement
Q20.	Industry Report Version: Update - Addendum	The Solution must have the functionality to set the ***Report Version*** value to "Update-Addendum" when all the following conditions are met: a. An industry report has been submitted and its ***Report Status*** value has been successfully set to "Registered". b. An industry report has previously been submitted for the same ***Report Section*** and ***Report Period*** values. c. the Solution has identified new data only. Example: Event 1 ***Report Section 11*** was submitted and "Registered" previously with the following information: ***a. Report Period*** value is ***"20190101-20191231".*** ***b. Brand*** value is ***"Smoky".*** ***c. Ingredient Chemical Name*** value is ***"triacetin".*** d. ***Amount*** value is "5". Event 2 second ***Report Section 11*** was later submitted and "Registered" with the addition of the following information: a. ***Report Period*** value is "20190101-20191231". b. ***Brand*** value is ***"***Smoky". c. ***Ingredient Chemical Name*** value is ***"***glycerol". d. ***Amount*** value is "20". Expected Result: Since a new ingredient, "glycerol", was added to the brand "Smoky" the Solution must have the functionality to set the ***Report Version*** value to "Update-Addendum".
Q21.	Industry Report Version: Update - Revision and Addendum	The Solution must have the functionality to set the ***Report Version*** value to "Update-Revision and Addendum" when all the following conditions are met: a. An industry report has been submitted and its ***Report Status*** value has been successfully set to "Registered" in response to a request for revision by Health Canada for the ***Report Section*** and ***Report Period*** values provided b. New data has been added that was not in the previous industry report and existing values have been revised Example: Event 1: ***Report Section 11*** was submitted originally with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is "Smoky" c. ***Ingredient Chemical Name*** value is "triacetin" d. ***Amount*** value is "5". Event 2: ***Report Section 11*** was later submitted in response to a request for revision by Health Canada with the following information: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is "Smoky" c. ***Ingredient Chemical Name*** value is "triacetin" d. ***Amount*** value is "7". and the following new data was not in the previous industry report: a. ***Report Period*** value is "20190101-20191231" b. ***Brand*** value is ***"***Smoky" c. ***Ingredient Chemical Name*** value is ***"***glycerol" d. ***Amount*** value is "20".

#	Title	Requirement
		Expected Result: Since the ***Amount*** value for "triacetin" changed from "5" to "7" and a new ingredient "glycerol" was added to the ***Brand*** "Smoky" the Solution must have the functionality to set the ***Report Version*** value to "Update-Revision and Addendum".
Q22.	Industry Report Version: Update -Replacement	The Solution must have the functionality to set the ***Report Version*** value to "Update-Replacement" when all the following conditions are met: a. An industry report has been submitted and its ***Report Status*** value has been successfully set to "Registered" b. An industry report was previously submitted for the same ***Report Section*** and ***Report Period*** values c. Values in the industry report have been revised
Q23.	Identification of Duplicate Industry Report	The Solution must have the functionality to: a. Set the ***Report Version*** value to "Duplication" b. Notify the ***Designated User*** that all industry report data is a duplicate of the previously submitted industry report c. Recommend closing the associated activity with no action required When all the following conditions are met: a. An industry report has been submitted and its ***Report Status*** value has been successfully set to "Registered" b. An industry report was previously submitted for the same ***Report Section*** and ***Report Period*** values c. All values in the industry report were identified as duplicates of those in the previously submitted industry report
Q24.	Industry Report Submission Interface - Brand Validation Error Display	The Solution must have the functionality to: a. Identify and display to the User the following errors and messages as applicable: i. Brand name(s) not found in the Solution ii. Required Brand name(s) currently in the Solution but missing from the industry report b. Permit the User to do the following: i. Correct the identified errors as applicable ii. Proceed with submitting the industry report iii. Save the industry report iv. Cancel the submission Before the following ***Report Sections***, including partial industry reports, can be submitted via the Industry Report Submission Interface: a. "10" b. "11" c. "12" d. "13" e. "14" f. "14.1" g. "14.2" h. "20"
Q25.	Portal-Submission Validation - Exemption Restriction	The Solution must have the functionality to: a. Verify if the brand is not required according to the legislated submission requirements for the relevant section before an industry report, including partial industry reports, can be submitted via the Industry Report Submission Interface that is any of the following Report Sections values: i. "10" ii. "11" iii. "12" iv. "13"

#	Title	Requirement
		v. "14" vi. "14.1" vii. "14.2" viii. "20" b. Exclude the brand from the displayed list of identified missing brands, if the brand is not required c. Not display the message that brands are missing if all brands missing are exempted.
Q26.	Submission Validation - establishment	The Solution must have the functionality, when an industry report is submitted, to identify and display the following errors that comprise the Establishment Error Display: a. Establishment information (for example ***Establishment Name***) not found in the Solution b. Establishment information currently in the Solution but missing from the industry report.
Q27.	Report Not Processed-API Submission-Unidentified Establishment	The Solution must have the functionality to: a. Not create an industry report activity b. Store the submission in the Solution with the following fields populated: i. Submission Confirmation Id value is [null] ii. Submitted By value is [name of the User] iii. Submission Date value is [system date] iv. ***Submission Processed*** value is [No] When the following conditions occur: a. An industry report has been submitted via the API based submission process. b. Validation of establishment information fails, that is, the establishment information does not match any of establishment profile stored in the Solution.
Q28.	Report Not Processed-API Submission-Unidentified Submission	The Solution must have the functionality to: a. Not create an industry report activity. b. Store the submission in the Solution with the following fields populated: i. Submission Confirmation Id value is [null] ii. Submitted By value is [name of the User] iii. Submission Date value is [system date] iv. ***Submission Processed*** value is [No] When the following conditions occur: a. An industry report has been submitted via the API based submission process. b. Either one of the following occurs: i. The ***Report Section*** value in the submission is not recognized. ii. The submitted data does not match any of the data structure of the ***Report Sections***. For example, the XML submitted data does not match any of the schemas of the ***Report Sections***.
Q29.	Partial Industry Reports Manufacturer	The Solution must have the functionality to prevent the Manufacturer from submitting their industry report until all the reports has been received from delegated suppliers, when a manufacturer delegates the responsibility for submitting an industry report to suppliers.
Q30.	Partial Industry Report Submission By Suppliers	The Solution must have the functionality to perform the following actions when a partial industry report is submitted by a supplier on behalf of the manufacturer: a. Store the partial industry report. b. Indicate to the manufacturer, in the Submit Industry Reports View field set of the Industry Report Submission Interface, that the partial industry report has been received from the supplier,
Q31.	Manufacturer Submits Industry Report Composed of Supplier Submissions	The Solution must have the functionality for a manufacturer who has delegated suppliers to submit their industry report along with all the partial industry reports received from their delegated suppliers.

#	Title	Requirement
Q32.	Industry Report Submission - Verification Criteria Report Error Display Message-Brand Submitted	The Solution must have the functionality to perform the following actions, when a brand already stored in the Solution is submitted that the manufacturer or supplier is not required to submit: a. Display an alert showing the name of the brand. b. Provide the option to proceed with the submission. c. Prompt the User to confirm before continuing.
Q33.	Partial Industry Report Submission - Verification Criteria Report Error Display Message Missing Brand	The Solution must have the functionality to perform the following actions, when a brand already stored in the Solution is not submitted that the manufacturer and supplier is required to submit. a. Display an alert indicating that the brand is missing in the industry report. b. Provide information on the consequence of not reporting the brand. c. Prompt the User to confirm before continuing.
Q34.	Data Capture Product/New Brand Via Submission of Required Industry Reports	The Solution must have the functionality to update the brand information fields in the Product and Brands component of the Establishment "tabbed pane" for any brand submitted in the industry report when either of the following occurred: a. The brand does not exist in the Solution. b. The brand exists in the Solution and there is a change in it's information.
Q35.	Product/New Brand Converted to "Active"	The Solution must have the functionality to set the ***Brand Status*** value to "Active" when a brand is submitted in an industry report whose: a. ***Report Section*** value is "Section 13-Report on Sales of Consumer Tobacco Products" b. The ***Total Sales CAD*** value is greater than "0" c. Has been previously reported in both of the following industry reports: i. ***Section 10-Manufacturing Processes*** ii. S***ection 11-Ingredients*** (with no ***Report Period***)
Q36.	Product/New Brand Converted to "Inactive"	The Solution must have the functionality to set the ***Brand Status*** value to "Inactive" when a brand has one of the following ***Brand Status*** values: a. "Active" b. "Pending" And either of the following conditions have occurred: a. For a calendar year, the industry reports whose ***Report Section Name*** value is "Section 13-Report on Sales of Consumer Tobacco Products" have had ***Total Sales CAD*** values less than or equal to "0" b. For a calendar year, the industry reports whose ***Report Section Name*** value is "Section 13-Report on Sales of Consumer Tobacco Products" have not reported the brand
Q37.	Display Requested Industry Report in Submit Industry Reports View	The Solution must have the functionality to: a. Display the requested industry report information in the Submit Industry Reports View in the Industry Report Submission Interface b. Set the ***Submission Display Status*** value to "Due Soon", When a linked activity is created with any of the following ***Activity Reason Type*** values: a. "Any of Industry Reports" b. "Scheduled: Industry Report-Audit" c. "Unscheduled: Industry Report-Audit"
Q38.	Electronic Data Exchange Component -	The Solution must have the functionality to notify the User that the session is timing out while the User is completing information for submission.

#	Title	Requirement
	Session Persistence	
Q39.	Product/New Brand Converted to "Pending"	The Solution must have the functionality to perform the following actions when a brand is submitted in an industry report and does not exist in the Solution: a. Add the brand information to the Solution. b. Set the Brand Status value to "Pending".
Q40.	Update Industry Reporting History Component in the Establishment	The Solution must have the functionality to update the Industry Reporting History component of the Establishment "tabbed pane" with the industry report information when an industry report has been submitted.

R. Reporting Specifications

#	Title	Requirement
R1.	Pre-defined Reports	The Solution must have the functionality for the User to design pre-defined reports with user-selectable criteria.
R2.	Pre-defined Reports with User-selectable Constraints	The Solution must have the functionality for Users to generate a pre-defined report based on user-selectable constraints to limit the number of report results. For example, the User can select the following values to obtain a report of all establishments in Ottawa with a status value of "Active": a. ***Establishment Status*** value of ***"***Active***"*** b. ***Region*** value of ***"***East***"*** c. ***City*** value of "Ottawa"
R3.	Save, Retrieve, and Delete Pre-defined Reports	The Solution must have the functionality for the User to perform the following actions: a. Save the designed pre-defined report. b. Update the designed pre-defined report. c. Retrieve a previously designed saved pre-defined report. d. Delete a previously designed saved pre-defined report.
R4.	Generate Documents from Templates	The Solution must have the functionality for the User to generate documents based on templates.
R5.	Standard Letter Generation from a Template: Warning Letter	The Solution must have the functionality to populate the information in a letter template to generate a letter. For example, when the User selects "Warning Letter" as the ***Enforcement Action Type*** value, the Solution must perform the following actions to generate a Warning Letter: a. Use fields, with the applicable options, that can be selected and pre-populated. For example: i. Name, Address, and contact information of the regulated party ii. ***Legislative Sections/Subsection*** values associated with the non-compliance b. Use applicable standard text. For example: i. text informing the regulated party there are non-compliances ii. text outlining the time given to correct the non-compliances and the consequences of not correcting the non-compliances
R6.	Save Documents Generated from Templates	The Solution must have the functionality for the User to perform the following actions on documents generated from templates: a. Save the generated document to the HC approved repository. b. Provide a link to the generated document.

S. Business Intelligence and Data Analytics Specifications

#	Title	Requirement
S1.	Extract, Transform, and Load (ETL)	The Solution must have the functionality for the Solution data to be accessible by Extract, Transform, and Load (ETL) tools. For example, Informatica tool.
S2.	Real-Time Solution Data Access	The Solution must have the functionality to provide direct access to the real-time Solution data for business intelligence and analytics purposes via either of the following methods: a. A business intelligence tool as part of the Solution. b. Integration with a business intelligence tool provided by Canada.

T. Off-Line Capacity

#	Title	Requirement
T1.	Off-line Capacity	The Solution must have the functionality for the User to access and work with the Solution in an off-line capacity that has the equivalent functionality as the online Solution, as follows: a. Access to the compliance and enforcement components of the Solution, including establishment information. b. Off-line creation of establishment profile. c. Off-line creation of activities.
T2.	Off-line Solution	The Solution must have the functionality to provide the latest version of the off-line Solution executable for download by the User as needed, if the off-line capacity is provided by a standalone Solution.
T3.	Off-line Solution: Synchronized Data Transfer Function	The Solution must have the functionality to provide a synchronized data transfer from the Online Solution to the Off-line Solution and vice versa, if the off-line capacity is provided by a standalone Solution.
T4.	Off-line Solution: Data Transfer to Off-line Solution - Unsuccessful	The Solution must have the functionality to perform the following actions: a. Leave the ***Activity Status*** value unchanged in the online Solution; that is, the value remains as "Pending Compliance". b. Delete from the off-line Solution any transferred data associated with the unsuccessful transfer, When the following conditions occur: a. Off-line capacity is provided by an Off-line Solution b. The data transfer to the Off-line Solution was unsuccessful
T5.	Off-line Solution: Data Transfer to Online - Unsuccessful	The Solution must have the functionality to perform the following actions: a. Leave the ***Activity Status*** value unchanged in the online Solution; that is, the value remains as "Off-line", and the ***Activity Status*** value remains unchanged in the Off-line Solution. b. Leave all data within an unsuccessfully transferred activity in the off-line Solution. c. Roll back values associated with the failed transfer to their value prior to the attempted transfer. d. Provide the User with the option to unlock the activity in the online Solution if the transfer error or problem cannot be corrected, When the following conditions occur: a. Off-line capacity is provided by an Off-line Solution b. The data transfer to the Off-line Solution was unsuccessful
T6.	Off-line Solution: Data Transfer to Online - Successful	The Solution must have the functionality to perform the following actions: a. Transfer the selected activity and associated establishment data from the off-line Solution to the online Solution. b. Prevent the off-line Solution from updating data in the online Solution that cannot be updated. c. Once the data has been transferred to the online Solution set the A***ctivity Status*** value in the online Solution to "Compliance in Progress". d. Delete all off-line information from the off-line Solution that has been successfully transferred to the online Solution, When the following conditions occur: a. Off-line capacity is provided by an Off-line Solution b. The data transfer to the On-line Solution was successful

U. User and Application Management

#	Title	Requirement
U1.	User Management: User Account Administration: User Profile - create, update, view	The Solution must have the functionality for the User to perform User account administration tasks including the following: a. Create or update a User profile b. Create User roles and assign privileges to each role c. Assign rights and roles to a User profile d. Associate a User profile with an establishment as required e. Set a ***User Status*** value to "Inactive" if the User Id is associated with an activity or establishment, as required f. Delete a User profile if the User Id is not associated with an activity or establishment g. View the field values for a User profile h. Assign a User to a User Group i. Create User Groups (for example the Regional User Group must contain all regional supervisors and subordinates)
U2.	Self-Management of User Preferences	The Solution must have the functionality for the User (external/internal) to set their User profile preferences.
U3.	User Management: Password Reset	The Solution must have the functionality for the User to reset their password.
U4.	User Management: Username Retrieval	The Solution must have the functionality for the User to retrieve their Username when requested.
U5.	User Management: Primary User Management	The Solution must have the functionality for the User to access the User Profile fields to perform the following actions: a. Update their ***Primary User*** account. b. Update their ***Delegated User*** account information. c. Update their ***Supplier User*** account information.
U6.	User Management	The Solution must have the functionality for the User to access the User Profile fields to update their User account.
U7.	User Management: Profile and User Management: Supplier Account Selection by Primary Account	The Solution must have the functionality for the User to perform the following from their Primary User account: a. Select the Supplier User from a list of available Supplier User accounts to provide permission to submit data on behalf of the User. b. Specify the industry report information that the Supplier User must submit on behalf of the User based on the values of the following fields: i. Report Section ii. Report Section Name iii. Brands required for the specified Report Section
U8.	User Management: Profile and User Management: Delegated User Account Selection by Primary Account	The Solution must have the functionality for the User to perform the following from their ***Primary User*** account: a. Select the "Delegated User" from a list of available "Delegated User" accounts to provide permission to submit data on behalf of the User. b. Specify the industry report information that the "Delegated User" must submit on behalf of the User based on the values of the following fields: i. ***Report Section*** ii. ***Report Section Name***
U9.	User Management: Role for Specialists	The Solution must have the functionality for the User with ***Profile Level*** value of "Specialist" to act as a "Supervisor" or as a "Subordinate", but must not permit the User to act as both for the same activity.

#	Title	Requirement
U10.	User Administration: Re-activate User Accounts	The Solution must have the functionality to re-activated inactive User accounts as required. Note: Inactivation of a User account affects only log in privileges and does not affect existing Solution data.
U11.	Configuration and Application Administration: Solution Parameters	The Solution must have the functionality for the User to configure and manage Solution parameter values including: a. Content of data validation and pick-list tables b. User account and User profile information c. Templates and Data Entry forms d. Notification and Alerts: i. Triggered and event driven ii. Compose and send ad-hoc notifications, for example, for Solution shut down for maintenance e. Workload Overview Displays. For example: a. New validation calculations to reflect changes in policy and legislation for example: i. Update to CIP analysis for # of full length burns ii. Update to TLPR analysis for available package types b. Manage the Scope ***Legislative Sections/Subsection*** parameter values and Enforcement Action values requiring Supervisor approval. c. Configure the type of variances for comparing values in industry report fields between ***Report Periods*** d. Set parameter values as active/inactive e. Add and update parameter values (no logic changes), for example: i. For each activity type: 1. Manage the ***Legislative Sections/Subsection*** parameter values 2. Manage the Enforcement Action parameter values (action, effective date, end date) ii. Set or update the ***Grace Period*** value for each ***Report Section*** (for example, 30 days after the due date)
U12.	List Sort Order	The Solution must have the functionality for the User to specify the sort order of a list rather than using the standard sort order parameters. For example: a. For a list of string values such as High, Medium, and Low, the User specifies the sort order so that the list is sorted in the following order: i. "High" ii. "Medium" iii. "Low" b. For a list of string values such as months of the year, the User specifies the sort order so that the list is sorted according to the actual logical sequence of the months rather than alphabetical: i. January ii. February iii. March iv. April
U13.	Automatic Solution Alert configuration	The Solution must have the functionality for User to update the message for automatic (Solution initiated, event driven) alerts.

