« Infrastructure (technologie et opérations) » du CCP

Statut du document : Recommandation finale V1.2

Conformément aux procédures opérationnelles du CCIAN, une recommandation finale est un livrable qui représente les conclusions d'un comité d'experts du CCIAN ayant été approuvées par un comité d'experts et ratifiées par un vote des membres bienfaiteurs du CCIAN.

Ce document a été élaboré par le comité d'experts du cadre de confiance du CCIAN avec les commentaires du public recueillis et traités dans le cadre d'un processus ouvert d'examen par les pairs. On s'attend à ce que le contenu de ce document soit examiné et mis à jour régulièrement afin de donner suite à la rétroaction reliée à la mise en œuvre opérationnelle, aux progrès technologiques, et aux changements de lois, règlements et politiques. Les avis concernant les changements apportés à ce document seront partagés sous la forme de communications électroniques, notamment le courriel et les réseaux sociaux. Les notifications seront également consignées dans le programme de travail du Cadre de confiance pancanadien (CCP).

Ce document est fourni « TEL QUEL » et aucun participant du CCIAN ne garantit de quelque façon que ce soit, d'une manière expresse ou implicite, y compris d'une manière sous-entendue, sa qualité marchande, le fait qu'il ne viole pas les droits de propriété intellectuelle de tierces parties et qu'il convient à une fin particulière. Les personnes désirant obtenir de plus amples renseignements au sujet de la gouvernance du CCIAN sont invitées à consulter les politiques qui régissent le CCIAN.

Table des matières

1. Introduction de la composante « Infrastructure (technologie et opérations) »

Le contenu ici présent concerne un sujet spécifique au domaine de ce composant du Cadre de confiance pancanadien (CPP). La section d'aperçu fournit des informations nécessaires pour une interprétation cohérente des critères de conformité inclus. Pour une introduction générale au CPP, veuillez consulter l'Aperçu du CPP, qui décrit le contexte, le but, la portée, les principes et les objectifs du cadre.

1.1 Raison d’être et avantages anticipés

La composante « Infrastructure (technologie et opérations) » du CCP vise à recenser les politiques, plans, et exigences relatives à la technologie et aux opérations technologiques pour soutenir la mise en œuvre des principes des profils du CCP dans le contexte de l’écosystème de l’identité numérique.

Un processus certifié est un processus de confiance auquel d’autres participants du CCP peuvent se fier. Les critères de conformité du CCP visent à compléter les lois et règlements existants sur la protection de la vie privée; on s’attend à ce que les participants à l’écosystème de l’identité numérique certifiés par le CCIAN satisfassent aux exigences et aux règlements prévus par la loi qui sont applicables dans leurs territoires.

La composante « Infrastructure (technologie et opérations) » du CCP définit :

- Les artéfacts officiels en matière de politiques et plans qui forment la base d’une installation technologique conforme et de ses opérations de soutien technologique.
- Les capacités de haut niveau en termes de technologie et d’outils technologiques requises pour soutenir une infrastructure technologique qui dessert un écosystème de l’identité numérique.
- Les outils et caractéristiques opérationnels de soutien technologique pour soutenir une infrastructure technologique installée qui dessert un écosystème de l’identité numérique.

1.2 Portée

Cette section définit la portée de la composante « Infrastructure (technologie et opérations) » du CCP. Les exigences incluses dans la portée sont identifiées à un haut

niveau pour illustrer la portée; les exigences détaillées sont élaborées dans le profil de conformité de la composante « Infrastructure (technologie et opérations) » du CCP.

1.2.1 Inclus dans la portée

Cette composante du CCP va spécifier les critères de conformité qui fournissent les exigences et lignes directrices générales concernant la fiabilité de l'infrastructure TI qui permet la mise en œuvre et la prestation de processus de confiance définis dans d'autres composantes du CCP. Les principaux domaines de la composante sont la sécurité et l'intégrité des composantes techniques. À l'intérieur de ces domaines d'intérêt, la portée de la composante inclut :

- La sécurité TI (en tant que considération générale).
- La supervision de la collecte, la validation, l'entreposage et l'accessibilité des données.
- Les audits et l'enregistrement.
- La prévention des événements TI qui compromettent la fiabilité de l'écosystème de l'identité numérique et la réaction à ceux-ci.
- Les politiques et plans qui soutiennent la gestion de la fiabilité de la technologie et des opérations technologiques.

1.2.2 Exclus de la portée

La portée de cette composante du CCP n'inclut pas :

- Le caractère adéquat des produits spécifiques pour soutenir un processus de confiance donné.
- Le caractère adéquat des normes, processus, technologies ou protocoles technologiques qui peuvent être spécifiques à ou imposés par un écosystème de l'identité numérique en particulier.
- L'obligation d'utiliser un ensemble spécifique de pratiques ou cadres standards pour gouverner les opérations technologiques (p. ex. IT Infrastructure Library <<ITIL>>, Control Objectives for Information Technology <<COBIT>>).

1.3 Relations avec le CCP

Le Cadre de confiance pancanadien consiste en une série de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées d'une manière indépendante pour être prises en considération comme composantes de confiance. Le CCP, qui tire parti d'une approche pancanadienne, permet aux secteurs public et privé de collaborer pour protéger les identités numériques en uniformisant les processus et pratiques dans tout l'écosystème numérique canadien.