#	Title	Requirement
		For example, the User updates the message for an alert that lets a User know that a business process workflow step has not been completed when the User attempts to proceed to the next business process workflow step.
U14.	Application Administration: Add, update, delete data	The Solution must have the functionality for the User to add, update, and/or delete any data entered into the Solution by any registered User.
U15.	Application Administration: Lock unlock data	The Solution must have the functionality for the User to unlock the precondition step in a workflow to permit the User to continue adding data in the precondition step until the User re-initiates the lock.
U16.	Application Administration: Reset Status of Activity	The Solution must have the functionality for the User (for example, the Solution Administrator) to reset a closed activity to its last state before it was closed.
U17.	Application Administration: Delete Establishment Profile	The Solution must have the functionality for the User to delete an establishment profile if there are no associated activities with the establishment.
U18.	Application Administration: Delete Activity	The Solution must have the functionality for the User to delete an activity if the Activity Status value is "Pending".
U19.	Configure Filename Format of Letters of Absence/Deficiency/Stop Sale	The Solution must have the functionality for the User to configure the filename format for the following documents as needed: a. Letter of Deficiency b. Letter of Absence c. Stop Sale Letter.
U20.	User Notification Subscription Management	The Solution must have the functionality for the User to manage their User notification subscription (scheduled and event driven). For example, the User selects to receive email notifications weekly showing the number open activities in their workload.
U21.	Notification Via Email Management	The Solution must have the functionality for the User to set their preferred notification frequency for each type of Solution-generated Email notification (only one email notification frequency for each Solution-generated email notification type).
U22.	Notification Via Internal Notification Management	The Solution must have the functionality for the User to set their preferred notification frequency for each type of Solution-generated internal notification***.***
U23.	User Preferences For Alerts	The Solution must have the functionality for the User to set their preference to show/hide Solution alerts. For example, for loss of unsaved data.
U24.	User Profile Management	The Solution must have the functionality for the User to update the following fields in their User profile: a. ***Full Name*** b. ***Profile Region*** c. ***Profile Sub-region*** d. ***Profile Province/Territory*** e. ***Profile City*** f. ***Profile Street*** g. ***Password***

#	Title	Requirement
		h. ***Phone Number*** i. ***Email address*** j. ***Language Preference.***

APPENDIX C - GLOSSARY OF TERMS

Term	Abbreviation	Definition
Activity		A unit of work documenting compliance and enforcement information related to a specific establishment. A data record containing details about a unit of work documented and tracked in the Solution.
Activity Scope		Activity scope is the specific legislative authorities (sections/sub sections) under which the specific activity is performed. Example, Section 15.1(1) of the TVPA provides the authority to assess compliance of the sale of vaping products.
Activity Scope Plan		Activity scope plan is a grouping of specific legislative authorities (sections/subsections) under which the specific activity is performed. Example, a "General" activity scope plan would include all sections/sub sections of the TVPA.
Alert		A transitory message sent by the Solution that is displayed immediately on the user's screen following the triggering event. An alert requires a response/action from the user. Example, the action the user is performing will trigger an alert indicating that the information will be lost. The alert requires the user to acknowledge the alert before the user can continue.
Artifact		An object taken for analysis to assess their compliance with the TVPA and its *Regulations*. Examples: a. product samples b. industry reports c. images d. photographs e. signs f. videos g. publications h. audio recordings i. other types of information which the user considers relevant to the activity: i. documented observations on paper ii. electronic document
Assign an activity		The act of transferring ownership of an activity from one user to another. This can be performed only within a region.

Term	Abbreviation	Definition
		A Manager can assign an activity to an Inspector; an Inspector cannot assign an activity to another Inspector. See Refer an activity
Associated activities		A relationship (link) between one or more activities and an establishment.
Associated establishments		A relationship (link) between one or more establishments.
Brand		All of the brand elements that as a whole are used by a manufacturer to identify to a consumer a tobacco product or a vaping product made by the manufacturer. For example, brand elements for a cigarette product would include the brand family name (e.g., Players Light), brand descriptor (e.g., Smooth), and brand size (e.g., King Size).
Business Intelligence Division	BID	A division within TCD.
Business Process Workflow		Workflows based on an approved business processes and procedures. See Workflow
Canada Consumer Product Safety Act	CCPSA	
Cigarette Ignition Propensity Regulation	CIP	A regulation within the CCPSA
Compliance and Enforcement	C&E	The act of planning and documenting the activities of compliance promotion, inspection, and investigation.
Compliance Assessment		The process by which the results of the an artifact analysis are used to determine the state of conformity of a regulated establishment, individual, other legal entity, product, substance, or activity with the requirements of the Tobacco and Vaping Products Act and its Regulations.
Component		A logical grouping of field sets, and fields within them, for the purpose of performing related functionality. Example, the enforcement component would be composed of the field sets and fields that would be used for data entry of enforcement action information. See Tabbed Pane-like Format
Conditionally mandatory (In		A field that must contain a value if a certain condition is met.

Term	Abbreviation	Definition
reference to data fields)		
Confirm		An indication of the completion of a workflow or workflow step. Selecting "Confirm" initiates the "lock" process in a workflow. See Lock and Unlock
Consistent		Performed in the same way over time; not changing; always behaving or happening in the same way.
Consumer Product Safety Directorate	CPSD	A directorate within the Healthy Environments and Consumer Safety Branch of Health Canada responsible for the CCPSA.
Control of activity		The user who has control of the activity has been assigned to it with full editing privileges. Usually this is the user who created the activity. A user may assume control of an activity that has been referred to a user group.
Controlled Substances and Cannabis Branch	CSCB	A branch within Health Canada.
Corporate Services Branch	CSB	A branch within Health Canada.
Data Analysis		The act of analyzing and evaluating data with the intent to: a. improve the *Tobacco and Vaping Products Act*, through policy and regulation updates. b. inform Canadians of the effects of tobacco and tobacco products. c. provide key performance measurement data.
Delegated User		A user delegated by a manufacturer's Primary User to submit specified industry reports on behalf of the manufacturer. Example, a lawyer or an accountant from a different organisation than the manufacturer. See Primary User
Designated User		A user who has been assigned by Reports Control Division to a specific establishment for the purposes of compliance and enforcement review of its industry reports.
Electronic Data Submission		A generic term to describe the means or process by which structured data can be submitted into the Solution, for example, API or form based submission process.
Email notification		An email notification is a notification generated by the Solution that is sent to the User's email address.

Term	Abbreviation	Definition
Enable		To make a field (s) available for the User to: a. Input data b. Update data c. View data
Establishment		A proprietorship, partnership, company, individual or other legal entity involved in a business, commercial activity or other activity that is subject to legislation. An establishment can be involved in one or more business functions such as the manufacture, import, labelling, distribution, promotion, and sale at retail.
Event-driven Workflow		Also known as a business process workflow, and guided workflow. A series of steps that is driven by an event (trigger) until the next event occurs or all steps are completed. Example, in an event-driven workflow for an activity, an inspection activity is triggered by an event, but the user will follow defined activity workflow steps (creation, planning, assessment, enforcement, closure). See Workflow.
Exhibit under the TVPA		An object collected as part of an enforcement action of Seizure initiated during an inspection activity under the authority of the TVPA. Examples of an exhibit: j. product samples k. industry reports l. images m. photographs n. signs o. videos p. publications q. audio recordings r. other types of information which the user considers relevant to the activity: i. documented observations on paper ii. electronic document See Artifact
Exhibit under the *Criminal Code*		An object collected as evidence via Seizure initiated during an investigation activity under the authority of the *Criminal Code*. Examples of an exhibit:

Term	Abbreviation	Definition
		s. product samples t. industry reports u. images v. photographs w. signs x. videos y. publications z. audio recordings aa. other types of information which the user considers relevant to the activity: i. documented observations on paper ii. electronic document See Artifact
External Stakeholder		Any external party who would be interested and/or influenced or affected by the outcomes of the TCD IM-IT project recommendations, but has no direct input into the project.
External User		Any user who accesses the Portal module of the Solution.
Federal Electronic Tobacco Reporting Evaluation System	FETRES	One of three legacy systems that make up the TCD suite of applications.
Field set		A grouping of related fields into a logical set within an area of the user interface, usually with a label identifying the field set.
Graphical User Interface	GUI	
Guided Form		A data entry form that has imbedded logic that moves the user from field to field within the form.
Healthy Environments and Consumer Safety Branch	HECSB	A branch of the Federal Government within Health Canada.
Health Products and Food Branch	HPFB	A branch of the Federal Government within Health Canada.
Inactive: DNS		A status value for an establishment that **D**oes **N**ot **S**ell tobacco and vaping products. Usually the establishment did sell at one time but no longer sells.
Industry		A regulated party who is required to submit mandatory data to Health Canada via the solution. See External User, Regulated Party.
"Industry Reports"		Statement that refers to the following *Activity Reason Type* values for activities where industry reports have been received by industry not subject to audit: a. Scheduled: Industry Report

Term	Abbreviation	Definition
		b. Unscheduled: Industry Report
Industry Report Submission Interface		The interface that the User logs into to submit industry reports.
Information Management, Privacy and Records Services		Advisor to the Project Sponsor. Ensures information management, privacy and record keeping policies are followed.
Internal notification		An internal notification is a notification generated by the Solution that appears in the notification area of the Solution.
Internal User		Any Government of Canada user who has access to all modules of the Solution.
Laboratories		An external user who submits requested data to Health Canada. See External User.
Linked Activity		An activity that is created as a result of a non-compliance and the resulting enforcement action against the establishment that is the focus of the current activity.
Lock and Unlock		Alternate terms: "locks it down"; "locks down", "locked down". The control process for preventing further changes to an activity, a step in the workflow process or a value, and allowing a subsequent action in the workflow process to be performed. Selecting a "confirm" initiates the "lock" process. See Confirm. "Lock" ensures a precondition is met before a subsequent step can be performed. "Unlock" removes the control process.
Mandatory field		A field that must contain a value.
Manufacturer		In respect of a tobacco product or vaping product, includes any entity that is associated with a manufacturer, including an entity that controls or is controlled by the manufacturer or that is controlled by the same entity that controls the manufacturer. Entity includes a corporation, firm, partnership association, society, trust or other organization, whether incorporated or not.
Modal Window		A modal window is a graphical control element subordinate to a parent window.
No Evidence of Non-Compliance (In reference to *Compliance & Enforcement Policy for the Tobacco and Vaping Products Act* and its Regulations)		A compliance assessment status resulting from an analysis of an artifact(s) under the TVPA and its *Regulations*.

Term	Abbreviation	Definition
Non-Compliance (In reference to *Compliance & Enforcement Policy for the Tobacco and Vaping Products Act* and its Regulations)		A compliance assessment status and value resulting from an analysis of an artifact(s) under the TVPA and its *Regulations*.
Notification		Does not require a response/action from the user. Can be triggered by an event or a user's action. The message can contain a high priority message that would be seen by all users, e.g., important information on planned Solution downtime for maintenance, known Solution issues, new policy announcements, etc. A notification may be sent by email or displayed in the notification area of the Solution.
Office of Compliance for Tobacco and Vaping Products	OCTVP	A division within the Tobacco Control Directorate.
Off-line		Disconnected from the internet.
Off-site Activity		An activity not conducted at an establishment's physical location: a. Remote – conducted via telecommunications b. Virtual – conducted on-line at an establishment's website or social media account
On-site Activity		An activity conducted at an establishment's physical location.
Organizational Unit		A group of users organized by geographical location, by role, or some other criteria. Organizational units exist across Canada. Each organizational unit is composed of specific regions, provinces and territories. Organizational units are periodically re-organized.
Portal		A secure gateway for External Users to access the following functionality: a. Submitting an industry report b. Submitting a complaint c. Submitting an enquiry d. Submitting a support request
Portal User Interface		An interface of the Portal accessible to users outside of Government of Canada registered users.
Primary User		An External User with the ability to submit industry reports and delegate reporting responsibilities to a Supplier User or Delegated User.

Term	Abbreviation	Definition
		A Primary User is a user authorised by the manufacturer to manage the Delegated User and Supplier User accounts, and submit industry reports on behalf of the manufacturer. See Delegated User, Supplier User
Project		A temporary endeavor undertaken to create a unique product or service, that has a defined beginning and end in time, and therefore defined scope and resources. Projects are different from other ongoing operations in an organization, because unlike operations, projects have a definite beginning and an end - they have a limited duration.
Project Plan		A formal, approved document used to guide both project execution and provide project control.
Read-only		Text that cannot be edited; able to be accessed but not modified; capable of being viewed but not being changed or deleted.
Refer an activity		The act of transferring ownership of an activity from one user to another. This can be performed within regions or between regions. A manager can refer an activity to another Manager or Manager Group. See Assign an activity.
Region		A region is composed of one or more provinces and territories.
Regulation		Rule or directive made and maintained by Canada.
Regulated Party		Any person subject to the *Tobacco and Vaping Products Act* and its regulations. This may include individuals, companies, and other organizations. Regulated parties are external users when interacting with the Solution. See External User.
Regulatory Operations and Enforcement Branch	ROEB	A branch of the Federal Government within Health Canada.
Reports Control Division	RCD	A division within the Tobacco Product Regulatory Office (TPRO), TCD; responsible for the tracking, documenting, verifying information, and performing C&E on the reports submitted by Tobacco (and Vaping Products) Industry. Project sponsor responsible for ensuring that the Solution meets the needs of the intended users, in addition to defining the business objectives.
Representative		Lead resource for coordination and reporting of work performed as part of this project.

Term	Abbreviation	Definition
Research and Surveillance		A division within TCD.
Sample (In reference to *Compliance & Enforcement Policy for the Tobacco and Vaping Products Act* and its Regulations)		An object related to tobacco and vaping products collected for analysis to verify compliance under legislation. See Artifact.
Search Warrant		See Warrant
Solution Administrator		A Solution User who has the rights to: a. dictate what actions the user can perform in the Solution b. configure Solution settings and parameters
Solution Parameter		A Solution parameter is a numerical or other measurable factor forming one of a set that defines a system or sets the conditions of its operation.
Stakeholder		An individual, group or organization who may affect, be affected by, or perceive itself to be affected by a decision, activity or outcome of the project.
Subordinate		A User with either of the following designations in the role of a Subordinate in the Solution: a. Inspector. Specialist - a User who can assume the role of Supervisor or Subordinate for an activity, but not both roles for the same activity.
Supervisor		A User with either of the following designations in the role of a Supervisor in the Solution: a. Manager. Specialist - a User who can assume the role of Supervisor or Subordinate for an activity, but not both roles for the same activity.
Supplier User		A user who is authorized to submit industry reports on behalf of the manufacturer with the following conditions: • Can submit only certain types of industry reports • Can submit only brands specified by the manufacturer • The industry report can never be viewed by the manufacturer
Submission Requirements		The requirements based on legislation that determine: • the frequency at which an industry report needs to be submitted • brands required to be submitted for that particular industry report.

Term	Abbreviation	Definition
		The Solution based on these requirements determines if an industry report has been received on or before the due date and if all the required brands have been submitted excluding those that have been exempted.
System		Refers to functionality external to the Solution.
Tabbed Pane-like Format		"Tabbed pane-like" format refers to a graphical user interface element used to hold a logical grouping of data. For example, a "tabbed pane-like" element could be windows, screens, pop-ups, tabs, accordions, forms, and components. See Component
Test Shopper		A young person who tests youth access restrictions for tobacco and vaping products.
Tobacco and Vaping Products Act	TVPA	The *Tobacco and Vaping Products Act* replaced the *Tobacco Act*. The new legislation, enacted in 2018, provides a legislative framework to address the impact of tobacco and vaping products in Canada.
Tobacco Compliance Information Management System	TCIMS	One of three legacy systems that make up the TCD suite of applications. TCIMS is used by TVCEP users (inspectors) to collect compliance data in a standard format to enable analysis of national and regional compliance information.
Tobacco Control Directorate	TCD	A directorate within CSCB responsible for legislating tobacco and vaping products.
Tobacco Product Information Regulations	TPIR	A regulation within the *Tobacco and Vaping Products Act*.
Tobacco Product Labeling Regulations	TPLR	A regulation within the *Tobacco and Vaping Products Act*.
Tobacco Product Regulatory Office	TPRO	An office within the Tobacco Control Directorate.
Tobacco Reporting Regulations	TRR	A regulation within the *Tobacco and Vaping Products Act*.
Tobacco Reporting Regulations (Plain and Standardized Appearance)	TPR(PSA)	A regulation within the *Tobacco and Vaping Products Act*.

Term	Abbreviation	Definition
Tobacco Reporting Regulations System	TRRS	One of three legacy systems that make up the TCD suite of applications. TRRS is used by the Tobacco Control Directorate to record submitted Tobacco Industry reports as required under the *Tobacco Reporting Regulations*.
Tobacco and Vaping Compliance and Enforcement Program	TVCEP	A program within the Regional Compliance and Enforcement Branch (ROEB) of Health Canada
User-centered Design		User-centred design ensures that users can effectively and efficiently find, understand, and use the information and services provided through websites and Web applications. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=24227
User Preferences		Settings that can be configured for a particular user. Each user can change some values for their preferences. For example, a user can change the time zone, language preference, and turn an option on or off.
Warrant under the TVPA		Refers to a "Warrant to Enter a Dwelling House" during an Inspection Activity.
Warrant under the *Criminal Code*		Refers to a "Search Warrant under the Criminal Code" during an Investigation Activity.
Workflow		A series of steps that moves the user through the execution of a specific task required to complete the work. A workflow may contain one or more sub-workflows. See Event-driven Workflow.
Vaping Products Labelling and Packaging Regulations	VPLPR	A regulation within the *Tobacco and Vaping Products Act*.

APPENDIX D – NICEMS CONTRACTOR ENGAGEMENT – PROTOTYPE PHASE

D.1 Purpose: Contractor Engagement Sessions

a) The agile systems development approach requires more interaction with Contractors to produce better results for the Government of Canada. Canada requires Contractors to thoroughly understand the requirements, be innovative and to have users at the forefront. Canada has a requirement to hold engagement sessions with Contractors to provide feedback on the prototypes as these are being developed. These sessions would be conducted in the same manner for each Contractor to allow each Contractor the same opportunity to demonstrate and seek feedback or input to their prototype work.

b) The scope of work involves the planning, design, development, configuration, testing and delivery of a production quality, hosted, working Prototype Solution ready to be deployed, in accordance with the Phase 1 - Prototype Solution Requirements and Deliverables.

c) Prototype:

i) **Description:** Contractor delivers the requirements for the CUA Scenarios (i.e. Prototype Solution) in the RFP.

ii) **Intent**: Allow Contractor to prove they can meet all the requirements in the CUA, but also, demonstrate any additional or advanced features that their product is capable within the timeframe.

D.2 Concept for Contractor Engagement Sessions

a) There will be two (2) engagement sessions held during the Prototype phase with each Contractor. The expectation is that each contractor will participate in the sessions throughout the prototype development process.

b) The two (2) sessions will be held in the early and latter periods of the Prototype phase. Contractors and their prototypes will not be assessed or evaluated during the sessions (i.e., scores are not taken in relation to the Capability Usability Assessment (CUA)). The objective is to provide feedback and answer questions to allow the Contractor to continue to build a better prototype to better meet Canada's needs.

c) There will be common elements and rules that will apply to all three sessions, but the objectives and composition for each of the sessions will differ slightly as described below.

D.2.1 Common to all Sessions

a) Each session will be a maximum of eight (8) hours long and conducted virtually with presentation capabilities and multiple points of connectivity. If in-person sessions are possible, in person sessions may be conducted at a location located in the National Capital Region.

b) Each session will allow the Contractor to demonstrate and seek input or feedback on the following capabilities based on the use cases that have been provided in the CUA:

i) Establishment Profile;
ii) Compliance and Enforcement (C&E) Activity;
iii) Electronic Data Submission;
iv) Pre-defined Reporting and Templates; and
v) User Account Administration.

c) The session may also allow for the discussion of non-functional capabilities. Canada is planning on the presence of TCD's Technical Subject Matter Experts (SMEs) at the engagement sessions in order to gain an understanding of Contractor prototypes and non-functional requirements.

D.2.2 Responses to Contractor

a) The Question and Answer (Q&A) process is already built-in to PSPC's procurement process as per the RFP and Standard Acquisition Clauses and Conditions[1] (SACC) 2003. Contractor proprietary information in a question is not shared with others during a Q&A process. Canada's responses (and questions) to other types of questions will be communicated directly to other contractors by the contracting authority to ensure transparency and fairness in the process. All written responses to contractor questions would go through the Contracting Authority and for documentation on the contract file.

b) As the purpose of the engagement sessions is not to formally evaluate the prototypes, Canada will not provide a score or formally confirm if something that is demonstrated by a Contractor meets or does not meet a requirement.

c) Canada will informally provide feedback to contractors on the basis of being "ON TRACK", "NOT ON-TRACK" or "UNABLE TO PROVIDE FEEDBACK AT THIS STAGE". This feedback does not constitute a formal assessment which formal assessment will be conducted during the CUA assessment process.

i) ON TRACK: aligned to functional capabilities described in CUA.

ii) NOT ON-TRACK: misaligned to functional capabilities described in CUA.

iii) UNABLE TO PROVIDE FEEDBACK AT THIS STAGE: not enough detail to comment.

[1] https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manualconditions-manual

d) Regardless of the feedback that is provided, Canada will not be held responsible for the feedback during the formal CUA assessment process (for example., Canada could indicate as feedback during the engagement sessions that a requirement is deemed "ON-TRACK", but then realise during the CUA assessment that the Contractor has not met the requirement based on a more fulsome assessment and the fact that many things could change from a demonstration to the formal assessment).

e) With respect to feedback sought on usability, look, and feel, responses will be limited to "ALIGNS WITH EXPECTATIONS", "DOES NOT ALIGN WITH EXPECTATIONS" or "UNABLE TO PROVIDE FEEDBACK AT THIS STAGE".

i) ALIGNS WITH EXPECTATIONS: user friendly.

ii) DOES NOT ALIGN WITH EXPECTATIONS: not user friendly.

iii) UNABLE TO PROVIDE FEEDBACK AT THIS STAGE: not enough detail to comment.

D.2.3 Contractor Engagement Process

a) The following procedures outline the steps and safeguards to be followed during the contractor engagement sessions that will occur during the Prototype phase of the Prototype development.

i) The Contractor must provide an advanced overview of what they are planning to demonstrate in each session. The overview must be provided to the Technical Authority at least three (3) business days prior to the demonstration to ensure that the Technical Authority has the appropriate SMEs present during the session.

ii) During the demonstration, there may be occasion for the Technical Authority to "flag" to the Contractor that questions will be asked on a certain topic.

iii) There may be a pause within the session so that a brief discussion can be held amongst key Technical Authority representatives.

iv) The Q&A session will allow for interaction between the Technical Authority and the Contractor where either side can pose and answer questions. All questions and answers will be recorded by scribes for record keeping purposes.

v) The Contractor may refer back to, or choose to re-demonstrate, their Prototype Solution when responding to questions from the Technical Authority.

vi) Any questions from the Contractor that cannot be answered directly by the Technical Authority during the Q&A Session will be placed in a "parking lot" to be answered in writing within five (5) business days of the demonstration. The Technical Authority reserves the right to decide which questions it would like to place in the "parking lot" during the session.

vii) Any questions from the Technical Authority that cannot be answered directly by the Contractor will be placed in a "parking lot" to be answered in writing within five (5) business days of the demonstration. The Contractor reserves the right to decide which questions it would like to place in the "parking lot" during the session. The Technical Authority will only respond and release information according to the security classification of the information that the Technical Authority is permitted to release at this stage of the process.

viii) The Contractor will receive a written transcript of the Q&As within five (5) business days of the demonstration.

ix) Any Q&A's that are proprietary in nature, as identified by the Contractor in their response, will not be shared with the other prototype Contractors. Q&As that are not proprietary in nature, will be shared with the other prototype Contractors.

D.3 Concept for Session 1

Table D-1:	**Concept for Session 1**		
Timeframe	4 weeks after beginning of prototype process		
Objective	A required early general demonstration of work to date, less focused on usability, more on technologies being used, overall concepts, Technical Authority providing feedback.		
Engagement Day	Morning and Early afternoon	Contractor general demos provided. Pose questions or seek feedback, does not need to cover some specific capabilities and use cases	6 hours
	Afternoon	Technical Authority questions and to provide unsolicited feedback	2 hours

D.4 Concept for Session 2

Table D-2:	**Concept for Session 2**
Timeframe	8 weeks after beginning of prototype process
Objective	The objective for the second session is for the Contractor to provide demonstrations of up to five (5) capabilities and how they work in relation to the use cases. As a minimum, this session should include a demonstration of the: • Establishment Profile, Scenario 1 • Compliance and Enforcement (C&E) Activity for Scenario 3 to 8 • Pre-defined Reporting and Templates, Scenario 15 • User Account Administration It is up to the Contractor to determine if they will showcase all five (5) capabilities and all use cases. This session should include more detailed and live demonstrations and explanations of functions or requirements for up to five (5) capabilities.

Table D-2:	**Concept for Session 2**		
	Visual presentation of the second session should include multiple displays so that the reviewers can see details up close.		
Engagement Day	Morning	Contractor Demos, pose questions or seek feedback. To cover at least the capabilities for session 2.	4.5 hours
	Afternoon	Allow Technical Authority SMEs to "test drive" the scenarios. Two additional requests for the Contractor to demonstrate aspects of this capability will be permitted during this hour.	1.5 hours
	Afternoon	Allow Technical Authority to request demonstration on certain elements (includes time required for the demo itself).	1 hour
	Afternoon	Allow Technical Authority questions and to provide unsolicited feedback.	1 hour

D.5 Concept for Session 3

Table D-3:	**Concept for Session 3**		
Timeframe	11 weeks after beginning of prototype process		
Objective	The objective for the third session is for the Contractor to provide a fulsome demonstration of all capabilities and how they work in relation to the use cases. This should include a demonstration of all capabilities and include an interactive portion where Technical Authority and SMEs are able to operate the prototype with a Contractor representative guiding them. Demonstrations do not need to cover all material demonstrated previously. This session should focus on quite detailed and live demonstrations and explanations of functions or requirements within each of the capabilities. This session must include the ability for Technical Authority and SMEs to work with the prototype and operating the system with the assistance of a Contractor representative. This session will mostly be accomplished virtually.		
Engagement Day	Morning	Contractor to provide general demonstrations, pose questions or seek feedback on all capabilities.	2 hours
	Afternoon	Allow Technical Authority and SMEs to "test-drive" all capabilities. Additional requests for the Contractor to demonstrate aspects of this capability will be permitted during this time.	1.5 hour

Table D-3: Concept for Session 3			
	Afternoon	Allow Technical Authority to request demonstration on certain elements (includes time for the demo itself).	0.75 hour

THIS PAGE HAS BEEN LEFT INTENTIONALLY BLANK

APPENDIX E – SECURITY CONTROLS

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AC-1	Access Control Policy and Procedures	Technical	Access Control Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with access control responsibilities: (a) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the access control policy and associated access controls. (B) The organization reviews and updates the current: (a) Access control policy at least every 3 years; and (b) Access control procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable policies, directives and standards. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the	X	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures						

AC-2	Account Management	Technical	Account Management	(A) The organization identifies and selects which types of information system accounts support organizational missions/business functions. (B) The organization assigns account managers for information system accounts. (C) The organization establishes conditions for group and role membership. (D) The organization specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. (E) The organization requires approvals by responsible managers for requests to create information system accounts. (F) The organization creates, enables, modifies, disables, and removes information system accounts in accordance with information system account management procedures. (G) The organization monitors the use of information system accounts. (H) The organization notifies account managers: (a) When accounts are no longer required; (b) When users are terminated or transferred; and (c) When individual information system usage or need-to-know changes. (I) The organization authorizes access to the	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or information technology security co-ordinator) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other	**X**	X	X	X	X	X

				information system based on: (a) A valid access authorization; (b) Intended system usage; and (c) Other attributes as required by the organization or associated missions/business functions. (J) The organization reviews accounts for compliance with account management requirements at least annually. (K) The organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local accounts used for special tasks defined by organizations or when network resources are						

					unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AC-2(1)	Account Management	Technical	Account Management | Automated System Account Management	ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT The organization employs automated mechanisms to support the management of information system accounts.	The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage.	X	X	X	X	X	X
AC-2(2)	Account Management	Technical	Account Management | Removal of Temporary / Emergency Accounts	ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically disables temporary and emergency accounts after no more than 30 days for both temporary and emergency accounts.	This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.	X	X	X	X	X	
AC-2(3)	Account Management	Technical	Account Management | Disable Inactive Accounts	ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS The information system automatically disables inactive accounts after 90 days.		X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-2(4)	Account Management	Technical	Account Management | Automated Audit Actions	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies responsible managers. Related controls: AU-2, AU-12.		**X**	X	X	X	X	
AC-2(5)	Account Management	Technical	Account Management | Inactivity Logout	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT The organization requires that users log out at the end of the users' standard work period unless otherwise defined in formal organizational policy. Related controls: SC-23		**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-2(7)	Account Management	Technical	Account Management | Role-Based Schemes	ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES (a) The organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) The organization monitors privileged role assignments; and (c) The organization disables (or revokes) privileged user assignments within 24 hours or sooner when privileged role assignments are no longer appropriate.	Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.	**X**	X	X	X	X	X
AC-2(9)	Account Management	Technical	Account Management | Restrictions on Use of Shared Groups / Accounts	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS The organization only permits the use of shared/group accounts that meet organization-defined conditions for establishing shared/group accounts.		**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AC-2(10)	Account Management	Technical	Account Management | Shared / Group Account Credential Termination	ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION The information system terminates shared/group account credentials when members leave the group.		X	X	X	X	X	
AC-3	Access Enforcement	Technical	Access Enforcement	(A) The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g.: access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3						

AC-4	Information Flow Enforcement	Technical	Information Flow Enforcement	(A) The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on deny all, approve by exception information flow policies.	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations should consider	**X**	X	X	X	X	

					mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy re-grading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a						

					packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/ inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-4(21)	Information Flow Enforcement	Technical	Information Flow Enforcement | Physical / Logical Separation of Information Flows	INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS The information system separates information flows logically or physically using session encryption to accomplish separation of all sessions.	Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.	**X**	X	X		X	
AC-5	Separation of Duties	Technical	Separation of Duties	(A) The organization: (a) Separate organization-defined duties of individuals including at least separation of operational, development, security monitoring, and management functions; (b) Documents separation of duties of individuals; and (c) Defines information system access authorizations to support separation of duties.	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2						
AC-6	Least Privilege	Technical	Least Privilege	(A) The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/ business functions. Organizations consider the creation of additional processes, roles, and information system accounts as	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2						
AC-6(1)	Least Privilege	Technical	Least Privilege | Authorize Access to Security Functions	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS The organization explicitly authorizes access to all security functions not publicly accessible and all security-relevant information not publicly available.	Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/ firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.						
AC-6(2)	Least Privilege	Technical	Least Privilege | Non-Privileged Access for Non-Security Functions	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS The organization requires that users of information system accounts, or roles, with access to any security function, use non-privileged accounts or roles, when accessing non-security functions.	This control enhancement limits an information system's exposure to threats when users are operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as RBAC and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					privileged and non-privileged account. Related control: PL-4.						
AC-6(5)	Least Privilege	Technical	Least Privilege | Privileged Accounts	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS The organization restricts privileged accounts on the information system to the minimum number of personnel required to securely administer, manage, and protect the information systems.	Privileged accounts, including super user accounts, are typically described as system administrators for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/ functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.						
AC-6(9)	Least Privilege	Technical	Least Privilege | Auditing Use of Privileged Functions	LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS The information system audits the execution of privileged functions.	Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					(APT). Related control: AU-2.						
AC-6(10)	Least Privilege	Technical	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-7	Unsuccessful Login Attempts	Technical	Unsuccessful Logon Attempts	(A) The information system enforces a limit of not more than three consecutive invalid logon attempts by a user during a 15-minute time period. (B) The information system automatically locks the account/node for a minimum of three (3) hours or until unlocked by an administrator.	Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may choose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14. This security control/enhancement requires careful balance between usability and security. Care needs to be	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					taken to ensure that the appropriate balance between the two seemingly conflicting requirements is achieved. If possible, an increasing time-out period should be used to deter determined attackers. For example, an original time-out of 5 minutes can become 10 minutes after the next 3 unsuccessful attempts, then 20 minutes, then 40 minutes, etc.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-8	System Use Notification	Technical	System Use Notification	(A) The information system displays to users a organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices in accordance with organization's network use policies. (B) The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system. (C) The information system for publicly accessible systems: (a) Displays system use information before granting further access; (b) Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (c) Includes a description of	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/ banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations should also consult with legal services for review and approval of warning banner content	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				the authorized uses of the system.							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-10	Concurrent Session Control	Technical	Concurrent Session Control	(A) The information system limits the number of concurrent sessions for all accounts unless justified for operation requirements to 3 sessions for privileged access and 2 sessions for non-privileged access.	Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-11	Session Lock	Technical	Session Lock	(A) The information system prevents further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user. (B) The information system retains the session lock until the user re-establishes access using established identification and authentication procedures.	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7	**X**	X	X	X	X	
AC-11(1)	Session Lock	Technical	Session Lock | Pattern-Hiding Displays	SESSION LOCK | PATTERN-HIDING DISPLAYS The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					images convey sensitive information.						
AC-12	Session Termination	Technical	Session Termination	(A) The information system automatically terminates a user session after a maximum of 24 hours of inactivity or upon request by the user.	This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e.,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-14	Permitted Actions Without Identification or Authentication	Technical	Permitted Actions without Identification or Authentication	(A) The organization identifies user actions that can be performed on the information system without identification or authentication consistent with organizational missions/ business functions. (B) The organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-17	Remote Access	Technical	Remote Access	(A) The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. (B) The organization authorizes remote access to the information system prior to allowing such connections. (AA) The organization ensures that all employees working off site safeguard information as per the organization's minimum security requirements (NOTE: Item (AA) is not applicable to CSPs).	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7,					

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-17(1)	Remote Access	Technical	Remote Access | Automated Monitoring / Control	REMOTE ACCESS | AUTOMATED MONITORING / CONTROL The information system monitors and controls remote access methods.	Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.	**X**	X	X	X	X	
AC-17(2)	Remote Access	Technical	Remote Access | Protection of Confidentiality / Integrity using Encryption	REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. The cryptography must be compliant with the requirements of SC-13.	Guidance on the encryption strength of mechanism can be obtained from CSE upon request.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-17(3)	Remote Access	Technical	Remote Access | Managed Access Control Points	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS The information system routes all remote accesses through approved managed network access control points.	Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Related control: SC-7.	**X**	X	X	X	X	
AC-17(4)	Remote Access	Technical	Remote Access | Privileged Commands / Access	REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS (a) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for approved operational requirements; and (b) The organization documents the rationale for such access in the security plan for the information system.	Related control: AC-6.	**X**	X	X	X	X	X
AC-17(9)	Remote Access	Technical	Remote Access | Disconnect / Disable Access	REMOTE ACCESS | DISCONNECT / DISABLE ACCESS The organization provides the capability to expeditiously disconnect or disable remote access to the information system within a period no greater than 15 minutes.	This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/ or disable further remote access. The speed of disconnect or disablement varies based on the criticality of	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.						
AC-17(100)	Remote Access	Technical	Remote Access | Remote Access to Privileged Accounts using Dedicated Management Console	Remote access to privileged accounts is performed on dedicated management consoles governed entirely by the system's security policies and used exclusively for this purpose (e.g. Internet access not allowed).		**X**	X	X	X	X	X
AC-18	Wireless Access	Technical	Wireless Access	(A) The organization establishes usage restrictions, configuration/ connection requirements, and implementation guidance for wireless access. (B) The organization authorizes wireless access to the information system prior to allowing such connections.	Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11, and Bluetooth. Wireless networks use authentication protocols (e.g., Extensible Authentication Protocol (EAP) / Transport Layer Security (TLS), Protected EAP (PEAP)), which provide credential	**X**	X	X		X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4, SC-9						
AC-18(1)	Wireless Access	Technical	Wireless Access | Authentication and Encryption	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION The information system protects wireless access to the system using authentication of devices to wireless networks (e.g., Wi-Fi) and users to enterprise services and encryption.	Related controls: SC-8, SC-13.	**X**	X	X		X	
AC-18(4)	Wireless Access	Technical	Wireless Access | Restrict Configurations by Users	WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15.	**X**				X	X