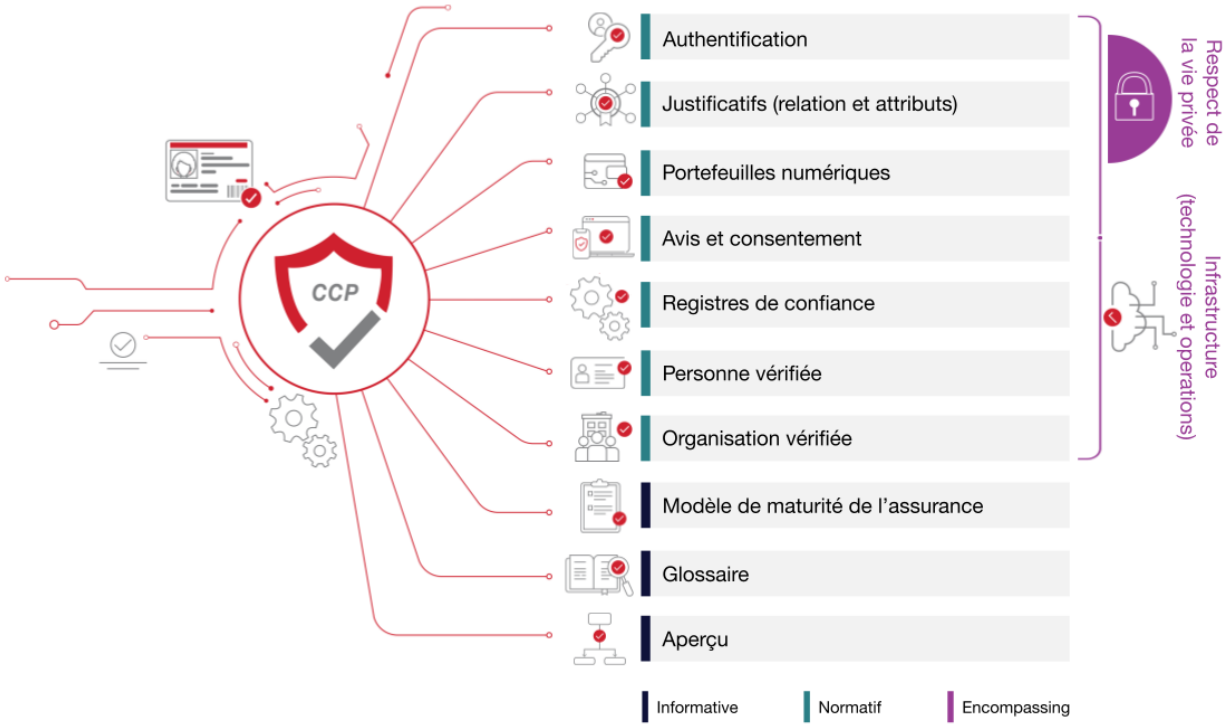

Figure 1. Composantes du Cadre de confiance pancanadien

Les critères de conformité du CCP ne remplacent pas les règlements existants et ne les substituent pas; on s'attend à ce que les organisations et les particuliers se conforment aux lois, aux politiques et aux règlements pertinents dans leur territoire.

2. Conventions de la composante « Infrastructure (technologie et opérations) »

Cette section décrit et définit les principaux termes et notions utlisés dans la composante « Infrastructure (technologie et opérations) » du CCP. Ces renseignements sont fournis pour assurer une utilisation et une interprétation uniformes des termes dans toute cette composante.

Remarques :

- Les conventions peuvent varier entre les composantes du CCP. Les lecteurs sont encouragés à passer en revue les conventions de chaque composante du CCP qu'ils lisent.

- Termes définis – les principaux termes et notions décrits et définis dans cette section et le glossaire du CCP sont écrits avec une majuscule dans ce document.
- Liens hypertextes – il se pourrait que des liens hypertextes soient intégrés dans les versions électroniques de ce document comme référence pour le lecteur. Tous les liens étaient accessibles au moment de la rédaction.

2.1 Termes et définitions

Pour les besoins de cette composante du CCP, les termes et les définitions figurant dans le glossaire du CCP et dans la présente section s'appliquent.

Critères de conformité

Exigences développées pour chacune des composantes du CCP et servant de base pour évaluer la conformité.

Écosystème de l'identité numérique

Écosystème interconnecté pour l'échange et la vérification de l'information sur l'identité numérique, qui implique des organisations des secteurs public et privé qui se conforment à un cadre de confiance commun pour la gestion et l'utilisation d'identités numériques, et les sujets de ces identités numériques.

Renseignements personnels

Tout renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable (Source : Survol de la LPRPDE, Commissariat de protection de la vie privée du Canada – Qu'entend-on par « renseignements personnels?).

2.2 Abréviations

Les abréviations et acronymes qui suivent apparaissent tout au long de cette composante du CCP :

- CCIAN – Conseil canadien de l'identité et de l'authentification numériques
- COBIT - Control Objectives for Information Technology
- ENISA – Agence de l'Union européenne pour la cybersécurité
- FEDRAMP - Federal Risk and Authorization Management Program
- ITIL - IT Infrastructure Library
- NIST - National Institute of Standards and Technology
- CCP – Cadre de confiance pancanadien

3. Couverture des critères de conformité

Les critères de conformité sont élaborés en détail dans le profil de conformité de la composante « Infrastructure (technologie et opérations) » du CCP. Les exigences ont été conçues pour refléter les capacités et les caractéristiques trouvées dans les opérations technologiques et les normes de gouvernance (p. ex., ITIL, COBIT) sans être aussi prescriptives qu'une norme spécifique l'exige.

De même, les organismes de normalisation du secteur public et les orientations concernant la mise en œuvre ont été mis à contribution pour aider à définir certaines exigences détaillées dans les critères de conformité. C'est notamment le cas du National Institute of Standards and Technology (NIST) et du Federal Risk and Authorization Management Program (FEDRAMP) aux États-Unis, de l'Agence de l'Union européenne pour la cybersécurité (ENISA) en Europe et de diverses directives du gouvernement fédéral au Canada. L'approche a consisté à s'inspirer de certaines orientations communes pour la mise en œuvre et la gestion technologiques tout en s'assurant que les critères de conformité du CCP étaient assez génériques pour coexister dans un domaine du secteur public ou privé.

Cela vaut la peine de souligner que les critères de conformité de la composante « Infrastructure (technologie et opérations) » du CCP sont décrits d'une manière générique, en mettant davantage l'accent sur les capacités nécessaires pour avoir une infrastructure de confiance comme plateforme pour fournir d'autres services conformes à l'intérieur du CCP. On s'attend à ce que les organisations désirant participer à un écosystème de l'identité numérique spécifique aient des exigences spécifiques en ce qui concerne la technologie et les opérations technologiques qui leur sont imposées par l'écosystème de l'identité numérique. L'identification d'un produit technologique, d'un protocole ou d'une norme opérationnelle tierce dans un écosystème particulier de l'identité numérique n'est pas inclus dans la portée de ce profil.

Les critères sont organisés en trois grandes catégories :

- Politiques et plans – saisit les principaux artéfacts officiels qui peuvent définir l'approche uniforme de l'organisation pour instancier et gérer les composantes technologiques et systèmes qui remplissent le rôle que l'organisation joue dans l'écosystème de l'identité numérique.
- Technologie – identifie les caractéristiques et capacités des composantes technologiques requises.
- Opérations – identifie les caractéristiques et capacités requises du cadre et de l'ensemble d'outils opérationnels utilisés pour jouer un rôle défini au sein de l'écosystème de l'identité numérique.