AC-19	Access Control for Mobile Devices	Technical	Access Control for Mobile Devices	(A) The organization establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices. (B) The organization authorizes the connection of mobile devices to organizational information systems.	A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of	**X**	X	X	X	X	X

					mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security						

					plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4							

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AC-20	Use of External Information Systems	Technical	Use of External Information Systems	(A) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems. (B) The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to process, store, or transmit organization-controlled information using external information systems.		X	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AC-20(1)	Use of External Information Systems	Technical	Use of External Information Systems | Limits of Authorized Use	USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-20(2)	Use of External Information Systems	Technical	Use of External Information Systems | Portable Storage Devices	USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES The organization restricts unless approval obtained for operational reasons the use of organization-controlled mobile devices by authorized individuals on external information systems.	Limits on the use of organization-controlled mobile devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.	**X**	X	X	X	X	X
AC-21	User-Based Collaboration and Information Sharing	Technical	Information Sharing	(A) The organization facilitates information sharing by enabling authorized users to determine if access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required; and (B) The organization employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.	This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					security category, or special access program/ compartment. Related control: AC-3						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AC-22	Publicly Accessible Content	Technical	Publicly Accessible Content	(A) The organization designates individuals authorized to post information onto a publicly accessible information system. (B) The organization trains authorized individuals to ensure that publicly accessible information does not contain confidentially sensitive information. (C) The organization reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that confidentially sensitive information is not included. (D) The organization reviews the content on the publicly accessible information system for confidentially sensitive information at least quarterly and removes such information, if discovered.	This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy. Related controls: AC-3, AC-4, AT-2, AT-3, AU-13	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AT-1	Security Awareness and Training Policy and Procedures	Operational	Security Awareness and Training Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with security awareness and training responsibilities: (a) A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. (B) The organization reviews and updates the current: (a) Security awareness and training policy at least every 3 years; and (b) Security awareness and training procedures at least annully..	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable organizational policies, directives, and standards. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizational risk management strategy is a key factor in establishing policy and procedures.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AT-2	Security Awareness	Operational	Security Awareness Training	(A) The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): (a) As part of initial training for new users; (b) When required by information system changes; and (c)At least annually thereafter.	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					events. Related controls: AT-3, AT-4, PL-4						
AT-2(2)	Security Awareness	Operational	Security Awareness Training | Insider Threat	SECURITY AWARENESS | INSIDER THREAT The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.	Potential indicators and possible precursors of insider threat can include behaviours such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PS-3, PS-6.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AT-3	Role Based Security Training	Operational	Role-Based Security Training	(A) The organization provides role-based security training to personnel with assigned security roles and responsibilities: (a) Before authorizing access to the information system or performing assigned duties; (b) When required by information system changes; and (c)At least annually thereafter.	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software with adequate security-related technical training specifically tailored for	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical security controls. Such training can include, for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AT-4	Security Training Records	Operational	Security Training Records	(A) The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and (B) The organization retains individual training records for at least one year.	Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3.	**X**	X	X	X	X	X
AU-1	Audit and Accountability Policy and Procedures	Technical	Audit and Accountability Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with audit responsibilities; (a) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. (B) The organization reviews and updates the current: (a) Audit and accountability poliat least every three years; and	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable organizational policies, directives, and standards. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				(b) Audit and accountability procedures at least annually.	conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures						

AU-2	Auditable Events	Technical	Audit Events	(A) The organization determines that the information system is capable of auditing the following 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. (B) The organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. (C) The organization provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents. (D) The organization determines what organizationally-defined audited events (a subset of the auditable events defined in AU-2 a.) and the frequency of (or situation requiring) auditing for each identified event.	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the	**X**	X	X	X	X	X

					potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable organizational policies, directives, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. The information system audits the following privileged user/process events at a minimum: (a) Successful and unsuccessful attempts to access, modify, or delete						

					security objects (Security objects include audit data, system configuration files and file or users' formal access permissions.) (b) Successful and unsuccessful logon attempts (c) Privileged activities or other system level access (see notes for AU-2 (4)) (d) Starting and ending time for user access to the system (e) Concurrent logons from different workstations (f) All program initiations (see notes for AU-2 (4)) In addition, the information system audits the following unprivileged user/process events at a minimum: (a) Successful and unsuccessful attempts to access, modify, or delete security objects (b) Successful and unsuccessful logon attempts (c) Starting and ending time for user access to the system (d) Concurrent logons from different workstations Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-2(3)	Auditable Events	Technical	Audit Events | Reviews and Updates	AUDIT EVENTS | REVIEWS AND UPDATES The organization reviews and updates the audited events annully or whenever there is a change in the threat environment.	Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.	**X**	X	X	X	X	X
AU-3	Content of Audit Records	Technical	Content of Audit Records	(A) The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-3(1)	Content of Audit Records	Technical	Content of Audit Records | Additional Audit Information	CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION The information system generates audit records containing the following additional 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.	Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Additional guidance for enhancement (1): Audit events should always be capable of being associated with an individual identity. Associating audit events with a group or role is insufficient.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-5	Response To Audit Processing Failures	Technical	Response to Audit Processing Failures	(A) The information system alerts organization-defined personnel or roles in the event of an audit processing failure; and (B) The information system overwrites the oldest audit records.	Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AU-6	Audit Review, Analysis, and Reporting	Technical	Audit Review, Analysis, and Reporting	(A) The organization reviews and analyzes information system audit records at least every 7 days for indications of compromise identified in SI-4(5). (B) The organization reports findings to organization-defined personnel or roles.	Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					(e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7						
AU-6(1)	Audit Review, Analysis, and Reporting	Technical	Audit Review, Analysis, and Reporting | Process Integration	AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for	Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, and contingency planning. Related control: AU-12.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				investigation and response to suspicious activities.							
AU-6(3)	Audit Review, Analysis, and Reporting	Technical	Audit Review, Analysis, and Reporting | Correlate Audit Repositories	AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-7	Audit Reduction and Report Generation	Technical	Audit Reduction and Report Generation	(A) The information system provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. (B) The information system provides an audit reduction and report generation capability that does not alter the original content or time ordering of audit records.	Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behaviour in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AU-7(1)	Audit Reduction and Report Generation	Technical	Audit Reduction and Report Generation | Automatic Processing	AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING The information system provides the capability to process audit records for events of interest based on all audit fields specified in AU-2, AU-3 and AU-3(1).	Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or sub-network) or selectable by specific information system component. Related controls: AU-2, AU-12.	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-8	Time Stamps	Technical	Time Stamps	(A) The information system uses internal system clocks to generate time stamps for audit records. (B) The information system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) within 1 second precision.	Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC) or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-8(1)	Time Stamps	Technical	Time Stamps | Synchronization with Authoritative Time Source	TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE (a) The information system compares the internal information system clocks at least every 24 hours with an organization-defined authoritative time source; and (b) The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than 1 millisecond.	This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.	**X**	X	X	X	X	
AU-9	Protection of Audit Information	Technical	Protection of Audit Information	(A) The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
AU-9(2)	Protection of Audit Information	Technical	Protection of Audit Information | Audit Backup on Separate Physical Systems / Components	PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited.	This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.	**X**	X	X	X	X	
AU-9(4)	Protection of Audit Information	Technical	Protection of Audit Information | Access by Subset of Privileged Users	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS The organization authorizes access to management of audit functionality to only an organization-defined subset of privileged users.	Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-11	Audit Record Retention	Technical	Audit Record Retention	(A) The CSP retains audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. (B) The client retains audit records and logs for at least 3 months online and at least 6 months in storage. (C) The client retains all audit records and logs associated with a security incident for at least 5 years.	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to legal requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. Related controls: AU-4, AU-5, AU-9, MP-6	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
AU-12	Audit Generation	Technical	Audit Generation	(A) The information system provides audit record generation capability for the auditable events defined in AU-2 a. of all information system and network components where audit capability is deployed/ available. (B) The information system allows organization-defined personnel or roles to select which auditable events are to be audited by specific components of the information system. (C) The information system generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CA-1	Security Assessment and Authorization Policies and Procedures	Management	Security Assessment and Authorization Policies and Procedures	(A) The organization develops, documents, and disseminates to all personnel or roles with security assessment responsibilities: (a) A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. (B) The organization reviews and updates the current: (a) Security assessment and authorization policy at least every 3 years; and (b) Security assessment and authorization procedures at least annually.	This control addresses the establishment of policies and procedures for the effective implementation of selected security controls and control enhancements in the CA family. The security assessment and authorization policies and procedures reflect applicable organizational policies, directives and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					needed. The organizational risk management strategy is a key factor in establishing policies and procedures.						

CA-2	Security Assessments	Management	Security Assessments	(A) The organization develops a security assessment plan that describes the scope of the assessment including: (a) Security controls and control enhancements under assessment; (b) Assessment procedures to be used to determine security control effectiveness; and (c) Assessment environment, assessment team, and assessment roles and responsibilities. (B) The organization assesses the security controls in the information system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements. (C) The organization produces a security assessment report that documents the results of the assessment. (D) The organization provides the results of the security control assessment to organization-defined individuals or roles.	Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) policy requirement for periodic assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Organizations can several types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy	**X**	X	X	X	X	X

					and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security control requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations, organizations assess security controls periodically during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in						

					accordance with organizational continuous monitoring strategies. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, RA-5, SA-11, SA-12, SI-4.							

CA-2(1)	Security Assessments	Management	Security Assessments | Independent Assessors	SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS The organization employs assessors or assessment teams with an external independent organization to conduct security control assessments.	Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to entities outside of the organizations. Authorizing officials determine the required level of independence based on the security categories of	**X**	X	X	X	X	X

					information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of						

					experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CA-2(2)	Security Assessments	Management	Security Assessments | Specialized Assessments	SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS The organization includes as part of security control assessments that they will be announced and done at least annually and include at least vulnerability scanning and penetration testing.	Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk management strategy. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CA-2(3)	Security Assessments	Management	Security Assessments | External Organizations	SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS The CSP accepts the results of an assessment of the CSP's information system within the scope of the cloud services provided excluding tenant components performed by an external, independet organization when the assessment meets all applicable requirements.	Organizations may often rely on assessments of specific information systems by other (external) organizations. Utilizing such existing assessments (i.e., reusing existing assessment evidence) can significantly decrease the time and resources required for organizational assessments by limiting the amount of independent assessment activities that organizations need to perform. The factors that organizations may consider in determining whether to accept assessment results from external organizations can vary. Determinations for accepting assessment results can be based on, for example, past assessment experiences one organization has had with another organization, the reputation that organizations have with regard to assessments, the level of detail of	**X**	X	X	X		

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					supporting assessment documentation provided, or mandates imposed upon organizations by organizational policies, directives, and standards.						

CA-3	Information System Connections	Management	System Interconnections	(a) The organization authorizes connection from information system to other information system through the use of Interconnection Security Agreements. (b) The organization documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated. (c) The organization reviews and updates Interconnection Security Agreements annually.	This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security control requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection	**X**	X	X	X	X	X

					Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4						
CA-3(3)	Information System Connections	Management	System Interconnections | Classified Non-National Security System Connections	SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS The organization prohibits the direct connection of any internal network or system to an external network without the use of security controls	Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified non-	**X**	X	X		X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				approved by the information owner.	national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting sensitive Information.						
CA-3(5)	Information System Connections	Management	System Interconnections | Restrictions on External Network Connections	SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS The organization employs allow-all, deny-by-exception; deny-all policy for allowing any systems to connect to external information systems.	Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.	**X**	X	X		X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CA-5	Plan of Action and Milestones	Management	Plan of Action and Milestones	(A) The organization develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and (B) The organization updates existing plan of action and milestones at least monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	Plans of action and milestones are key sections of the operations security plan, which is are key documents in the security authorization packages and may be subject to organizational reporting. Related controls: CA-2, CA-7, CM-4.	**X**	X	X	X	X	X

CA-6	Security Authorization	Management	Security Authorization	(A) The organization assigns a senior-level executive or manager as the authorizing official for the information system. (B) The organization ensures that the authorizing official authorizes the information system for processing before commencing operations. (C) The organization updates the security authorization at least every three years or when a significant change occurs.	Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals and other organizations based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. Organizations should conduct ongoing authorizations of	**X**	X	X	X	X	X

					information systems by implementing continuous monitoring programs. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions. Related controls: CA-2, CA-7						

CA-7	Continuous Monitoring	Management	Continuous Monitoring	(A) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes establishment of organization-defined metrics to be monitored. (B) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes establishment of at least monthly monitoring and assessments of at least operating system scans, database, and web application scan. (C) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security control assessments in accordance with the organizational continuous monitoring strategy. (D) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy. (E) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to	**X**	X	X	X	X	X

				correlation and analysis of security-related information generated by assessments and monitoring. (F) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes response actions to address results of the analysis of security-related information. (G) The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes reporting the security status of organization and the information system to organization-defined personnel or roles at organization-defined frequency.	security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, RA-5, SA-11, SA-12, SI-2, SI-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CA-7(1)	Continuous Monitoring	Management	Continuous Monitoring | Independent Assessment	CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT The organization employs assessors or assessment teams with full independence from the organizational unit responsible for day to day security operations to monitor the security controls in the information system on an ongoing basis.	Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CA-8	Penetration Testing	Management	Penetration Testing	(A) The organization conducts penetration testing at least annually on organization-defined information systems or system components.	Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the	**X**	X	X	X		

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CA-8(1)	Penetration Testing	Management	Penetration Testing | Independent Penetration Testing Agent for Team	PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.	Independent penetration agents or teams are individuals or groups who conduct impartial penetration testing of organizational information systems. Impartiality implies that penetration agents or teams are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the information systems that are the targets of the penetration testing. Supplemental guidance for CA-2 (1) provides additional information regarding independent assessments that can be applied to penetration testing. Related control: CA-2.	**X**	X	X	X		

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CA-9	Internal System Connections	Management	Internal System Connections	(A) The organization authorizes internal connections of information system components or classes of components to the information system. (B) The organization documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/ desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12,	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					CA-7, CM-2, IA-3, SC-7, SI-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-1	Configuration Management Policy and Procedures	Operational	Configuration Management Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with configuration management responsibilities: (a) A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. (B) The organization reviews and updates the current: (a) Configuration management policy at least every 3 years; and (b) Configuration management procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general (or the IT program) and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CM-2	Baseline Configuration	Operational	Baseline Configuration	(A) The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/ parameters),	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. A baseline configuration should include all current patches for the operating system and applications installed. The baseline should also deactivate all unused ports, services and software and use an hardened configuration (e.g., guest accounts deactivated, access control to all system files and directories applied, default passwords changed) Related controls: CM-3, CM-6, CM-8, CM-9, SA-10.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-2(1)	Baseline Configuration	Operational	Baseline Configuration | Reviews and Updates	BASELINE CONFIGURATION | REVIEWS AND UPDATES The organization reviews and updates the baseline configuration of the information system: (a)at least annually; or (b) When required due to significant changes as defined in NIST SP 800-37 rev1; and (c) As an integral part of information system component installations and upgrades.	Related control: CM-5.	**X**	X	X	X	X	
CM-2(2)	Baseline Configuration	Operational	Baseline Configuration | Automation Support for Accuracy / Currency	BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5.						
CM-2(3)	Baseline Configuration	Operational	Baseline Configuration | Retention of Previous Configurations	BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS The organization retains the two most recent precious versions of baseline configurations of the information system to support rollback.	Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CM-2(7)	Baseline Configuration	Operational	Baseline Configuration | Configure Systems, Components, or Devices for High-Risk Areas	BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS (a) The organization issue organization-defined information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that the organization deems to be of significant risk; and (b) The organization applies organization-defined security safeguards to the devices when the individuals return.	When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/ reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.						

CM-3	Configuration Change Control	Operational	Configuration Change Control	(A) The organization determines the types of changes to the information system that are configuration-controlled. (B) The organization reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses. (C) The organization documents configuration change decisions associated with the information system. (D) The organization implements approved configuration-controlled changes to the information system. (E) The organization retains records of configuration-controlled changes to the information system for at least 90 days. (F) The organization audits and reviews activities associated with configuration-controlled changes to the information system. (G) The organization coordinates and provides oversight for configuration change control activities through a central communication process that includes organizational governance bodies that convenes at least annually.	Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of	**X**	X	X	X	X	

					changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12							

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CM-3(4)	Configuration Change Control	Operational	Configuration Change Control | Security Representative	CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE The organization requires an information security representative to be a member of the organization-defined configuration change control element.	Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CM-3(6)	Configuration Change Control	Operational	Configuration Change Control | Cryptography Management	CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT The organization ensures that cryptographic mechanisms used to provide any cryptographic-based safeguards are under configuration management.	Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-4	Security Impact Analysis	Operational	Security Impact Analysis	(A) The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-5	Access Restrictions for Change	Operational	Access Restrictions for Change	(A) The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation,	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3						
CM-5(1)	Access Restrictions for Change	Operational	Access Restrictions for Change | Automated Access Enforcement / Auditing	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING The information system enforces access restrictions and supports auditing of the enforcement actions.	Related controls: AU-2, AU-12, AU-6, CM-3, and CM-6.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-5(5)	Access Restrictions for Change	Operational	Access Restrictions for Change | Limit Production / Operational Privileges	ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES (a) The organization limits privileges to change information system components and system-related information within a production or operational environment; and (b) The organization reviews and re-evaluates privileges at least quarterly.	In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/ business processes are in some cases, unknown to developers. Related control: AC-2.	**X**	X	X	X	X	
CM-5(6)	Access Restrictions for Change	Operational	Access Restrictions for Change | Limit Library Privileges	ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES The organization limits privileges to change software resident within software libraries.	Software libraries include privileged programs. Related control: AC-2.	**X**	X	X	X	X	

CM-6	Configuration Settings	Operational	Configuration Settings	(A) The organization establishes and documents configuration settings for information technology products employed within the information system using 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) that reflect the most restrictive mode consistent with operational requirements. (B) The organization implements the configuration settings. (C) The organization identifies, documents, and approves any deviations from established configuration settings for any configurable infomation system components. (D) The organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings	**X**	X	X	X	X	

					for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baselineCommon secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides (STIG)) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal government organizations, and others in the public and private sectors. The						

					Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.							

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CM-6(1)	Configuration Settings	Operational	Configuration Settings | Automated Central Management / Application / Verification	CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for organization-defined information system components.	Related controls: CA-7, CM-4.	X	X	X	X	X	
CM-6(2)	Configuration Settings	Operational	Configuration Settings | Respond to Unauthorized Changes	CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES The organization employs organization-defined security safeguards to respond to unauthorized changes to organization-defined configuration settings.	Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7.	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-7	Least Functionality	Operational	Least Functionality	(A) The organization configures the information system to provide only essential capabilities. (B) The organization prohibits or restricts the use of identified functions, ports, protocols, and/or services following one or more standards from Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), or Defense Information Systems Agency (DISA).	Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					over Internet Protocol (VoIP), Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., USB, FTP, IPv6, HTTP) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunnelling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7					

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-7(1)	Least Functionality	Operational	Least Functionality | Periodic Review	LEAST FUNCTIONALITY | PERIODIC REVIEW The organization reviews the information system at least annually to identify unnecessary and/or non-secure functions, ports, protocols, and services; and The organization disables all functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure.	The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.	**X**	X	X	X	X	
CM-7(5)	Least Functionality	Operational	Least Functionality | Authorized Software / Whitelisting	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING (a) The organization identifie authorized software programs in baseline configuration and information system component inventory; (b) The organization employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) The organization reviews and updates the list of authorized software programs at least annually or when there is a change.	The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system start-up. Related controls:	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					CM-2, CM-6, CM-8, SA-10, SC-34, SI-7						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CM-8	Information System Component Inventory	Operational	Information System Component Inventory	(A) The organization develops and documents an inventory of information system components that accurately reflects the current information system. (B) The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system. (C) The organization develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting. (D) The organization develops and documents an inventory of information system components that includes unique asset identifier, NetBIOS name, baseline configuration name, OS Name, OS Version, system owner information. (E) The organization reviews and updates the information system component inventory at least monthly.	Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-8(1)	Information System Component Inventory	Operational	Information System Component Inventory | Updates During Installations / Removals	INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.		**X**	X	X	X	X	
CM-8(2)	Information System Component Inventory	Operational	Information System Component Inventory | Automated Maintenance	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					activities. Related control: SI-7.						
CM-8(3)	Information System Component Inventory	Operational	Information System Component Inventory | Automated Unauthorized Component Detection	INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION (a) The organization employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detectionto detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) The organization takes the organization-defined actions when unauthorized components are detected such as disables network access by such components; isolates the components;	This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				notifies organization-defined personnel or roles.	such components. This type of component isolation is commonly referred to as sandboxing. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.						
CM-8(5)	Information System Component Inventory	Operational	Information System Component Inventory | No Duplicate Accounting of Components	INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.	This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.	**X**	X	X	X	X	

CM-9	Configuration Management Plan	Operational	Configuration Management Plan	(A) The organization develops, documents, and implements a configuration management plan for the information system that addresses roles, responsibilities, and configuration management processes and procedures. (B) The organization develops, documents, and implements a configuration management plan for the information system that establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. (C) The organization develops, documents, and implements a configuration management plan for the information system that defines the configuration items for the information system and places the configuration items under configuration management; and (D) The organization develops, documents, and implements a configuration management plan for the information system that protects the configuration management plan from unauthorized disclosure and modification.	Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration	**X**	X	X	X	X	

					management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CM-10	Software Usage Restrictions	Operational	Software Usage Restrictions	(A) The organization uses software and associated documentation in accordance with contract agreements and copyright laws. (B) The organization tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution. (C) The organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7	**X**	X	X	X	X	X
CM-10(1)	Software Usage Restrictions	Operational	Software Usage Restrictions | Open Source Software	SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE The organization establishes organization-defined restrictions on the use of open source software.	Open source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open source	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					software is that it provides organizations with the ability to examine the source code. However, there are also various licensing issues associated with open source software including, for example, the constraints on derivative use of such software.						
CM-11	User Installed Software	Operational	User-Installed Software	(A) The organization establishes organization-defined policies governing the installation of software by users. (B) The organization enforces software installation policies through organization-defined methods. (C) The organization monitors policy compliance continuously via 7(5).	If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example,	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-1	Contingency Planning Policy and Procedures	Operational	Contingency Planning Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with contingency planning responsibilities: (a) A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. (B) The organization reviews and updates the current: (a) Contingency planning policy at least every 3 years; and (b) Contingency planning procedures at least annually. (AA) The organization develops an audit cycle for the contingency plan program as the basis of regular reporting.	This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family. The contingency planning policy and procedures are consistent with organizational policies, directive, and standards. Existing organizational policies and procedures may make additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					contingency planning policy.						

CP-2	Contingency Plan	Operational	Contingency Plan	(A) The organization develops a contingency plan for the information system that: (a) Identifies essential missions and business functions and associated contingency requirements; (b) Provides recovery objectives, restoration priorities, and metrics; (c) Addresses contingency roles, responsibilities, and assigned individuals with contact information; (d) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; (e) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and (f) Is reviewed and approved by organization-defined personnel or roles. (B) The organization distributes copies of the contingency plan to key personnel or roles and organizational elements identified in the contingency plan. (C) The organization coordinates contingency planning activities with incident handling activities. (D) The organization reviews the contingency plan for the information system at least annually. (E) The organization updates the contingency plan to	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/ business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/ business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable organizational policies, directives and standards. In addition to information system availability, contingency plans also address other	**X**	X	X	X	X	X

				address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. (F) The organization communicates contingency plan changes to key personnel or roles and organizational elements identified in the contingency plan. (G) The organization protects the contingency plan from unauthorized disclosure and modification.	security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/ graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5.						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-2(1)	Contingency Plan	Operational	Contingency Plan | Coordinate with Related Plans	CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan development with organizational elements responsible for related plans.	Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.	**X**	X	X	X	X	X
CP-2(2)	Contingency Plan	Operational	Contingency Plan | Capacity Planning	CONTINGENCY PLAN | CAPACITY PLANNING The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber-attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/ business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					degradation into capacity planning.						
CP-2(3)	Contingency Plan	Operational	Contingency Plan | Resume Essential Missions / Business Functions	CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the resumption of essential missions and business functions within 24 hours of contingency plan activation.	Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/ extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CP-2(4)	Contingency Plan	Operational	Contingency Plan | Resume All Missions / Business Functions	CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS The organization plans for the resumption of all missions and business functions within organization-defined time period of contingency plan activation.	Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/ extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.	**X**				X	X
CP-2(5)	Contingency Plan	Operational	Contingency Plan | Continue Essential Missions / Business Functions	CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the	**X**				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.						
CP-2(6)	Contingency Plan	Operational	Contingency Plan | Alternate Processing / Storage Site	CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites.	Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.	X				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-2(8)	Contingency Plan	Operational	Contingency Plan | Identify Critical Assets	CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS The organization identifies critical information system assets supporting essential missions and business functions.	Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/ business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/ or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CP-3	Contingency Training	Operational	Contingency Training	(A) The organization provides contingency training to information system users consistent with assigned roles and responsibilities within 10 days of assuming a contingency role or responsibility. (B) The organization provides contingency training to information system users consistent with assigned roles and responsibilities when required by information system changes. (C) The organization provides contingency training to information system users consistent with assigned roles and responsibilities at least annually.	Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other entities for purposes of coordination on contingency-related activities. Training for	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2						
CP-4	Contingency Plan Testing and Exercises	Operational	Contingency Plan Testing	(A) The organization tests the contingency plan for the information system at least annually for moderate impact systems; at least every three years for low impact systems using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan. (B) The organization reviews the contingency plan test results. (C) The organization initiates corrective actions, if needed.	Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3						
CP-4(1)	Contingency Plan Testing and Exercises	Operational	Contingency Plan Testing | Coordinate with Related Plans	CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan testing with organizational elements responsible for related plans.	Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Business Recovery Plans, Incident Response Plans, and Emergency Action Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related control: IR-8.						
CP-4(2)	Contingency Plan Testing and Exercises	Operational	Contingency Plan Testing | Alternate Processing Site	CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE (a) The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources; and (b) The organization tests the contingency plan at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations.	Related control: CP-7.	X				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-6	Alternate Storage Site	Operational	Alternate Storage Site	(A) The organization establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information. (B) The organization ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/ retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CP-6(1)	Alternate Storage Site	Operational	Alternate Storage Site | Separation from Primary Site	ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant. Related control: RA-3.	**X**	X	X	X	X	X
CP-6(2)	Alternate Storage Site	Operational	Alternate Storage Site | Recovery Times / Point Objectives	ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.		**X**				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-6(3)	Alternate Storage Site	Operational	Alternate Storage Site | Accessibility	ALTERNATE STORAGE SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.	X	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-7	Alternate Processing Site	Operational	Alternative Processing Site	(A) The organization establishes an alternate processing site including necessary agreements to permit the transfer and resumption of organization-defined information system operations for essential missions/business functions within organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable. (B) The organization ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption. (C) The organization ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.	Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					CP-6, CP-8, CP-9, CP-10, MA-6						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CP-7(1)	Alternate Processing Site	Operational	Alternative Processing Site | Separation from Primary Site	ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant. Related control: RA-3.	**X**	X	X	X	X	X
CP-7(2)	Alternate Processing Site	Operational	Alternative Processing Site | Accessibility	ALTERNATE PROCESSING SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					assessments of risk. Related control: RA-3.						
CP-7(3)	Alternate Processing Site	Operational	Alternative Processing Site | Priority of Service	ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).	Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.	**X**	X	X	X	X	X
CP-7(4)	Alternate Processing Site	Operational	Alternative Processing Site | Preparation for Use	ALTERNATE PROCESSING SITE | PREPARATION FOR USE The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.	Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in	**X**				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					place. Related controls: CM-2, CM-6.						
CP-8	Telecommunications Services	Operational	Telecommunications Services	(A) The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of all information system operations covered by the contingency plan (CP-2) for essential missions and business functions within the recovery time objectives specified in the service agreement when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-8(1)	Telecommunications Services	Operational	Telecommunications Services | Priority of Service Provisions	TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS (a) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and (b) The organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.	**X**	X	X	X	X	X
CP-8(2)	Telecommunications Services	Operational	Telecommunications Services | Single Points of Failure	TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.		**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-8(3)	Telecommunications Services	Operational	Telecommunications Services | Separation of Primary / Alternate Providers	TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.	Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/ commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.	X				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CP-8(5)	Telecommunications Services	Operational	Telecommunications Services | Alternate Telecommunication Service Testing	TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING The organization tests alternate telecommunication services at least annually.		**X**				X	X
CP-9	Information System Backup	Operational	Information System Backup	(A) The organization conducts backups of user-level information contained in the information system daily incremental; weekly full. (B) The organization conducts backups of system-level information contained in the information system daily incremental; weekly full. (C) The organization conducts backups of information system documentation including security-related documentation daily incremental; weekly full. (D) The organization protects the confidentiality, integrity, and availability of backup information at storage locations. (AA) The organization determines retention periods for essential business	System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				information and archived backups.	requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13						
CP-9(1)	Information System Backup	Operational	Information System Backup | Testing for Reliability / Integrity	INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY The organization tests backup information at least annually to verify media reliability and information integrity.	Related control: CP-4.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
CP-9(2)	Information System Backup	Operational	Information System Backup | Test Restoration using Sampling	INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	Related control: CP-4.	**X**				X	X
CP-9(3)	Information System Backup	Operational	Information System Backup | Separate Storage for Critical Information	INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION The organization stores backup copies of all operating system and critical software code in a separate facility or in a fire-rated container that is not collocated with the operational system.	Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-9(5)	Information System Backup	Operational	Information System Backup | Transfer to Alternate Storage Site	INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE The organization transfers information system backup information to the alternate storage site at organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives.	Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.	X				X	X
CP-9(7)	Information System Backup	Operational	Information System Backup | Dual Authorization	INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION The organization enforces dual authorization for the deletion or destruction of organization-defined backup information.	Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/ destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.	X				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
CP-10	Information System Recovery and Reconstitution	Operational	Information System Recovery and Reconstitution	(A) The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-4, CP-6, CP-7, CP-9, SC-24						
CP-10(2)	Information System Recovery and Reconstitution	Operational	Information System Recovery and Reconstitution | Transaction Recovery	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY The information system implements transaction recovery for systems that are transaction-based.	Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					transaction rollback and transaction journaling.						
CP-10(4)	Information System Recovery and Reconstitution	Operational	Information System Recovery and Reconstitution | Restore within Time Period	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD The organization provides the capability to restore information system components within organization-defined restoration time-periods from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Restoration of information system components includes, for example, re-imaging which restores components to known, operational states. Related control: CM-2.	**X**				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-1	Identification and Authentication Policy and Procedures	Technical	Identification and Authentication Policy and Procedures	(A) The organization Develops, documents, and disseminates to all personnel: (a) An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. (B) The organization Reviews and updates the current: (a) Identification and authentication policy at least every 3 years; and (b) Identification and authentication procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable organizational policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					key factor in establishing policy and procedures.						

IA-2	Identification and Authentication (Organizational Users)	Technical	Identification and Authentication (Organizational Users)	(A) The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case of multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational	**X**	X	X	X	X	

					information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted VPNs for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems						

					gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and identity smart cards. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-2(1)	Identification and Authentication (Organizational Users)	Technical	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to privileged accounts.	Related control: AC-6.	**X**	X	X	X	X	
IA-2(3)	Identification and Authentication (Organizational Users)	Technical	Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts	IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to privileged accounts.	Related control: AC-6.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-2(6)	Identification and Authentication (Organizational Users)	Technical	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Separate Device	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets the requirements identified in CCCS ITSP.30.031.	Related control: AC-6.	**X**				X	X
IA-2(8)	Identification and Authentication (Organizational Users)	Technical	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant	IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
IA-2(11)	Identification and Authentication (Organizational Users)	Technical	Identification and Authentication (Organizational Users) | Remote Access - Separate Device	IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system being accessed and the device meets the requirements in CCCS's ITSP.30.031.	For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system being accessed as one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-3	Device Identification and Authentication	Technical	Device Identification and Authentication	(A) The information system uniquely identifies and authenticates organization-defined specific and/or types of devices before establishing network connections.	Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and EAP, Radius server with EAP-TLS authentication, Kerberos) to identify/ authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-4	Identifier Management	Technical	Identifier Management	(A) The organization manages information system identifiers by receiving authorization from organization-defined personnel or roles to assign an individual, group, role, or device identifier. (B) The organization manages information system identifiers by selecting an identifier that identifies an individual, group, role, or device. (C) The organization manages information system identifiers by assigning the identifier to the intended individual, group, role, or device. (D) The organization manages information system identifiers by preventing reuse of identifiers for at least two years. (E) The organization manages information system identifiers by disabling the identifier after 90 days for user identifiers.	Common device identifiers include, for example, MAC, IP addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37						
IA-4(2)	Identifier Management	Technical	Identifier Management | Supervisor Authorization	IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION The organization requires that the registration process to receive an individual identifier includes supervisor authorization.		X				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
IA-4(3)	Identifier Management	Technical	Identifier Management | Multiple Forms of Certification	IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.	Requiring multiple forms of identification reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries.	X				X	X
IA-4(4)	Identifier Management	Technical	Identifier Management | Identify User Status	IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS The organization manages individual identifiers by uniquely identifying each individual as employee, integrees, foreign nationals, or contractors.	Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful to know that one of the individuals on an email message is from an external organization. Related control: AT-2.	X	X	X	X	X	X

IA-5	Authenticator Management	Technical	Authenticator Management	(A) The organization manages information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator. (B) The organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization. (C) The organization manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use. (D) The organization manages information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. (E) The organization manages information system authenticators by changing the default content of authenticators prior to information system installation. (F) The organization manages information system authenticators by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators. (G) The organization	Individual authenticators include, for example, passwords, tokens, biometrics, Public Key Infrastructure (PKI) certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual	**X**	X	X	X	X	X

				manages information system authenticators by changing/ refreshing authenticators in accordance with CCCS's ITSP.30.031. (H) The organization manages information system authenticators by protecting authenticator content from unauthorized disclosure and modification. (I) The organization manages information system authenticators by requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators. (J) The organization manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes.	authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28						

IA-5(1)	Authenticator Management	Technical	Authenticator Management | Password-Based Authentication	AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION (a) The information system, for password-based authentication, enforces minimum password complexity of case sensitive, minimum of eight characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters; (b) The information system, for password-based authentication, enforces that at least one of the characters are changed when new passwords are created; (c) The information system, for password-based authentication, stores and transmits only cryptographically-protected passwords; (d) The information system, for password-based authentication, enforces password minimum and maximum lifetime restrictions of one-day minimum, sixty-day maximum; (e) The information system, for password-based authentication prohibits password reuse for 24 generations; and (f) The information system, for password-based authentication allows the use of a temporary password for system logons with an immediate change to a permanent password.	This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-5(2)	Authenticator Management	Technical	Authenticator Management | PKI-Based Authentication	AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION (a) The information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) The information system, for PKI-based authentication, enforces authorized access to the corresponding private key; (c) The information system, for PKI-based authentication, maps the authenticated identity to the account of the individual or group; and (d) The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. Related control: IA-6.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-5(3)	Authenticator Management	Technical	Authenticator Management | In-Person or Trusted Third-Party Registration	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION The organization requires that the registration process to receive be conducted in person before an organization-defined registration authority with authorization by organization- defined personnel or roles.		**X**	X	X	X	X	X
IA-5(4)	Authenticator Management	Technical	Authenticator Management | Automated Support for Password Strength Determination	AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy password length, complexity, rotation and lifetime restrictions established by IA-5(1).	This control enhancement focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems in IA-5 (1). Related controls: CA-2, CA-7, RA-5.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-5(6)	Authenticator Management	Technical	Authenticator Management | Protection of Authenticators	AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.	**X**	X	X	X	X	X
IA-5(7)	Authenticator Management	Technical	Authenticator Management | No Embedded Unencrypted Static Authenticators	AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
IA-5(8)	Authenticator Management	Technical	Authenticator Management | Multiple Information System Accounts	AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS The organization implements organization-defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.	When individuals have accounts on multiple information systems, there is the risk that the compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include, for example: (i) having different authenticators on all systems; (ii) employing some form of single sign-on mechanism; or (iii) including some form of one-time passwords on all systems.	**X**				X	X
IA-5(11)	Authenticator Management	Technical	Authenticator Management | Hardware Token-Based Authentication	AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION The information system, for hardware token-based authentication, employs mechanisms that satisfy CCCS's ITSP.30.031 token quality requirements.	Hardware token-based authentication typically refers to the use of PKI-based tokens.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-6	Authenticator Feedback	Technical	Authenticator Feedback	(A) The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. Related control: PE-18						
IA-7	Cryptographic Module Authentication	Technical	Cryptographic Module Authentication	(A) The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable organizational policies, directives, and standards for such authentication.	Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IA-8	Identification and Authentication (Non-Organizational Users)	Technical	Identification and Authentication (Non-Organizational Users)	(A) The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. Authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-1	Incident Response Policy and Procedures	Operational	Incident Response Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with incident management responsibilities: (a) An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the incident response policy and associated incident response controls. (B) The organization reviews and updates the current: (a) Incident response policy at least every 3 years; and (b) Incident response procedure at least annually. (AA) The organization's incident response policy and procedures facilitate the incorporation of heightened levels of readiness during emergency and heightened IT threat situations.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable organizational policies, directives, and standards. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizational risk management strategy is a key factor in establishing policy and procedures.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-2	Incident Response Training	Operational	Incident Response Training	(A) The organization provides incident response training to information system users consistent with assigned roles and responsibilities within 30 days of assuming an incident response role or responsibility. (B) The organization provides incident response training to information system users consistent with assigned roles and responsibilities when required by information system changes. (C) The organization provides incident response training to information system users consistent with assigned roles and responsibilities at least annually.	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-3	Incident Response Testing and Exercises	Operational	Incident Response Testing	(A) The organization tests the incident response capability for the information system at least annually using tests and exercises defined in NIST SP 800-61 to determine the incident response effectiveness and documents the results.	Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8	**X**	X	X	X	X	X
IR-3(2)	Incident Response Testing and Exercises	Operational	Incident Response Testing | Coordination with Related Plans	INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS The organization coordinates incident response testing with organizational elements responsible for related plans.	Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans,	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					Critical Infrastructure Plans, and Occupant Emergency Plans.						
IR-4	Incident Handling	Operational	Incident Handling	(A) The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. (B) The organization coordinates incident handling activities with contingency planning activities. (C) The organization incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/ business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7						
IR-4(1)	Incident Handling	Operational	Incident Handling | Automated Incident Handling Processes	INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process.	Automated mechanisms supporting incident handling processes include, for example, online incident management systems.	**X**	X	X	X		