3.1 Politique et plans

La base de la composante technologique d'une architecture d'entreprise est un ensemble complet de politiques et plans organisationnels clairement cartographiés selon les objectifs commerciaux identifiés dans les composantes commerciales de l'architecture d'entreprise. Ce profil identifie les exigences concernant les artéfacts officiels et leur gestion continue dans les domaines suivants :

- Évaluation des risques;
- Audit et imputabilité;
- Évaluation de la sécurité;
- Planification des désastres ou des situations d'urgence;
- Identification et authentification;
- Protection des systèmes et des communications;
- Intervention en cas d'incident;
- Intégrité des systèmes et de l'information;
- Gestion de la configuration;
- Gestion de l'information;
- Maintenance des systèmes;
- Contrôle de l'accès technique;
- Contrôle de l'accès physique;
- Sécurité du personnel.

D'une façon générale, on retient surtout de cet ensemble de critères le besoin d'avoir une planification ordonnée qui commence par la détermination des objectifs dans les énoncés de politique, et est soutenue par des plans officiels qui régissent la mise en œuvre et le fonctionnement de la technologie.

3.2 Critères technologiques

Ces critères mettent l'accent sur l'identification des outils et des capacités technologiques génériques nécessaires pour soutenir une infrastructure opérationnelle qui fournit des services conformes au CCP. Les produits ou protocoles spécifiques ne sont pas précisés, car ils tendent à varier selon le processus de confiance spécifique fourni à un écosystème de l'identité numérique en particulier. On s'attend à ce que les organisations aient des exigences spécifiques supplémentaires dans ce domaine qui sont imposées par l'écosystème de l'identité numérique dans lequel elles veulent fonctionner.

Les capacités qui sont spécifiques à d'autres processus de confiance du CCP (authentification, respect de la vie privée, personne vérifiée, etc.) ne sont pas élaborées dans ce profil. Ces critères sont identifiés dans les profils de conformité du CCP spécifiques au sujet. Il y a plusieurs références croisées à d'autres profils de conformité lors c'est approprié.

3.3 Critères des opérations technologiques

La troisième catégorie de critères de conformité identifie les opérations technologiques et les capacités de soutien nécessaires pour exploiter une infrastructure conforme au CCP. Ces capacités, qui s'alignent sur les politiques et les plans indiqués plus tôt, représentent les caractéristiques technologiques, opérationnelles et en matière de soutien permanentes qui sont requises pour respecter les capacités d'entreprise identifiées dans les politiques et les plans associés à une architecture d'entreprise globale.

4. Introduction au profil de conformité de la composante « Infrastructure (technologie et opérations) » du CCP

Ce document spécifie les critères de conformité de la composante « Infrastructure (technologie et opérations) » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction générale du CCP, y compris des renseignements contextuels et les buts et objectifs du CCP, veuillez consulter l'aperçu du modèle de CCP.

Les critères de conformité de la composante « Infrastructure » spécifient les caractéristiques de la technologie et des opérations technologiques soutenant la mise en œuvre des systèmes qui fournissent des services conformes aux profils du CCP. Les critères sont exprimés dans des termes génériques reconnaissant que les technologies ou caractéristiques technologiques spécifiques (p. ex., les protocoles) seront sans doute imposées et varieront à l'intérieur de chaque écosystème individuel de l'identité numérique.

Remarque : Ces critères de conformité ne remplacent pas des politiques ou des règlements existants; on s'attend à ce que les organisations se conforment aux lois, aux politiques et aux règlements pertinents en vigueur dans leur territoire.

4.1 Mots clés des critères de conformité

Les mots clés suivants sont utilisés dans les critères de conformité pour indiquer leur priorité et/ou leur rigidité générale, et doivent être interprétés de la façon suivante :

- **DOIT** signifie que l'exigence est impérative en ce qui concerne les critères de conformité.
- **NE DOIT PAS** signifie que l'exigence est une interdiction absolue des critères de conformité.
- **DEVRAIT** signifie qu'on s'attend à ce que l'exigence soit remplie, sauf dans les cas limités où le candidat présente des raisons ou des circonstances valables d'ignorer l'exigence. Toutes les implications d'une telle exception doivent être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité comme décrit.
- **NE DEVRAIT PAS** signifie qu'il peut exister une raison valable dans des circonstances particulières pour que l'exigence soit acceptable ou même utile, mais que toutes les implications devraient être comprises et le cas devrait être bien pris en considération avant de choisir de ne pas se conformer aux exigences telles que décrites.
- **PEUT** signifie que l'exigence est discrétionnaire mais recommandée.

Remarque : Les mots clés ci-dessus sont en **caractères gras** et en MAJUSCULES dans ce profil de conformité.

4.2 Conventions de l'infrastructure

Chaque composante du CCP comporte des conventions qui assurent une utilisation et une interprétation uniformes des termes et des notions apparaissant dans la composante. L'aperçu de la composante « Infrastructure (technologie et opérations) » du CCP fournit les conventions pour cette composante. Ces conventions incluent des définitions et descriptions des éléments suivants auxquels il est fait référence dans ce profil de conformité :

- Principaux termes et notions
- Abréviations et acronymes

Remarques :

- Les conventions peuvent varier entre les composantes du CCP. Les lecteurs sont invités à passer en revue les conventions de chaque composante du CCP qu'ils lisent.
- Termes définis – pour les besoins du présent profil de conformité, les termes et les définitions figurant dans l'aperçu de la composante « Infrastructure » du CCP et le glossaire du CCP s'appliquent. Les principaux termes et notions décrits et définis dans cette section ou l'aperçu de la composante « Infrastructure » du CCP ou encore le glossaire du CCP sont écrits en majuscules dans tout ce document.
- Liens hypertextes – il se pourrait que des liens hypertextes soient intégrés dans les versions électroniques de ce document. Tous les liens étaient accessibles au moment de la rédaction.

5. Critères de conformité de la composante « Infrastructure »

Les critères de conformité ci-dessous sont répartis en trois grandes catégories :

- **POL** – exigences des politiques et plans qui définissent et soutiennent l'architecture technologique selon laquelle fonctionnent les composantes du système participant à l'écosystème de l'identité numérique.
- **TECH** – exigences technologiques
- **OPS** – opérations technologiques

Par souci de convivialité, les critères sont numérotés à l'intérieur de leur section et on peut y faire référence en utilisant ces identifiants (p. ex., on peut utiliser POL-1 pour faire référence au premier critère dans la section POL).

On peut supposer que la portée des critères s'applique uniquement aux composantes de la technologie ou des systèmes utilisées par une organisation pour fournir ou consommer un service à l'intérieur de l'écosystème de l'identité numérique.