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-4(3)	Incident Handling	Operational	Incident Handling | Continuity of Operations	INCIDENT HANDLING | CONTINUITY OF OPERATIONS The organization identifies organization-defined classes of incidents and actions to take in response to classes of incidents to ensure continuation of organizational missions and business functions.	Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, information system shutdown, fall back to manual mode/ alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack.	**X**				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-5	Incident Monitoring	Operational	Incident Monitoring	(A) The organization tracks and documents information system security incidents.	Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7	**X**	X	X	X	X	X
IR-6	Incident Reporting	Operational	Incident Reporting	(A) The organization requires personnel to report suspected security incidents to the organizational incident response capability within 2 hours. (B) The organization reports security incident information to organization-defined authorities.	The intent of this control is to address specific incident reporting requirements within an organization and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable organizational policies, directives and standards. Related controls: IR-4, IR-5, IR-8						
IR-6(1)	Incident Reporting	Operational	Incident Reporting | Automated Reporting	INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents.	Related control: IR-7.	**X**	X	X	X	X	X
IR-7	Incident Response Assistance	Operational	Incident Response Assistance	(A) The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-7(1)	Incident Response Assistance	Operational	Incident Response Assistance | Automation Support for Availability of Information / Support	INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response-related information and support.	Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	**X**	X	X	X	X	X
IR-7(2)	Incident Response Assistance	Operational	Incident Response Assistance | Coordination with External Providers	INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS (a) The organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) The organization identifies organizational incident response team members to the external providers.	External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.	**X**	X	X	X	X	X

IR-8	Incident Response Plan	Operational	Incident Response Plan	(A) The organization develops an incident response plan that: (a) Provides the organization with a roadmap for implementing its incident response capability; (b) Describes the structure and organization of the incident response capability; (c) Provides a high-level approach for how the incident response capability fits into the overall organization; (d) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; (e) Defines reportable incidents; (f) Provides metrics for measuring the incident response capability within the organization; (g) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and (h) Is reviewed and approved by organization-defined personnel or roles. (B) The organization distributes copies of the incident response plan to all personnel with a role or responsibility for implementing the incident response plan. (C) The organization reviews the incident response plan at least annually incorporating lessons from past incidents. (D) The organization updates	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5	**X**	X	X	X	X	X

				the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. (E) The organization communicates incident response plan changes to all personnel with a role or responsibility for implementing the incident response plan. (F) The organization protects the incident response plan from unauthorized disclosure and modification.								

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-9	Information Spillage Response	Operational	Information Spillage Response	(A) The organization responds to information spills by identifying the specific information involved in the information system contamination. (B) The organization responds to information spills by alerting incident response personnel as documented within the Incident Management Plan of the information spill using a method of communication not associated with the spill. (C) The organization responds to information spills by isolating the contaminated information system or system component. (D) The organization responds to information spills by eradicating the information from the contaminated information system or component. (E) The organization responds to information spills by identifying other information systems or system components that may have been subsequently contaminated. (F) The organization	Information spillage refers to instances where sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				responds to information spills by performing other actions documented within the Incident Managment Plan.	contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-9(1)	Information Spillage Response	Operational	Information Spillage Response | Responsible Personnel	INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL The organization assigns incident response personnel as documented within the Incident Management Plan with responsibility for responding to information spills.		**X**	X	X	X	X	X
IR-9(2)	Information Spillage Response	Operational	Information Spillage Response | Training	INFORMATION SPILLAGE RESPONSE | TRAINING The organization provides information spillage response training annually.		**X**	X	X	X	X	X
IR-9(3)	Information Spillage Response	Operational	Information Spillage Response | Post-Spill Operations	INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS The organization implements organization-defined procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	Corrective actions for information systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
IR-9(4)	Information Spillage Response	Operational	Information Spillage Response | Exposure to Unauthorized Personnel	INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL The organization employs organization-defined security safeguards for personnel exposed to information not within assigned access authorizations.	Security safeguards include, for example, making personnel exposed to spilled information aware of the organizational policies, directives and standards regarding the information and the restrictions imposed based on exposure to such information	**X**	X	X	X	X	X
MA-1	System Maintenance Policy and Procedures	Operational	System Maintenance Policy and Procedures	(A) The organization develops, documents, and disseminates to all personnel: (a) A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. (B) The organization reviews and updates the current: (a) System maintenance policy at least every 3 years; and (b) System maintenance procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable organizational policies, directives and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures						

MA-2	Controlled Maintenance	Operational	Controlled Maintenance	(A) The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements. (B) The organization approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. (C) The organization requires that organization-defined personnel or roles explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs. (D) The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. (E) The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. (F) The organization include date and time of maintenance, name of the individual performing the maintenance; name of escort (if applicable), description of the maintenance performed;	This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider	**X**	X	X	X	X	

				equipment removed or replaced (including identification numbers, if applicable) in organizational maintenance records.	supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MA-3	Maintenance Tools	Operational	Maintenance Tools	(A) The organization approves, controls, and monitors information system maintenance tools.	This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, such as the software implementing "ping," "ls," "ipconfig," or the hardware	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6						
MA-3(1)	Maintenance Tools	Operational	Maintenance Tools | Inspect Tools	MAINTENANCE TOOLS | INSPECT TOOLS The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/ unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MA-3(2)	Maintenance Tools	Operational	Maintenance Tools | Inspect Media	MAINTENANCE TOOLS | INSPECT MEDIA The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.	**X**	X	X	X	X	
MA-3(3)	Maintenance Tools	Operational	Maintenance Tools | Prevent Unauthorized Removal	MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from the information owner explicitly authorizing removal of the equipment from the facility.	Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
MA-4	Non-Local Maintenance	Operational	Nonlocal Maintenance	(A) The organization approves and monitors nonlocal maintenance and diagnostic activities. (B) The organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan for the information system. (C) The organization employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. (D) The organization maintains records for nonlocal maintenance and diagnostic activities.	Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					biometric. Enforcing requirements in MA-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17						
MA-4(1)	Non-Local Maintenance	Operational	Nonlocal Maintenance | Auditing and Review	NONLOCAL MAINTENANCE | AUDITING AND REVIEW (a) The organization audits nonlocal maintenance and diagnostic sessions as defined in the organizations formal audit policy (AU-2, AU-6, AU-12); and (b) The organization reviews the records of the maintenance and diagnostic sessions.	Related controls: AU-2, AU-6, AU-12.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MA-4(2)	Non-Local Maintenance	Operational	Nonlocal Maintenance | Document Nonlocal Maintenance	NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.		**X**	X	X	X	X	
MA-4(3)	Non-Local Maintenance	Operational	Nonlocal Maintenance | Comparable Security / Sanitization	NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION (a) The organization requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) The organization removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the	Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				component (with regard to potentially malicious software) before reconnecting the component to the information system.							
MA-4(6)	Non-Local Maintenance	Operational	Nonlocal Maintenance | Cryptographic Protection	NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.	Related controls: SC-8, SC-13.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MA-5	Maintenance Personnel	Operational	Maintenance Personnel	(A) The organization establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel. (B) The organization ensures that non-escorted personnel performing maintenance on the information system have required access authorizations. (C) The organization designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example,	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3						

MA-5(1)	Maintenance Personnel	Operational	Maintenance Personnel | Individuals without Appropriate Access	MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS (a) The organization implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not Canadian citizens, that include the following requirements: - Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; - Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured; and (b) The organization develops and implements alternate security safeguards in the event an information system	This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not Canadian citizens, visual and electronic access to any sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2.	**X**	X	X	X	X	

				component cannot be sanitized, removed, or disconnected from the system.							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MA-6	Timely Maintenance	Operational	Timely Maintenance	(A) The organization obtains maintenance support and/or spare parts for all system components requiring vendor support and/or spare parts as needed to support availability commitments.	Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or Canada when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-1	Media Protection Policy and Procedures	Operational	Media Protection Policy and Procedures	(A) The organization develops, documents, and disseminates to all personnel: (a) A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the media protection policy and associated media protection controls. (B) The organization reviews and updates the current: (a) Media protection policy at least every 3 years; and (b) Media protection procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. The media protection policy and procedures reflect applicable organizational policies, directives and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizational risk management strategy is a key factor in establishing policy and procedures						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
MP-2	Media Access	Operational	Media Access	(A) The organization restricts access to all types of digital and/or non-digital media containing information not cleared for public release	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2	X	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-3	Media Marking	Operational	Media Marking	(A) The organization marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. (B) The organization exempt no removable media types from marking as long as the media remain within organization-defined controlled areas.	The term security marking refers to the application/use of human-readable security attributes. The term security labelling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					information indicating that the information is publicly releasable. Marking of information system media reflects applicable organizational policies, directives and standards. Related controls: AC-16, PL-2, RA-3						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-4	Media Storage	Operational	Media Storage	(A) The organization physically controls and securely stores all types of digital and non-digital media with sensitive informatio within organization-defined controlled areas and in accordance with organizational policies and standards. (B) The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizational operations and assets, individuals, other organizations, or Canada if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3						

MP-5	Media Transport	Operational	Media Transport	(A) The organization protects and controls all media with sensitive information during transport outside of controlled areas using organization-defined security safeguards in accordance with organizational policies and standards. (B) The organization maintains accountability for information system media during transport outside of controlled areas. (C) The organization documents activities associated with the transport of information system media. (D) The organization restricts the activities associated with the transport of information system media to authorized personnel.	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media and consistent with organizational policies, directives and standards. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide	**X**	X	X	X	X	X

					confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., Canada Post or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the						

					different types of media transport as part of an overall system of transport-related records. Related controls: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.							

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
MP-5(4)	Media Transport	Operational	Media Transport | Cryptographic Protection	MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms compliant with the requirements of Control SC-13 to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). Related control: SC-13.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-6	Media Sanitization	Operational	Media Sanitization	(A) The organization sanitize organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable organizational policies and standards. (B) The organization employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. Related controls: MA-2, MA-4, RA-3, SC-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-6(1)	Media Sanitization	Operational	Media Sanitization | Review / Approve / Track / Document / Verify	MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.	Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.	**X**	X	X	X	X	X
MP-6(2)	Media Sanitization	Operational	Media Sanitization | Equipment Testing	MEDIA SANITIZATION | EQUIPMENT TESTING The organization tests sanitization equipment and procedures at least annually to verify that the intended sanitization is being achieved.	Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					agencies or external service providers).						
MP-6(3)	Media Sanitization	Operational	Media Sanitization | Non-destructive Techniques	MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES The organization applies non-destructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under organization-defined circumstances requiring sanitization of portable storage devices.	This control enhancement applies to digital media containing sensitive information. Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider non-destructive	X				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-7	Media Use	Operational	Media Use	(A) The organization prohibits the use of unauthorized removable media on all components using technical safeguards.	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/ removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behaviour) to restrict the use of information system media. Organizations may	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-7(1)	Media Use	Operational	Media Use | Prohibit Use without Owner	MEDIA USE | PROHIBIT USE WITHOUT OWNER The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
MP-8	Media Downgrading	Operational	Media Downgrading	(A) The organization establishes organization-defined information system media downgrading process that includes employing downgrading mechanisms with organization-defined strength and integrity. (B) The organization ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information. (C) The organization identifies organization-defined information system media requiring downgrading. (D) The organization downgrades the identified information system media using the established process.	This control applies to all information system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information	**X**				X	X
MP-8(1)	Media Downgrading	Operational	Media Downgrading | Documentation of Process	MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS The organization documents information system media downgrading actions.	Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of	**X**				X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.						
PE-1	Physical and Environmental Protection Policy and Procedures	Operational	Physical and Environmental Protection Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with physical and environmental protection responsibilities: (a) A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. (B) The organization reviews and updates the current: (a) Physical and environmental protection policy at least every 3 years; and (b) Physical and	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. The physical and environmental protection policy and procedures reflect applicable organizational policies, directives, and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				environmental protection procedures at least annually.	procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
PE-2	Physical Access Authorizations	Operational	Physical Access Authorizations	(A) The organization develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides. (B) The organization issues authorization credentials for facility access. (C) The organization reviews the access list detailing authorized facility access by individuals at least annually. (D) The organization removes individuals from the facility access list when access is no longer required.	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with organizational directives, standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3	X	X				

PE-3	Physical Access Control	Operational	Physical Access Control	(A) The organization enforces physical access authorizations at all physical access points to the facility by: (a) Verifying individual access authorizations before granting access to the facility; and (b) Controlling ingress/egress to the facility using controlled areas that meet the requirements of the GC Industrial Security Program; (B) The organization maintains physical access audit logs for all physical access points to the facility. (C) The organization provides organization-defined security safeguards to control access to areas within the facility officially designated as publicly accessible. (D) The organization escorts visitors and monitors visitor activity at all times while in the data center. (E) The organization secures keys, combinations, and other physical access devices. (F) The organization inventories organization-defined physical access devices at least annually. (G) The organization changes combinations and keys at least annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	Control of access to restricted-access areas and other organizational space is to be provided in a manner which does not contravene the applicable life safety requirements of building codes, fire codes and related codes, standards and guidelines. This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable organizational policies, directives, and standards.	**X**	X				

					Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated, or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-3(1)	Physical Access Control	Operational	Physical Access Control | Information System Access	PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at organization-defined physical spaces containing one or more components of the information system.	This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, and data and communications centres). Related control: PS-2.	**X**	X				
PE-4	Access Control for Transmission Medium	Operational	Access Control for Transmission Medium	(A) The organization controls physical access to all distribution and transmission lines within organizational facilities using in accordance with, or uses an adequate risk-based approach aligned with the practices with TBS and RCMP physical security standards.	Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii)	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8						
PE-5	Access Control for Output Devices	Operational	Access Control for Output Devices	(A) The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-6	Monitoring Physical Access	Operational	Monitoring Physical Access	(A) The organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents. (B) The organization reviews physical access logs at least monthly and upon occurrence of organization-defined events or potential indications of events. (C) The organization coordinates results of reviews and investigations with the organizational incident response capability.	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8	**X**	X				
PE-6(1)	Monitoring Physical Access	Operational	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment	MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT The organization monitors physical intrusion alarms and surveillance equipment.		**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-6(4)	Monitoring Physical Access	Operational	Monitoring Physical Access | Monitoring Physical Access to Information Systems	MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as identified under PE-3(1).	This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centres). Related controls: PS-2, PS-3.	**X**	X				
PE-8	Access Records	Operational	Visitor Access Records	(A) The organization maintains visitor access records to the facility where the information system resides for at least 1 year; and (B) The organization reviews visitor access records at least monthly.	Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-9	Power Equipment and Power Cabling	Operational	Power Equipment and Cabling	(A) The organization protects power equipment and power cabling for the information system from damage and destruction.	Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data centre, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4	**X**	X				
PE-10	Emergency Shutoff	Operational	Emergency Shutoff	(A) The organization provides the capability of shutting off power to the information system or individual system components in emergency situations. (B) The organization places emergency shutoff switches or devices in organization-defined location by information system or system component to facilitate safe and easy access for personnel.	This control applies primarily to facilities containing concentrations of information system resources including, for example, data centres, server rooms, and mainframe computer rooms. Related control: PE-15	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				(C) The organization protects emergency power shutoff capability from unauthorized activation.							
PE-11	Emergency Power	Operational	Emergency Power	(A) The organization provides a short-term uninterruptible power supply to facilitate transition of the information system to long-term alternate power in the event of a primary power source loss.	Related controls: AT-3, CP-2, CP-7	**X**	X				
PE-12	Emergency Lighting	Operational	Emergency Lighting	(A) The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	This control applies primarily to facilities containing concentrations of information system resources including, for example, data centres, server rooms, and mainframe computer rooms. Related controls: CP-2, CP-7	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-13	Fire Protection	Operational	Fire Protection	(A) The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	This control applies primarily to facilities containing concentrations of information system resources including, for example, data centres, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors	**X**	X				
PE-13(2)	Fire Protection	Operational	Fire Protection | Suppression Devices / Systems	FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined personnel or roles and local fire department.	Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-13(3)	Fire Protection	Operational	Fire Protection | Automatic Fire Suppression	FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.		**X**	X				
PE-14	Temperature and Humidity Controls	Operational	Temperature and Humidity Controls	(A) The organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels. (B) The organization monitors temperature and humidity levels continuously.	This control applies primarily to facilities containing concentrations of information system resources, for example, data centres, server rooms, and mainframe computer rooms. Related control: AT-3	**X**	X				
PE-14(2)	Temperature and Humidity Controls	Operational	Temperature and Humidity Controls | Monitoring with Alarms / Notifications	TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.		**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PE-15	Water Damage Protection	Operational	Water Damage Protection	(A) The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	This control applies primarily to facilities containing concentrations of information system resources including, for example, data centres, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations. Related control: AT-3	**X**	X				
PE-16	Delivery and Removal	Operational	Delivery and Removal	(A) The organization authorizes, monitors, and controls all information system components entering and exiting the facility and maintains records of those items.	Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Related controls: CM-3, MA-2, MA-3, MP-5, SA-12	**X**	X				

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
PE-17	Alternate Work Site	Operational	Alternate Work Site	(A) The organization employs security controls commensurate with that of the primary site at alternate work sites. (B) The organization assesses as feasible, the effectiveness of security controls at alternate work sites. (C) The organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.	While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. Related controls: AC-17, CP-7	X	X				

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
PL-1	Security Planning Policy and Procedures	Management	Security Planning Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with security planning responsibilities (a) A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the security planning policy and associated security planning controls. (B) The organization reviews and updates the current: (a) Security planning policy at least every 3 years; and (b) Security planning procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. The security planning policy and procedures reflect organizational policies, directives, and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					management strategy is a key factor in establishing policy and procedures						

PL-2	System Security Plan	Management	System Security Plan	(A) The organization develops a security plan for the information system that: (a) Is consistent with the organization's enterprise architecture; (b) Explicitly defines the authorization boundary for the system; (c) Describes the operational context of the information system in terms of missions and business processes; (d) Provides the security categorization of the information system including supporting rationale; (e) Describes the operational environment for the information system and relationships with or connections to other information systems; (f) Provides an overview of the security requirements for the system; (g) Identifies any relevant overlays, if applicable; (h) Describes the security controls in place or planned for meeting those requirements including a rationale for tailoring decisions; and (i) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation. (B) The organization distributes copies of the security plan and communicates subsequent changes to the plan to personnel or roles with security planning	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals and other organizations. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where	**X**	X	X	X	X	X

				responsibilities. (C) The organization reviews the security plan for the information system at least annually. (D) The organization updates the plan to address changes to the information system/ environment of operation or problems identified during plan implementation or security control assessments. (E) The organization protects the security plan from unauthorized disclosure and modification.	more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, SA-5, SA-17.					