Remarques :

- Les niveaux d'assurance associés aux critères individuels ci-dessous ne correspondent pas aux niveaux d'assurance traditionnels de l'authentification, de l'identité et des justificatifs. Ils visent plutôt à indiquer le niveau de maturité de la technologie et de l'infrastructure soutenant ces assurances. Par exemple, une organisation qui soutient un processus d'assurance de l'identité de niveau 2 devrait remplir tous les critères indiqués comme étant appropriés pour le niveau 2 ci-dessous.
- Le niveau 4 déborde de la portée de cette version. La référence est conservée pour un développement futur.

Remarque : C'est important de noter que ces niveaux d'assurance représentent des capacités à aborder et qu'ils ne devraient pas être interprétés comme des artéfacts de politiques ou de plans individuels. Bon nombre de ces capacités sont habituellement combinées et traitées dans un seul artéfact.

Référence	**Critères de conformité**				
POL	**Exigences reliées aux politiques et aux plans technologiques nécessaires pour soutenir l'infrastructure mise à profit pour desservir l'écosystème de l'identité numérique.**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Les politiques, plans ou artéfacts qui sont nécessaires pour d'autres critères de ce profil **DOIVENT** être examinés et mis à jour sur une base continue pour refléter l'évolution des exigences commerciales ou opérationnelles.	X	X	X	
2	La capacité commerciale et l'architecture des services **DOIVENT** être officialisées et documentées.	X	X	X	

3	Une politique d'évaluation du risque **PEUT** être développée, documentée et disséminée au sein de l'organisation.	X			
4	Une politique d'évaluation du risque **DOIT** être développée, documentée et disséminée au sein de l'organisation.		X	X	
5	Une politique d'évaluation du risque **PEUT** couvrir, sans s'y limiter, ce qui suit : • Contexte et priorités pour gérer le risque (y compris le risque pour la sécurité et la protection de la vie privée). Cela peut inclure une évaluation du risque au niveau organisationnel, au niveau des processus opérationnels et/ou au niveau des systèmes. • Catégorisation du ou des systèmes et de l'information traitée, enregistrée et transmise par le ou les systèmes en fonction d'une analyse de l'incidence de la perte. • Recensement des principaux facteurs de risque, notamment, sans s'y limiter, l'incidence de la perte, les menaces, les vulnérabilités et la probabilité que cela se produise.	X			

6	Une politique d'évaluation du risque **DEVRAIT** couvrir, sans s'y limiter, ce qui suit : • Contexte et priorités pour gérer le risque (y compris le risque pour la sécurité et la protection de la vie privée). Cela peut inclure une évaluation du risque au niveau organisationnel, au niveau des processus opérationnels et/ou au niveau des systèmes. • Catégorisation du ou des systèmes et de l'information traitée, enregistrée et transmise par le ou les systèmes en fonction d'une analyse de l'incidence de la perte. • Recensement des principaux facteurs de risque, notamment, sans s'y limiter, l'incidence de la perte, les menaces, les vulnérabilités et la probabilité que cela se produise.		X	X	

7	Un plan d'évaluation du risque **PEUT** couvrir, sans s'y limiter, ce qui suit : • Un plan pour la conception de systèmes de contrôle afin d'atténuer le risque à des niveaux acceptables. • Un plan pour créer ou maintenir un ou des guides de mise en œuvre et une ou des procédures opérationnelles normalisées pour les contrôles opérationnels. • Un plan pour évaluer les contrôles afin de déterminer s'ils sont mis en œuvre correctement, fonctionnent comme prévu, et fournissent les résultats souhaités pour ce qui est de satisfaire aux exigences de l'entité (notamment les exigences de sécurité et de protection de la vie privée). • Des plans pour surveiller le système et les contrôles qui y sont associés, et en rendre compte, sur une base continue afin d'inclure l'évaluation de l'efficacité, de documenter les changements apportés au système et à l'environnement opérationnel en menant des évaluations du risque et des analyses d'impact..	X			

8	Un plan d'évaluation du risque **DEVRAIT** couvrir, sans s'y limiter, ce qui suit : • Un plan pour la conception de systèmes de contrôle afin d'atténuer le risque à des niveaux acceptables. • Un plan pour créer ou maintenir un ou des guides de mise en œuvre et une ou des procédures opérationnelles normalisées pour les contrôles opérationnels. • Un plan pour évaluer les contrôles afin de déterminer s'ils sont mis en œuvre correctement, fonctionnent comme prévu, et fournissent les résultats souhaités pour ce qui est de satisfaire aux exigences de l'entité (notamment les exigences de sécurité et de protection de la vie privée). • Des plans pour surveiller le système et les contrôles qui y sont associés, et en rendre compte, sur une base continue afin d'inclure l'évaluation de l'efficacité, de documenter les changements apportés au système et à l'environnement opérationnel en menant des évaluations du risque et des analyses d'impact.		X	X	
9	Une politique d'audit et d'imputabilité **PEUT** être développée, documentée et disséminée au sein de l'organisation.	X			
10	Une politique d'audit et d'imputabilité **DOIT** être développée, documentée et disséminée au sein de l'organisation.		X	X	
11	Un plan d'audit et d'imputabilité **PEUT** être développé, documenté et disséminé au sein de l'organisation.	X			
12	Un plan d'audit et d'imputabilité **DOIT** être développé, documenté et disséminé au sein de l'organisation.		X	X	

13	Un plan d'audit et de responsabilisation **PEUT** couvrir et détailler, sans s'y limiter, ce qui suit : • Propriétaires des données; • Événements pouvant être audités; • Contenu des dossiers d'audit; • Capacité d'entreposage des audits; • Réponse aux failles du traitement des audits; • Processus d'examen, d'analyse et de déclaration des audits; • Protection de l'information sur les audits; • Rétention et élimination des dossiers d'audit.	X			
14	Un plan d'audit et de responsabilisation **DEVRAIT** couvrir et détailler, sans s'y limiter, ce qui suit : • Propriétaires des données; • Événements pouvant être audités; • Contenu des dossiers d'audit; • Capacité d'entreposage des audits; • Réponse aux failles du traitement des audits; • Processus d'examen, d'analyse et de déclaration des audits; • Protection de l'information sur les audits; • Rétention et élimination des dossiers d'audit.		X	X	
15	Une politique d'évaluation de la sécurité **PEUT** être développée, documentée et disséminée au sein de l'organisation.	X			
16	Une politique d'évaluation de la sécurité **DOIT** être développée, documentée et disséminée au sein de l'organisation		X	X	

17	Un plan d'évaluation de la sécurité **PEUT** être développé, documenté et disséminé au sein de l'organisation.	X			
18	Un plan d'évaluation de la sécurité **DOIT** être développé, documenté et disséminé au sein de l'organisation.		X	X	
19	Un plan d'évaluation de la sécurité **PEUT** détailler, sans s'y limiter, ce qui suit : • Les contrôles de sécurité en cours d'évaluation; • Les outils d'évaluation; • Les rôles et responsabilités; • Les procédures d'évaluation de la sécurité; • L'examen, l'analyse et le compte rendu de l'évaluation.	X			
20	Un plan d'évaluation de la sécurité **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Les contrôles de sécurité en cours d'évaluation; • Les outils d'évaluation; • Les rôles et responsabilités; • Les procédures d'évaluation de la sécurité; • L'examen, l'analyse et le compte rendu de l'évaluation.		X	X	
21	Une politique d'intervention d'urgence TI **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
22	Une politique d'intervention d'urgence TI **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	

23	Un plan d'intervention d'urgence TI **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
24	Un plan d'intervention d'urgence TI **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	
25	Un plan d'intervention d'urgence TI **PEUT** détailler, sans s'y limiter, ce qui suit : • Missions et fonctions commerciales essentielles, et exigences connexes en matière d'intervention d'urgence; • Objectifs en termes de reprise, priorités en matière de rétablissement et paramètres; • Rôles, responsabilités et personnes affectées en cas d'intervention d'urgence, avec leurs coordonnées; • Maintien des missions et des fonctions commerciales essentielles en dépit d'une perturbation, d'une compromission ou d'une panne des systèmes d'information; • Rétablissement complet des systèmes d'information, incluant les données des systèmes et les renseignements personnels, sans détérioration des mécanismes de sécurité initialement planifiés et mis en œuvre.	X			

26	Un plan d'intervention d'urgence TI **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Missions et fonctions commerciales essentielles, et exigences connexes en matière d'intervention d'urgence; • Objectifs en termes de reprise, priorités en matière de rétablissement et paramètres; • Rôles, responsabilités et personnes affectées en cas d'intervention d'urgence, avec leurs coordonnées; • Maintien des missions et des fonctions commerciales essentielles en dépit d'une perturbation, d'une compromission ou d'une panne des systèmes d'information; • Rétablissement complet des systèmes d'information, incluant les données des systèmes et les renseignements personnels, sans détérioration des mécanismes de sécurité initialement planifiés et mis en œuvre.		X	X	
27	Une politique d'identification et d'authentification **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
28	Une politique d'identification et d'authentification **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
29	Un plan d'identification et d'authentification **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
30	Un plan d'identification et d'authentification **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	

31	Un plan d'identification et d'authentification **PEUT** détailler, sans s'y limiter, ce qui suit : • Rôles et responsabilités; • Identification et authentification des utilisateurs organisationnels; • Identification et authentification des utilisateurs non organisationnels; • Identification et authentification des appareils; • Gestion des identifiants; • Gestion et rétroaction des authentifiants.	X			
32	Un plan d'identification et d'authentification **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Rôles et responsabilités; • Identification et authentification des utilisateurs organisationnels; • Identification et authentification des utilisateurs non organisationnels; • Identification et authentification des appareils; • Gestion des identifiants; • Gestion et rétroaction des authentifiants.		X	X	
33	Une politique de protection des systèmes et des communications **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
34	Une politique de protection des systèmes et des communications **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	

35	Un plan de protection des systèmes et des communications **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
36	Un plan de protection des systèmes et des communications **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	
37	Un plan de protection des systèmes et des communications **PEUT** détailler, sans s'y limiter, ce qui suit : • Partitionnement des applications; • Renseignements sur les ressources partagées; • Protection contre le déni de service; • Protection des frontières; • Confidentialité et intégrité de la transmission; • Protection des renseignements au repos; • Fin de session; • Gestion des clés cryptographiques; • Protection cryptographique; • Appareils informatiques coopératifs; • Authenticité des sessions; • Isolation des processus.	X			

38	Un plan de protection des systèmes et des communications **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Partitionnement des applications; • Renseignements sur les ressources partagées; • Protection contre le déni de service; • Protection des frontières; • Confidentialité et intégrité de la transmission; • Protection des renseignements au repos; • Fin de session; • Gestion des clés cryptographiques; • Protection cryptographique; • Appareils informatiques coopératifs; • Authenticité des sessions; • Isolation des processus.		X	X	
39	Une politique d'intervention en cas d'incident **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
40	Une politique d'intervention en cas d'incident **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
41	Un plan d'intervention en cas d'incident **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
42	Un plan d'intervention en cas d'incident **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	

43	Un plan d'intervention en cas d'incident **PEUT** détailler, sans s'y limiter, ce qui suit : • Une feuille de route pour mettre en œuvre une capacité d'intervention en cas d'incident; • Les exigences propres à l'organisation, qui sont reliées à la mission, à la taille, à la structure et aux fonctions; • Les incidents à déclarer; • Les paramètres pour mesurer la capacité d'intervention en cas d'incident au sein de l'organisation; • Les ressources et le soutien en matière de gestion nécessaires pour maintenir efficacement la capacité d'intervention en cas d'incident; • Les procédures nécessaires pour l'identification, le confinement, l'éradication, le rétablissement, le signalement et la révision du plan.	X			

44	Un plan d'intervention en cas d'incident **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Une feuille de route pour mettre en œuvre une capacité d'intervention en cas d'incident; • Les exigences propres à l'organisation, qui sont reliées à la mission, à la taille, à la structure et aux fonctions; • Les incidents à déclarer; • Les paramètres pour mesurer la capacité d'intervention en cas d'incident au sein de l'organisation; • Les ressources et le soutien en matière de gestion nécessaires pour maintenir efficacement la capacité d'intervention en cas d'incident; • Les procédures nécessaires pour l'identification, le confinement, l'éradication, le rétablissement, le signalement et la révision du plan.		X	X	

45	Une politique d'intégrité des systèmes et de l'information **PEUT** être élaborée, documentée et disséminée au sein de l'organisation, et : • Couvrir la raison d'être, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination parmi les entités organisationnelles et la conformité; • Être conforme aux lois, aux règlements, aux politiques, aux normes et aux lignes directrices applicables; • Désigner un responsable défini par l'organisation pour gérer le développement, la documentation et la dissémination de la politique et des procédures d'intégrité des systèmes et de l'information; • Examiner et mettre à jour les politiques et les procédures actuelles reliées à l'intégrité des systèmes et de l'information à une fréquence définie ou en fonction d'événement définis. **Remarque :** Les événements qui peuvent précipiter la mise à jour de la politique et des procédures d'intégrité des systèmes et de l'information incluent les conclusions d'une évaluation ou d'un audit, des incidents ou des infractions de sécurité, ou encore des changements apportés aux lois, décrets en conseil, directives, règlements, politiques, normes et lignes directrices applicables. La simple reformulation des contrôles ne constitue par une politique ou procédure organisationnelle.	X			