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PL-2(3)	System Security Plan	Management	System Security Plan | Plan / Coordinate with Other Organizational Entities	SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES The organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities.	Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and non-emergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PL-4	Rules of Behaviour	Management	Rules of Behavior	(A) The organization establishes and makes readily available to individuals requiring access to the information system the rules that describe their responsibilities and expected behaviour with regard to information and information system usage. (B) The organization receives a signed acknowledgment from such individuals, indicating that they have read, understood, and agreed to abide by the rules of behaviour, before authorizing access to information and the information system. (C) The organization reviews and updates the rules of behaviour at least every 3 years. (D) The organization requires individuals who have signed a previous version of the rules of behaviour to read and resign when the rules of behaviour are revised/ updated.	This control enhancement applies to organizational users. Organizations consider rules of behaviour based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behaviour for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behaviour for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behaviour. Organizations can use electronic signatures for acknowledging rules of behaviour. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PL-4(1)	Rules of Behaviour	Management	Rules of Behavior | Social Media and Networking Restrictions	RULES OF BEHAVIOUR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS The organization includes in the rules of behaviour, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	This control enhancement addresses rules of behaviour related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/ networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.	**X**	X	X	X	X	X

PL-8	Information Security Architecture	Management	Information System Architecture	(A) The organization develops an information security architecture for the information system that: (a) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; (b) Describes how the information security architecture is integrated into and supports the enterprise architecture; and (c) Describes any information security assumptions about and dependencies on, external services. (B) The organization reviews and updates the information security architecture at least annually or when changes to the information system or its environment warrant to reflect updates in the enterprise architecture. (C) The organization ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/ acquisitions.	This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture, which is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other	**X**	X	X	X	X	

					specific protection needs. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/ business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational information systems is critical to implementing and maintaining effective information security architecture. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information						

					technology product/ system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, SA-5, SA-17						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
PS-1	Personnel Security Policy and Procedures	Operational	Personnel Security Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with personnel security responsibilities: (a) A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. (B) The organization reviews and updates the current: (a) Personnel security policy at least every 3 years; and (b) Personnel security procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. The personnel security policy and procedures reflect applicable organizational policies, directives and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					organizational risk management strategy is a key factor in establishing policy and procedures						
PS-2	Position Categorization	Operational	Position Risk Designation	(A) The organization categorizes all positions based on the injury the individuals could cause by malicious acts resulting from the privileges associated with the position. (B) The organization selects the appropriate screening for individuals filling those positions. (C) The organization reviews		**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				and revises categorizations at least annually.							
PS-3	Personnel Screening	Operational	Personnel Screening	(A) The organization screens individuals prior to authorizing access to the information system in accordance with organizational standards. (B) The organization rescreens individuals according to the TBS Standard on Security Screening and any related provisions of the Industrial Security Program.	Personnel screening and rescreening activities reflect applicable organizational policies, directives and standards, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. Related controls: AC-2, IA-4, PE-2, PS-2	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
PS-3(3)	Personnel Screening	Operational	Personnel Screening | Information with Special Protection Measures	PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: (a) Have valid access authorizations that are demonstrated by assigned official organizational duties; and (b) Satisfy the TBS Standard on Security Screening and any related provisions of the Industrial Security Program.	Organizational information requiring special protection includes, for example, Protected Information and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PS-4	Personnel Termination	Operational	Personnel Termination	(A) The organization, upon termination of individual employment disables information system access within the same day. (B) The organization, upon termination of individual employment terminates/ revokes any authenticators/ credentials associated with the individual. (C) The organization, upon termination of individual employment conducts exit interviews that include a discussion of items identified in the TBS Standard on Security Screening and any related provisions of the Industrial Security Program. (D) The organization, upon termination of individual employment retrieves all security-related organizational information system-related property. (E) The organization, upon termination of individual employment retains access to organizational information and information systems formerly controlled by terminated individual. (F) The organization, upon	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				termination of individual employment notifies terminated personnel's manager within 24 hours.	Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PS-5	Personnel Transfer	Operational	Personnel Transfer	(A) The organization reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. (B) The organization initiates reassignment of access to data within 5 days of the formal transfer action. (C) The organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. (D) The organization notifies transferring personnel's manager within 5 days.	This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					information system accounts. Related controls: AC-2, IA-4, PE-2, PS-4						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PS-6	Access Agreements	Operational	Access Agreements	(A) The organization develops and documents access agreements for organizational information systems. (B) The organization reviews and updates the access agreements at least annually. (C) The organization ensures that individuals requiring access to organizational information and information systems: (a) Sign appropriate access agreements prior to being granted access; and (b) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at least annually.	Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behaviour, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understood, and agreed to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PS-7	Third-Party Personnel Security	Operational	Third-Party Personnel Security	(A) The organization establishes personnel security control requirements including security roles and responsibilities for third-party providers. (B) The organization requires third-party providers to comply with personnel security control policies and procedures established by the organization. (C) The organization documents personnel security requirements. (D) The organization requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within organization-defined time period. (E) The organization monitors provider compliance.	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security control requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
PS-8	Personnel Sanctions	Operational	Personnel Sanctions	(A) The organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures. (B) The organization notifies organization-defined personnel or roles within one working day when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.	Organizational sanctions processes reflect applicable organizational policies, directives, and standards. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with their legal counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
RA-1	Risk Assessment Policy and Procedures	Management	Risk Assessment Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with risk assessment responsibilities: (a) A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. (B) The organization reviews and updates the current: (a) Risk assessment policy at least every 3 years; and (b) Risk assessment procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable organizational policies, directives and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					management strategy is a key factor in establishing policy and procedures.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
RA-2	Security Categorization	Management	Security Categorization	(A) The organization categorizes information and the information system. (B) The organization documents the security categorization results (including supporting rationale) in the security plan for the information system. (C) The organization ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative.	Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are compromised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/ stewards. Organizations also consider the potential adverse impacts to other organizations. Security categorization processes carried out by	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
RA-3	Risk Assessment	Management	Risk Assessment	(A) The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. (B) The organization documents risk assessment results in a security assessment report. (C) The organization reviews risk assessment results at least annually or when a significant change occurs. (D) The organization disseminates risk assessment results to organization-defined personnel or roles. (E) The organization updates the risk assessment at least every 3 years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals and other organizations based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities)Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework of ITSG-33, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation. Related controls: RA-2.						

RA-5	Vulnerability Scanning	Management	Vulnerability Scanning	(A) The organization scans for vulnerabilities in the information system and hosted applications monthly for operating systems/infrastructure, web applications, and database management systems and when new vulnerabilities potentially affecting the system/applications are identified and reported. (B) The organization employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) Enumerating platforms, software flaws, and improper configurations; (b) Formatting checklists and test procedures; and (c) Measuring vulnerability impact. (C) The organization analyzes vulnerability scan reports and results from security control assessments. (D) The organization remediates legitimate vulnerabilities within 30 days for high-risk vulnerabilities and 90 days for moderate-risk vulnerabilities from the date of discovery in accordance with an organizational assessment of risk. (E) The organization shares information obtained from the vulnerability scanning process and security control assessments with	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms	**X**	X	X	X	X	

				organization-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).								

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
RA-5(1)	Vulnerability Scanning	Management	Vulnerability Scanning | Update Tool Capability	VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.	**X**	X	X	X	X	
RA-5(2)	Vulnerability Scanning	Management	Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified	VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED The organization updates the information system vulnerabilities scanned prior to a new scan.	Related controls: SI-3, SI-5.	**X**	X	X	X	X	
RA-5(3)	Vulnerability Scanning	Management	Vulnerability Scanning | Breadth / Depth of Coverage	VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information		**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				system components scanned and vulnerabilities checked).							
RA-5(5)	Vulnerability Scanning	Management	Vulnerability Scanning | Privileged Access	VULNERABILITY SCANNING | PRIVILEGED ACCESS The information system implements privileged access authorization to operating systems, web applications, databases for selected all scans.	In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.	**X**	X	X	X	X	
RA-5(6)	Vulnerability Scanning	Management	Vulnerability Scanning | Automated Trend Analyses	VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in	Related controls: IR-4, IR-5, SI-4.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
				information system vulnerabilities.							
RA-5(8)	Vulnerability Scanning	Management	Vulnerability Scanning | Review Historic Audit Logs	VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.	Related control: AU-6.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-1	System and Services Acquisition Policy and Procedures	Management	System and Services Acquisition Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with system and services acquisition responsibilities: (a) A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. (B) The organization reviews and updates the current: (a) System and services acquisition policy at least every 3 years; and (b) System and services acquisition procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. The system and services acquisition policy and procedures reflect applicable organizational policies, directives, and standards. Security program policies and procedures at the organizational level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizational risk management strategy is a key factor in establishing policy and procedures						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-2	Allocation of Resources	Management	Allocation of Resources	(A) The organization determines information security control requirements for the information system or information system service in mission/business process planning. (B) The organization determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process. (C) The organization establishes a discrete line item for information security in organizational programming and budgeting documentation.	Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/ service.	**X**	X	X	X	X	X

SA-3	System Development Lifecycle	Management	System Development Lifecycle	(A) The organization manages the information system using organization-defined system development life cycle that incorporates information security considerations. (B) The organization defines and documents information security roles and responsibilities throughout the system development life cycle. (C) The organization identifies individuals having information security roles and responsibilities. (D) The organization integrates the organizational information security risk management process into system development life cycle activities.	A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/ business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the	**X**	X	X	X	X	

					development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/ business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, SA-8.						

SA-4	Acquisition Process	Management	Acquisition Process	(A) The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable organizational policies, directives and standards, and organizational mission/business needs: (a) Security functional requirements; (b) Security strength requirements; (c) Security assurance requirements; (d) Security-related documentation requirements; (e) Requirements for protecting security-related documentation; (f) Description of the information system development environment and environment in which the system is intended to operate; and (g) Acceptance criteria. (AA) The client organization includes security-related documentation, requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk. (BB) The client organization includes the development and evaluation-related requirements and/or specifications, explicitly or by reference, in information system acquisition contracts	Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system	**X**	X	X	X	X	

				based on an assessment of risk and in accordance with applicable organizational policies, directives and standards.	development life cycleSecurity functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings						

					specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-4(1)	Acquisition Process	Management	Acquisition Process | Functional Properties of Security Controls	ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.	**X**	X	X	X	X	
SA-4(2)	Acquisition Process	Management	Acquisition Process | Design / Implementation Information for Security Controls	ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes security-relevant external system interfaces and high-level design at organization-defined level of detail.	Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SA-4(8)	Acquisition Process	Management	Acquisition Process | Continuous Monitoring Plan	ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains at least the minimum requirement as defined in CA-7.	The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur. Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into the continuous monitoring strategies and programs implemented by organizations. Related control: CA-7.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-4(9)	Acquisition Process	Management	Acquisition Process | Functions / Ports / Protocols / Services in Use	ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.						

SA-5	Information System Documentation	Management	Information System Documentation	(A) The organization obtains administrator documentation for the information system, system component, or information system service that describes: (a) Secure configuration, installation, and operation of the system, component, or service; (b) Effective use and maintenance of security functions/mechanisms; and (c) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. (B) The organization obtains user documentation for the information system, system component, or information system service that describes: (a) User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; (b) Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and (c) User responsibilities in maintaining the security of the system, component, or service. (C) The organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent	This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system,	**X**	X	X	X	X	

				and organization-defined actions in response. (D) The organization protects documentation as required, in accordance with the risk management strategy. (E) The organization distributes documentation to developer or tester roles.	includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-8	Security Engineering Principles	Management	Security Engineering Principles	(A) The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: SA-3, SA-4, SA-17, SC-2, SC-3						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-9	External Information System Services	Management	External Information System Services	(A) The organization requires that providers of external information system services comply with organizational information security control requirements and employ applicable security controls if GC data is processed or stored within the external system. (B) The organization defines and documents government oversight and user roles and responsibilities with regard to external information system services. (C) The organization employs GC continuous monitoring strategies, processes, methods, and techniques for external systems where GC data is processed or stored to monitor security control compliance by external service providers on an ongoing basis.	External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					non-compliance. Related controls: CA-3, IR-7, PS-7						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-9(1)	External Information System Services	Management	External Information System Services | Risk Assessments / Organizational Approvals	EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS (a) The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) The organization ensures that the acquisition or outsourcing of dedicated information security services is approved by the Chief Information Officer or delegate as detailed in organizational orders.	Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3.	**X**	X	X	X	X	X
SA-9(2)	External Information System Services	Management	External Information System Services | Identification of Functions / Ports / Protocols / Services	EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES The organization requires providers of all external information systems and serviceso identify the functions, ports, protocols, and other services required for the use of such services.	Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/ protocols. Related control: CM-7.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SA-9(4)	External Information System Services	Management	External Information System Services | Consistent Interests of Consumers and Providers	EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS The organization employs organization-defined security safeguards to ensure that the interests of any external service provider that is responsible to process, transmit, or store GC information are consistent with and reflect organizational interests.	As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive experiences), and	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					conducting periodic/unscheduled visits to service provider facilities.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-9(5)	External Information System Services	Management	External Information System Services | Processing, Storage, and Service Location	EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION The organization restricts the location of information processing, information/data, and information system services to locations witihin Canada based on 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).	The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident response activities (e.g., forensic analyses, after-the-fact investigations) in case of information security breaches/compromises. Such incident response activities may be	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					adversely affected by the governing laws or protocols in the locations where processing and storage occur and/or the locations from which information system services emanate.						

SA-10	Developer Configuration Management	Management	Developer Configuration Management	(A) The organization requires the developer of the information system, system component, or information system service to perform configuration management during system, component, or service development, implementation, and operation. (B) The organization requires the developer of the information system, system component, or information system service to document, manage, and control the integrity of changes to all items under configuration management; (C) The organization requires the developer of the information system, system component, or information system service to implement only organization-approved changes to the system, component, or service; (D) The organization requires the developer of the information system, system component, or information system service to document approved changes to the system, component, or service and the potential security impacts of such changes; and (E) The organization requires the developer of the information system, system component, or information system service to track security flaws and flaw resolution within the system, component, or service and	This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/ use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data;	**X**	X	X	X	X	

				report findings to the Chief Information Officer or delegate.	implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/ firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-10(1)	Developer Configuration Management	Management	Developer Configuration Management | Software / Firmware Integrity Verification	DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.	This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components. Related control: SI-7.	**X**	X	X	X	X	