46	Une politique d'intégrité des systèmes et de l'information **DOIT** être élaborée, documentée et disséminée au sein de l'organisation, et : • Couvrir la raison d'être, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination parmi les entités organisationnelles et la conformité; • Être conforme aux lois, aux règlements, aux politiques, aux normes et aux lignes directrices applicables; • Désigner un responsable défini par l'organisation pour gérer le développement, la documentation et la dissémination de la politique et des procédures d'intégrité des systèmes et de l'information; • Examiner et mettre à jour les politiques et les procédures actuelles reliées à l'intégrité des systèmes et de l'information à une fréquence définie ou en fonction d'événement définis. **Remarque :** Les événements qui peuvent précipiter la mise à jour de la politique et des procédures d'intégrité des systèmes et de l'information incluent les conclusions d'une évaluation ou d'un audit, des incidents ou des infractions de sécurité, ou encore des changements apportés aux lois, décrets en conseil, directives, règlements, politiques, normes et lignes directrices applicables. La simple reformulation des contrôles ne constitue par une politique ou procédure organisationnelle.		X	X	
47	Un plan d'intégrité des systèmes et de l'information **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
48	Un plan d'intégrité des systèmes et de l'information **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	

49	Un plan d'intégrité des systèmes et de l'information **PEUT** détailler, sans s'y limiter, ce qui suit : • Identification, signalement et correction des failles des systèmes; • Essai des mises à jour de logiciels et de micrologiciels reliées à la correction des failles pour déterminer l'efficacité et les possibles effets collatéraux avant l'installation; • Installation des mises à jour de logiciels et de micrologiciels pertinentes à la sécurité à l'intérieur d'une période définie; • Incorporation des corrections de failles dans le processus de gestion de la configuration organisationnelle.	X			
50	Un plan d'intégrité des systèmes et de l'information **DOIT** détailler, sans s'y limiter, ce qui suit : • Identification, signalement et correction des failles des systèmes; • Essai des mises à jour de logiciels et de micrologiciels reliées à la correction des failles pour déterminer l'efficacité et les possibles effets collatéraux avant l'installation; • Installation des mises à jour de logiciels et de micrologiciels pertinentes à la sécurité à l'intérieur d'une période définie; • Incorporation des corrections de failles dans le processus de gestion de la configuration organisationnelle.		X	X	
51	Une politique de gestion de la configuration **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			

52	Une politique de gestion de la configuration **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
53	Un plan gestion de la configuration **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
54	Un plan de gestion de la configuration **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	
55	Un plan de gestion de la configuration **PEUT** détailler, sans s'y limiter, ce qui suit : • Rôles, responsabilités, et processus et procédures de gestion de la configuration; • Processus pour identifier les éléments de configuration pendant tout le cycle de vie du développement des systèmes et pour gérer la configuration des éléments de configuration; • Les éléments de configuration et les produits de base à gérer dans le cadre du plan.	X			
56	Un plan de gestion de la configuration **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Rôles, responsabilités, et processus et procédures de gestion de la configuration; • Processus pour identifier les éléments de configuration pendant tout le cycle de vie du développement des systèmes et pour gérer la configuration des éléments de configuration; • Les éléments de configuration et les produits de base à gérer dans le cadre du plan.		X	X	

57	Une politique de gestion de l'information et de protection de la vie privée **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
58	Une politique de gestion de l'information et de protection de la vie privée **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
59	Un plan de gestion de l'information et de protection de la vie privée **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
60	Un plan de gestion de l'information et de protection de la vie privée **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	
61	Un plan de gestion de l'information et de protection de la vie privée **PEUT** détailler, sans s'y limiter, ce qui suit : • Rôles et responsabilités; • Définitions des données; • Principes de la gestion de l'information et de la protection de la vie privée; • Autorisations et cadres en vigueur; • Signalement des infractions.	X			
62	Un plan de gestion de l'information et de protection de la vie privée **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Rôles et responsabilités; • Définitions des données; • Principes de la gestion de l'information et de la protection de la vie privée; • Autorisations et cadres en vigueur; • Signalement des infractions.		X	X	

63	Une politique de maintenance des systèmes **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
64	Une politique de maintenance des systèmes **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
65	Un plan de maintenance des systèmes **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
66	Un plan de maintenance des systèmes **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	
67	Un plan de maintenance des systèmes **PEUT** détailler, sans s'y limiter, ce qui suit : • Ordonnancement, documentation et examen des dossiers de maintenance; • Utilisation d'activités de maintenance automatisée; • Inspection, restriction, utilisation et mise à jour des outils de maintenance; • Activités de maintenance non locales; • Rapidité de la maintenance.	X			
68	Un plan de maintenance des systèmes **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Ordonnancement, documentation et examen des dossiers de maintenance; • Utilisation d'activités de maintenance automatisée; • Inspection, restriction, utilisation et mise à jour des outils de maintenance; • Activités de maintenance non locales; • Rapidité de la maintenance.		X	X	

69	Une politique de contrôle de l'accès technique **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
70	Une politique de contrôle de l'accès technique **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
71	Un plan de contrôle de l'accès technique **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
72	Un plan de contrôle de l'accès technique **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	
73	Un plan de contrôle de l'accès technique **PEUT** détailler, sans s'y limiter, ce qui suit : • Gestion des comptes; • Exécution de l'accès; • Exécution du flux d'information; • Séparation des tâches; • Droit d'accès minimal; • Tentatives de connexion infructueuses; • Accès à distance; • Accès sans fil; • Notifications système; • Gestion des sessions; • Attributs de la sécurité et de la protection de la vie privée; • Utilisation de systèmes externes; • Protection de l'exploration des données.	X			

74	Un plan de contrôle de l'accès technique **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Gestion des comptes; • Exécution de l'accès; • Exécution du flux d'information; • Séparation des tâches; • Droit d'accès minimal; • Tentatives de connexion infructueuses; • Accès à distance; • Accès sans fil; • Notifications système; • Gestion des sessions; • Attributs de la sécurité et de la protection de la vie privée; • Utilisation de systèmes externes; • Protection de l'exploration des données.		X	X	
75	Une politique de contrôle de l'accès physique **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
76	Une politique de contrôle de l'accès physique **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
77	Un plan de contrôle de l'accès physique **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
78	Un plan de contrôle de l'accès physique **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	

79	Un plan de contrôle de l'accès physique **PEUT** détailler, sans s'y limiter, ce qui suit : • Autorisation; • Gestion du contrôle; • Surveillance; • Accès des visiteurs; • Surveillance et suivi des actifs; • Autres sites de travail.	X			
80	Un plan de contrôle de l'accès physique **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Autorisation; • Gestion du contrôle; • Surveillance; • Accès des visiteurs; • Surveillance et suivi des actifs; • Autres sites de travail.		X	X	
81	Une politique sur la sécurité du personnel **PEUT** être élaborée, documentée et disséminée au sein de l'organisation.	X			
82	Une politique sur la sécurité du personnel **DOIT** être élaborée, documentée et disséminée au sein de l'organisation.		X	X	
83	Un plan sur la sécurité du personnel **PEUT** être élaboré, documenté et disséminé au sein de l'organisation.	X			
84	Un plan sur la sécurité du personnel **DOIT** être élaboré, documenté et disséminé au sein de l'organisation.		X	X	

85	Un plan sur la sécurité du personnel **PEUT** détailler, sans s'y limiter, ce qui suit : • Contrôle du personnel; • Licenciement du personnel; • Mutation du personnel; • Ententes d'accès incluant la non-divulgation, l'utilisation acceptable, les conflits d'intérêts, etc.; • Sécurité du personnel extérieur.	X			
86	Un plan sur la sécurité du personnel **DEVRAIT** détailler, sans s'y limiter, ce qui suit : • Contrôle du personnel; • Licenciement du personnel; • Mutation du personnel; • Ententes d'accès incluant la non-divulgation, l'utilisation acceptable, les conflits d'intérêts, etc.; • Sécurité du personnel extérieur.		X	X	
Référence	**Critères de conformité**				
TECH	**Exigences technologiques requises par les organisations qui desservent l'écosystème de l'identité numérique**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Il **PEUT** y avoir en place des outils et techniques qui fournissent des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie des systèmes d'information (p. ex., pare-feux, passerelles, systèmes de détection des intrusions au niveau de l'hôte) pour détecter et éradiquer un code malveillant.	X			

2	Il **DEVRAIT** y avoir en place des outils et techniques qui fournissent des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie des systèmes d'information (p. ex., pare-feux, passerelles, systèmes de détection des intrusions au niveau de l'hôte) pour détecter et éradiquer un code malveillant.		X		
3	Il **DOIT** y avoir en place des outils et techniques qui fournissent des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie des systèmes d'information (p. ex., pare-feux, passerelles, systèmes de détection des intrusions au niveau de l'hôte) pour détecter et éradiquer un code malveillant.			X	
4	Les outils de protection contre les codes malveillants **PEUVENT** mettre à jour les mécanismes de protection contre les codes malveillants conformément à la politique.	X			
5	Les outils de protection contre les codes malveillants **DEVRAIENT** mettre à jour les mécanismes de protection contre les codes malveillants conformément à la politique.		X		
6	Les outils de protection contre les codes malveillants **DOIVENT** mettre à jour les mécanismes de protection contre les codes malveillants conformément à la politique.			X	
7	Le système d'information **DEVRAIT** assurer la confidentialité et l'intégrité de l'information sur l'identité numérique au repos et en transit. Veuillez vous reporter au Profil de conformité de la vie privée du CCP pour connaître les exigences connexes supplémentaires dans ce domaine.	X			

8	Le système d'information **DOIT** assurer la confidentialité et l'intégrité de l'information sur l'identité numérique au repos et en transit. Veuillez vous reporter au Profil de conformité de la vie privée du CCP pour connaître les exigences connexes supplémentaires dans ce domaine.		X	X	
9	Le système d'information **PEUT** assurer l'authenticité des sessions de communication (p. ex., identifiants de sessions aléatoires uniques, invalidation des identifiants de session à la déconnexion, application appropriée des certificats de cryptage approuvés basés sur la politique de l'entreprise).	X			
10	Le système d'information **DEVRAIT** assurer l'authenticité des sessions de communication (p. ex., identifiants de sessions aléatoires uniques, invalidation des identifiants de session à la déconnexion, application appropriée des certificats de cryptage approuvés basés sur la politique de l'entreprise).		X		
11	Le système d'information **DOIT** assurer l'authenticité des sessions de communication (p. ex., identifiants de sessions aléatoires uniques, invalidation des identifiants de session à la déconnexion, application appropriée des certificats de cryptage approuvés basés sur la politique de l'entreprise).			X	
12	Le système d'information **PEUT** invalider les identifiants de session à la déconnexion de l'utilisateur ou toute autre fin de session. Veuillez vous référer également à la section Fin de session du Profil de conformité de l'authentification du CCP pour plus de contexte.	X			

13	Le système d'information **DEVRAIT** invalider les identifiants de session à la déconnexion de l'utilisateur ou toute autre fin de session. Veuillez vous référer également à la section Fin de session du Profil de conformité de l'authentification du CCP pour plus de contexte.		X		
14	Le système d'information **DOIT** invalider les identifiants de session à la déconnexion de l'utilisateur ou toute autre fin de session. Veuillez vous référer également à la section Fin de session du Profil de conformité de l'authentification du CCP pour plus de contexte.			X	
15	L'organisation **PEUT** délivrer des certificats de clés publiques conformément à la politique sur les certificats définie par l'entreprise ou obtenir des certificats de clés publiques auprès d'une autorité de certification ancre de confiance publique bien connue.	X			
16	L'organisation **DOIT** délivrer des certificats de clés publiques conformément à la politique sur les certificats définie par l'entreprise ou obtenir des certificats de clés publiques auprès d'une autorité de certification ancre de confiance publique bien connue.		X	X	
17	Le système d'information **PEUT** mettre fin à la connexion réseau associée à une session utilisateur, ou à une session de communication de système à système, à la fin de la session ou après une période d'inactivité prédéfinie.	X			
18	Le système d'information **DEVRAIT** mettre fin à la connexion réseau associée à une session utilisateur, ou à une session de communication de système à système, à la fin de la session ou après une période d'inactivité prédéfinie.		X		