SA-11	Developer Security Testing	Management	Developer Security Testing and Evaluation	(A) The organization requires the developer of the information system, system component, or information system service to create and implement a security assessment plan. (B) The organization requires the developer of the information system, system component, or information system service to perform all testing is defined during initial phases at organization level at organization-defined depth and coverage. Further testing can be defined as required. (C) The organization requires the developer of the information system, system component, or information system service to produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation. (D) The organization requires the developer of the information system, system component, or information system service to implement a verifiable flaw remediation process. (E) The organization requires the developer of the information system, system component, or information system service to correct flaws identified during security testing/evaluation.	Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/ evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools,	**X**	X	X	X	X	

					binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigour to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigour and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/ processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection						

					requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-11(1)	Developer Security Testing	Management	Developer Security Testing and Evaluation | Static Code Analysis	DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.						
SA-11(2)	Developer Security Testing	Management	Developer Security Testing and Evaluation | Threat and Vulnerability Analyses	DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related control: RA-5.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-11(8)	Developer Security Testing	Management	Developer Security Testing and Evaluation | Dynamic Code Analysis	DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.	Dynamic code analysis provides run-time verification of software programs, using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs run-time tools to help to ensure that security functionality performs in the manner in which it was designed. A specialized type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies derive from the intended use of applications and the functional and design specifications for the applications. To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SA-15	Development Process, Standards, and Tool	Management	Development Process, Standards, and Tools	(A) The organization requires the developer of the information system, system component, or information system service to follow a documented development process that: (a) Explicitly addresses security requirements; (b) Identifies the standards and tools used in the development process; (c) Documents the specific tool options and tool configurations used in the development process; and (d) Documents, manages, and ensures the integrity of changes to the process and/ or tools used in development. (B) The organization reviews the development process, standards, tools, and tool options/configurations at least annually to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security requirements.	Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-1	System and Communications Protection Policy and Procedures	Technical	System and Communications Protection Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with system and communications protection responsibilities: (a) A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. (B) The organization reviews and updates the current: (a) System and communications protection policy at least every 3 years; and (b) System and communications protection procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. The system and communications protection policy and procedures reflect applicable organizational policies, directives, and standards. Security program policies and procedures at the organization level may make system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					needed. The organizational risk management strategy is a key factor in establishing policy and procedures						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-2	Application Partitioning	Technical	Application Partitioning	(A) The information system separates user functionality (including user interface services) from information system management functionality.	Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					(e.g., using a logical separation, web administrators would use 2-factor authentication and normal users of the web application would use username/password authentication). Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls. Related controls: SA-4, SA-8, SC-3						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-4	Information in Shared Resources	Technical	Information in Shared Resources	(A) The information system prevents unauthorized and unintended information transfer via shared system resources.	This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. Related controls: AC-3, AC-4, MP-6						
SC-5	Denial of Service Protection	Technical	Denial of Service Protection	(A) The information system protects against or limits the effects of the following denial of service attempts that attack bandwidth, transactional capacity and storage by employing geo-replication, IP address blocking, and network-based DDoS protections.	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks. Related controls: SC-6, SC-7						
SC-6	Resource Availability	Technical	Resource Availability	(A) The information system protects the availability of resources by allocating organization-defined resources by priority; quota, or organization-defined security safeguards.	Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-7	Boundary Protection	Technical	Boundary Protection	(A) The information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system. (B) The information system implements sub-networks for publicly accessible system components that are physically or logically separated from internal organizational networks. (C) The information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected sub-networks). Sub-networks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13						
SC-7(3)	Boundary Protection	Technical	Boundary Protection | Access Points	BOUNDARY PROTECTION | ACCESS POINTS The organization limits the number of external network connections to the information system.	Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					outbound communications traffic.						
SC-7(4)	Boundary Protection	Technical	Boundary Protection | External Telecommunications Services	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES (a) The organization implements a managed interface for each external telecommunication service; (b) The organization establishes a traffic flow policy for each managed interface; (c) The organization protects the confidentiality and integrity of the information being transmitted across each interface; (d) The organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) The organization reviews exceptions to the traffic flow policy at least annually and removes exceptions that are no longer supported by an explicit mission/business need.	Related control: SC-8.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SC-7(5)	Boundary Protection	Technical	Boundary Protection | Deny by Default / Allow by Exception	BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-7(7)	Boundary Protection	Technical	Boundary Protection | Prevent Split Tunneling for Remote Devices	BOUNDARY PROTECTION | PREVENT SPLIT TUNNELLING FOR REMOTE DEVICES The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunnelling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunnelling (or of configuration settings that allow split tunnelling) in the remote device, and by prohibiting the connection if the remote device is using split tunnelling. Split tunnelling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunnelling would in effect allow unauthorized external connections, making the system more vulnerable to	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunnelling.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-7(8)	Boundary Protection	Technical	Boundary Protection | Route Traffic to Authenticated Proxy Servers	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS The information system routes organization-defined internal communications traffic to all untrusted networks ouside the control of the organization through authenticated proxy servers at managed interfaces.	External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.						
SC-7(12)	Boundary Protection	Technical	Boundary Protection | Host-Based Protection	BOUNDARY PROTECTION | HOST-BASED PROTECTION The organization implements organization-defined host-based boundary protection mechanisms at organization-defined information system components.	Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SC-7(13)	Boundary Protection	Technical	Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS The organization isolates organization-defined information security tools, mechanisms, and support components from other internal information system components by implementing physically separate sub-networks with managed interfaces to other components of the system.	Separate sub-networks with managed interfaces are useful, for example, in isolating computer network defences from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques of organizations. The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets. Related controls: SA-8, SC-2, SC-3.	X	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SC-7(18)	Boundary Protection	Technical	Boundary Protection | Fail Secure	BOUNDARY PROTECTION | FAIL SECURE The information system fails securely in the event of an operational failure of a boundary protection device.	Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected sub-networks commonly referred to as demilitarized zones), information systems do not enter into insecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases. Related controls: CP-2, SC-24.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-8	Transmission Confidentiality and Integrity	Technical	Transmission Confidentiality and Integrity	(A) The information system protects the confidentiality and integrity of transmitted information.	This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4					

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-8(1)	Transmission Confidentiality and Integrity	Technical	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by 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. The cryptography must be compliant with the requirements of control SC-13.	Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-10	Network Disconnect	Technical	Network Disconnect	(A) The information system terminates the network connection associated with a communications session at the end of the session or after no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions of inactivity.	This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-12	Cryptographic Key Establishment and Management	Technical	Cryptographic Key Establishment and Management	(A) The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with CSE-approved cryptography.	Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable organizational policies, directives, and standards, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. The cryptography must be compliant with the requirements of control SC-13. Related controls: SC-13, SC-17	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-12(1)	Cryptographic Key Establishment and Management	Technical	Cryptographic Key Establishment and Management | Availability	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY The organization maintains availability of information in the event of the loss of cryptographic keys by users.		**X**				X	X
SC-12(2)	Cryptographic Key Establishment and Management	Technical	Cryptographic Key Establishment and Management | Symmetric Keys	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS The organization produces, controls, and distributes symmetric cryptographic keys using CSE compliant key management technology and processes.		**X**	X	X	X	X	X
SC-12(3)	Cryptographic Key Establishment and Management	Technical	Cryptographic Key Establishment and Management | Asymmetric Keys	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS The organization produces, controls, and distributes asymmetric cryptographic keys using CSE-approved key management technology and processes; approved PKI medium assurance certificates or prepositioned keying material; approved medium assurance or high assurance certificates and		**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				hardware security tokens that protect the user's private key.							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SC-13	Cryptographic Protection	Technical	Cryptographic Protection	(A) The information system implements CSE approved cryptography in accordance with applicable organizational policies, directives and standards.	Cryptography can be employed to support a variety of security solutions including, for example, the protection of sensitive information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls or policies, organizations document each type of cryptographic use and the	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					type of cryptography required (e.g., protection of classified information: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7						
SC-15	Collaborative Computing Devices	Technical	Collaborative Computing Devices	(A) The information system prohibits remote activation of collaborative computing devices with no exceptions. (B) The information system provides an explicit indication of use to users physically present at the devices.	Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. Related control: AC-21	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-17	Public Key Infrastructure Certificates	Technical	Public Key Infrastructure Certificates	(A) The organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates from an approved service provider.	For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12	**X**	X	X	X	X	X
SC-18	Mobile Code	Technical	Mobile Code	(A) The organization defines acceptable and unacceptable mobile code and mobile code technologies. (B) The organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies. (C) The organization authorizes, monitors, and controls the use of mobile code within the information system.	Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems. Related controls: AU-2, AU-12, CM-2, CM-6, SI-3						
SC-18(3)	Mobile Code	Technical	Mobile Code | Prevent Downloading / Execution	MOBILE CODE | PREVENT DOWNLOADING / EXECUTION The information system prevents the download and execution of all unacceptable mobile code and mobile code technologies defined under SC-18.		**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-18(4)	Mobile Code	Technical	Mobile Code | Prevent Automatic Execution	MOBILE CODE | PREVENT AUTOMATIC EXECUTION The information system prevents the automatic execution of mobile code in software applications and such as but not limited to email, scriptable document/ file editing applications that support documents with embedded code (e.g., MS Office applications/ documents), etc. and prompts the user for permission. and enforces organization-defined actions prior to executing the code.	Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of mobile code includes, for example, disabling auto execute features on information system components employing portable storage devices such as Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.	**X**	X	X	X	X	
SC-19	Voice Over Internet Protocol	Technical	Voice over Internet Protocol	(A) The organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously. (B) The organization authorizes, monitors, and controls the use of VoIP within the information system.	Related controls: CM-6, SC-7, SC-15	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-20	Secure Name / Address Resolution Service (Authoritative Source)	Technical	Secure Name / Address Resolution Service (Authoritative Source)	(A) The information system provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. (B) The information system provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/ service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. Information systems that use technologies other than the DNS to map	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	Technical	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	(A) The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. Related controls: SC-20, SC-22	**X**	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-22	Architecture and Provisioning for Name / Address Resolution Service	Technical	Architecture and Provisioning for Name / Address Resolution Service	(A) The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network sub-networks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists). Related controls: SC-2, SC-20, SC-21, SC-24						
SC-23	Session Authenticity	Technical	Session Authenticity	(A) The information system protects the authenticity of communications sessions.	This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. Related controls: SC-8, SC-10, SC-11						
SC-23(1)	Session Authenticity	Technical	Session Authenticity | Invalidate Session Identifiers at Logout	SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT The information system invalidates session identifiers upon user logout or other session termination.	This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-28	Protection of Information At Rest	Technical	Protection of Information at Rest	(A) The information system protects the confidentiality and integrity ofall information not cleared for public release and all data with a higher than low integrity requirement.	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7						

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SC-28(1)	Protection of Information At Rest	Technical	Protection of Information at Rest | Cryptographic Protection	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of all information not cleared for public release and all data with a higher than low integrity requirements.	Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12.						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SC-39	Process Isolation	Technical	Process Isolation	(A) The information system maintains a separate execution domain for each executing process.	Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies. Related controls: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-1	System and Information Integrity Policy and Procedures	Operational	System and Information Integrity Policy and Procedures	(A) The organization develops, documents, and disseminates to personnel or roles with system and information integrity responsibilities: (a) A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. (B) The organization reviews and updates the current: (a) System and information integrity policy at least every 3 years; and (b) System and information integrity procedures at least annually.	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. The system and information integrity policy and procedures reflect applicable organizational policies, directives, and. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					organizational risk management strategy is a key factor in establishing policy and procedures.						

SI-2	Flaw Remediation	Operational	Flaw Remediation	(A) The organization identifies, reports, and corrects information system flaws. (B) The organization tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. (C) The organization installs security-relevant software and firmware updates within 30 days of release of the release of the updates. (D) The organization incorporates flaw remediation into the organizational configuration management process.	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance	**X**	X	X	X	X	

					and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-						

					4, RA-5, SA-10, SA-11, SI-11							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-2(2)	Flaw Remediation	Operational	Flaw Remediation | Automated Flaw Remediation Status	FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.	Related controls: CM-6, SI-4.	**X**	X	X	X	X	
SI-2(3)	Flaw Remediation	Operational	Flaw Remediation | Time to Remediate Flaws / Benchmarks for Corrective Actions	FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS (a) The organization measures the time between flaw identification and flaw remediation; and (b) The organization establishes benchmarks of 30 days for high risk flaws, 90 days for moderate risk flaws for taking corrective actions.	This control enhancement requires organizations to determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by type of flaw and/or severity of the potential vulnerability if the flaw can be exploited.	**X**	X	X	X	X	

SI-3	Malicious Code Protection	Operational	Malicious Code Protection	(A) The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. (B) The organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. (C) The organization configures malicious code protection mechanisms to: (a) Perform periodic scans of the information system at least weekly and real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and (b) Block and quarantine malicious code; send alert to the key role as defined in the system and information integrity policy in response to malicious code detection. (D) The organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be	**X**	X	X	X	X	

					effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when						

					attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.							

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
SI-3(1)	Malicious Code Protection	Operational	Malicious Code Protection | Central Management	MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT The organization centrally manages malicious code protection mechanisms.	Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.	**X**	X	X	X	X	
SI-3(2)	Malicious Code Protection	Operational	Malicious Code Protection | Automatic Updates	MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES The information system automatically updates malicious code protection mechanisms.	Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-3(7)	Malicious Code Protection	Operational	Malicious Code Protection | Non Signature-Based Detection	MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION The information system implements non-signature-based malicious code detection mechanisms.	Non-signature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behaviour of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms.	**X**	X	X	X	X	

SI-4	Information System Monitoring	Operational	Information System Monitoring	(A) The organization monitors the information system to detect: (a) Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and (b) Unauthorized local, network, and remote connections; (B) The organization identifies unauthorized use of the information system through organization-defined techniques and methods. (C) The organization deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. (D) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. (E) The organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or Canada based on law enforcement information, intelligence information, or other credible sources of information. (F) The organization obtains legal opinion with regard to	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defence and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical	**X**	X	X	X	X	

				information system monitoring activities in accordance with orgnanizational policies, directives and standards. (G) The organization provides organization-defined information system monitoring information to organization-defined personnel or roles at an organization-defined frequency.	applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, HTTP traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3,						

					RA-5, SC-7, SC-26, SC-35, SI-3, SI-7						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-4(1)	Information System Monitoring	Operational	Information System Monitoring | System-Wide Intrusion Detection System	INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.		**X**	X	X	X	X	
SI-4(2)	Information System Monitoring	Operational	Information System Monitoring | Automated Tools for Real-Time Analysis	INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS The organization employs automated tools to support near real-time analysis of events.	Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.	**X**	X	X	X	X	
SI-4(4)	Information System Monitoring	Operational	Information System Monitoring | Inbound and Outbound Communications Traffic	INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC The information system monitors inbound and outbound communications traffic continously for unusual or unauthorized activities or conditions.	Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					propagating among system components, the unauthorized exporting of information, or signalling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.						
SI-4(5)	Information System Monitoring	Operational	Information System Monitoring | System-Generated Alerts	INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS The information system alerts organization-defined personnel or roles and client governance bodies when organization-defined compromise or potential compromise indicators occur.	Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
					security officers. Related controls: AU-5, PE-6.						
SI-4(7)	Information System Monitoring	Operational	Information System Monitoring | Automated Response to Suspicious Events	INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS The information system notifies organization-defined incident response personnel (identified by name and/or by role) of detected suspicious events and takes organization-defined least-disruptive actions to terminate suspicious events.	Least-disruptive actions may include, for example, initiating requests for human responses.	**X**	X	X	X	X	

Solicitation No. – Nº de l'invitation	Amd. No – Nº de la modif.	Buyer ID – Id de l'acheteur
HT372-192532/B		152XL
Client Ref. No. – Nº de réf. De client	**File No. – Nº du dossier**	**CCC No./ Nº CCC – FMS No/ Nº VME**
HT372-192532	HT372-192532/001/XL	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-4(11)	Information System Monitoring	Operational	Information System Monitoring | Analyze Communications Traffic Anomalies	INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES The organization analyzes outbound communications traffic at the external boundary of the information system and selected organization-defined interior points within the system (e.g., sub-networks, subsystems) to discover anomalies.	Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.	**X**	X	X	X	X	X	
SI-4(14)	Information System Monitoring	Operational	Information System Monitoring | Wireless Intrusion Detection	INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	Wireless signals may radiate beyond the confines of organization-controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems. Related controls: AC-18, IA-3.	**X**	X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-4(16)	Information System Monitoring	Operational	Information System Monitoring | Correlate Monitoring Information	INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION The organization correlates information from monitoring tools employed throughout the information system.	Correlating information from different monitoring tools can provide a more comprehensive view of information system activity. The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns. Understanding the capabilities/limitations of diverse monitoring tools and how to maximize the utility of information generated by those tools can help organizations to build, operate, and maintain effective monitoring programs. Related control: AU-6.	**X**	X	X	X	X	
SI-4(20)	Information System Monitoring	Operational	Information System Monitoring | Privileged User	INFORMATION SYSTEM MONITORING | PRIVILEGED USER The organization implements a privilege user authorization process in accordance with Identity and Access Management policies.		**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-4(23)	Information System Monitoring	Operational	Information System Monitoring | Host-Based Devices	INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES The organization implements system logging tools at components running general purpose operating systems.	Information system components where host-based monitoring can be implemented include, for example, servers, workstations, and mobile devices. Organizations consider employing host-based monitoring mechanisms from multiple information technology product developers.	**X**	X	X	X	X	
SI-5	Security Alerts, Advisories, and Directives	Operational	Security Alerts, Advisories, and Directives	(A) The organization receives information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis. (B) The organization generates internal security alerts, advisories, and directives as deemed necessary. (C) The organization disseminates security alerts, advisories, and directives to: organization-defined personnel, roles, elements, and external organizations including affected clients. (D) The organization implements security directives in accordance with established time frames, or	Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals and other organizations should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2	**X**	X	X	X	X	X

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
				notifies the issuing organization of the degree of non-compliance.							

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-6	Security Functional Verification	Operational	Security Function Verification	(A) The information system verifies the correct operation of organization-defined security functions. (B) The information system performs this verification organization-defined system transitional states including at least system startup and restart and at least monthly. (C) The information system notifies organization-defined personnel or roles including system administrators and security personnel of failed security verification tests. (D) The information system takes organization-defined action(s) when anomalies are discovered and notifies system administrators and security personnel.	Transitional states for information systems include, for example, system start-up, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-7	Software, Firmware, and Information Integrity	Operational	Software, Firmware, and Information Integrity	(A) The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information on production systems as a minimum.	Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-7(1)	Software, Firmware, and Information Integrity	Operational	Software, Firmware, and Information Integrity | Integrity Checks	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS The information system performs an integrity check of organization-defined software, firmware, and information at start-up and at least every 30 days.	Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system start-up, restart, shutdown, and abort.	**X**	X	X	X	X	
SI-7(7)	Software, Firmware, and Information Integrity	Operational	Software, Firmware, and Information Integrity | Integration of Detection and Response	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE The organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability.	This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-8	Spam Protection	Operational	Spam Protection	(A) The organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages. (B) The organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3	**X**	X	X	X	X	
SI-8(1)	Spam Protection	Operational	Spam Protection | Central Management of Protection Mechanisms	SPAM PROTECTION | CENTRAL MANAGEMENT The organization centrally manages spam protection mechanisms.	Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)											
								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					controls. Related controls: AU-3, SI-2, SI-7.						
SI-8(2)	Spam Protection	Operational	Spam Protection | Automatic Updates	SPAM PROTECTION | AUTOMATIC UPDATES The information system automatically updates spam protection mechanisms.		X	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-10	Information Input Validation	Operational	Information Input Validation	(A) The information system checks the validity of organization-defined information inputs.	Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS Medium Profile for Cloud	CSP Full Stack	Stacked PaaS	Stacked SaaS	IaaS / PaaS	SaaS
						353	331	309	304	327	171
					information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Pre-screening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks						

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-11	Error Handling	Operational	Error Handling	(A) The information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. (B) The information system reveals error messages only to organization-defined personnel or roles.	Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/ business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31	**X**	X	X	X	X	

CCCS Cloud Security Control Recommendations (31-May-2019)								CSP		Client	
ID	**Name**	**Class**	**Title**	**Definition**	**Supplemental Guidance**	**CCCS Medium Profile for Cloud**	**CSP Full Stack**	**Stacked PaaS**	**Stacked SaaS**	**IaaS / PaaS**	**SaaS**
						353	**331**	**309**	**304**	**327**	**171**
SI-12	Information Output Handling and Retention	Operational	Information Handling and Retention	(A) The organization handles and retains information within the information system and information output from the system in accordance with applicable organizational policies, directives and standards.	Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4	**X**	X	X	X	X	X
SI-16	Memory Protection	Operational	Memory Protection	(A) The information system implements organization-defined security safeguards to protect its memory from unauthorized code execution.	Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. Related controls: AC-25, SC-3	**X**	X	X	X	X	