19	Le système d'information **DOIT** mettre fin à la connexion réseau associée à une session utilisateur, ou à une session de communication de système à système, à la fin de la session ou après une période d'inactivité prédéfinie.			X	
20	L'organisation **PEUT** employer des outils de vérification de l'intégrité pour déceler les changements non autorisés apportés aux logiciels, aux micrologiciels et à l'information.	X			
21	L'organisation **DEVRAIT** employer des outils de vérification de l'intégrité pour déceler les changements non autorisés apportés aux logiciels, aux micrologiciels et à l'information.		X	X	
22	Des outils **PEUVENT** être en place pour surveiller les communications entrantes et sortantes afin de déceler les activités ou conditions inhabituelles ou non autorisées.	X			
23	Des outils **DEVRAIENT** être en place pour surveiller les communications entrantes et sortantes afin de déceler les activités ou conditions inhabituelles ou non autorisées.		X		
24	Des outils **DOIVENT** être en place pour surveiller les communications entrantes et sortantes afin de déceler les activités ou conditions inhabituelles ou non autorisées.			X	

25	Des outils, appareils et techniques de surveillance et d'alerte **PEUVENT** être employés pour amener le système d'information à : • Déceler les attaques et indications d'attaques potentielles; • Déceler les connexions locales, réseau et à distance non autorisées; • Déceler les communications entrantes et sortantes pour des activités ou des conditions inhabituelles ou non autorisées; • Atténuer la possibilité de menaces internes et d'exfiltration de données. La section Surveillance des menaces du Profil de conformité de l'authentification du CCP fournit des orientations supplémentaires.	X			
26	Des outils, appareils et techniques de surveillance et d'alerte **DEVRAIENT** être employés pour amener le système d'information à : • Déceler les attaques et indications d'attaques potentielles; • Déceler les connexions locales, réseau et à distance non autorisées; • Déceler les communications entrantes et sortantes pour des activités ou des conditions inhabituelles ou non autorisées; • Atténuer la possibilité de menaces internes et d'exfiltration de données. La section Surveillance des menaces du Profil de conformité de l'authentification du CCP fournit des orientations supplémentaires.		X		

27	Des outils, appareils et techniques de surveillance et d'alerte **DOIVENT** être employés pour amener le système d'information à : • Déceler les attaques et indications d'attaques potentielles; • Déceler les connexions locales, réseau et à distance non autorisées; • Déceler les communications entrantes et sortantes pour des activités ou des conditions inhabituelles ou non autorisées; • Atténuer la possibilité de menaces internes et d'exfiltration de données. La section Surveillance des menaces du Profil de conformité de l'authentification du CCP fournit des orientations supplémentaires.			X	
28	Des outils, appareils et techniques de protection des frontières **PEUVENT** être employés pour : • Surveiller et contrôler les communications à la frontière externe et aux principales frontières internes du système; • Mettre en place des sous-réseaux pour les composantes de systèmes accessibles au public qui sont logiquement séparées des réseaux organisationnels internes; et • Se connecter aux réseaux ou systèmes d'information externes uniquement à partir d'interfaces gérées composées d'appareils de protection des frontières arrangés conformément à une architecture de sécurité organisationnelle.	X			

29	Des outils, appareils et techniques de protection des frontières **DEVRAIENT** être employés pour : • Surveiller et contrôler les communications à la frontière externe et aux principales frontières internes du système; • Mettre en place des sous-réseaux pour les composantes de systèmes accessibles au public qui sont logiquement séparées des réseaux organisationnels internes; et • Se connecter aux réseaux ou systèmes d'information externes uniquement à partir d'interfaces gérées composées d'appareils de protection des frontières arrangés conformément à une architecture de sécurité organisationnelle.		X		

30	Des outils, appareils et techniques de protection des frontières **DOIVENT** être employés pour : • Surveiller et contrôler les communications à la frontière externe et aux principales frontières internes du système; • Mettre en place des sous-réseaux pour les composantes de systèmes accessibles au public qui sont logiquement séparées des réseaux organisationnels internes; et • Se connecter aux réseaux ou systèmes d'information externes uniquement à partir d'interfaces gérées composées d'appareils de protection des frontières arrangés conformément à une architecture de sécurité organisationnelle.			X	
31	L'organisation **PEUT** employer des outils et techniques pour se protéger contre ou limiter les effets des attaques par déni de service.	X			
32	L'organisation **DEVRAIT** employer des outils et techniques pour se protéger contre ou limiter les effets des attaques par déni de service.		X		
33	L'organisation **DOIT** employer des outils et techniques pour se protéger contre ou limiter les effets des attaques par déni de service.			X	
34	Le système d'information **PEUT** identifier et authentifier d'une manière unique les utilisateurs non organisationnels, ou les processus agissant pour le compte d'utilisateurs non organisationnels, lorsque l'authentification est appropriée.	X			

35	Le système d'information **DEVRAIT** identifier et authentifier d'une manière unique les utilisateurs non organisationnels, ou les processus agissant pour le compte d'utilisateurs non organisationnels, lorsque l'authentification est appropriée.		X		
36	Le système d'information **DOIT** identifier et authentifier d'une manière unique les utilisateurs non organisationnels, ou les processus agissant pour le compte d'utilisateurs non organisationnels, lorsque l'authentification est appropriée.			X	
37	L'organisation **PEUT** faire en sorte que les authentificateurs statiques non chiffrés ne soient pas intégrés dans des applications ou scripts d'accès ou encore entreposés dans des touches de fonction. Les sections sur l'émission et l'authentification des justificatifs du Profil de conformité de l'authentification du CCP fournissent des orientations supplémentaires.	X			
38	L'organisation **DOIT** faire en sorte que les authentificateurs statiques non chiffrés ne soient pas intégrés dans des applications ou scripts d'accès ou encore entreposés dans des touches de fonction. Les sections sur l'émission et l'authentification des justificatifs du Profil de conformité de l'authentification du CCP fournissent des orientations supplémentaires.		X	X	
39	L'organisation **PEUT** employer des outils automatisés pour déterminer si les authentificateurs de mots de passe sont assez robustes pour satisfaire aux exigences de la politique de sécurité de l'organisation. Les sections sur l'émission et l'authentification des justificatifs du Profil de conformité de l'authentification du CCP fournissent des orientations supplémentaires.	X			

40	L'organisation **DEVRAIT** employer des outils automatisés pour déterminer si les authentificateurs de mots de passe sont assez robustes pour satisfaire aux exigences de la politique de sécurité de l'organisation. Les sections sur l'émission et l'authentification des justificatifs du Profil de conformité de l'authentification du CCP fournissent des orientations supplémentaires.		X	X	
41	L'organisation **PEUT** mettre en place des outils pour se défendre contre les attaques consistant à rejouer l'authentification et à deviner les secrets pour obtenir accès au réseau. La section sur l'atténuation des menaces du Profil de conformité de l'authentification du CCP fournit des orientations supplémentaires.	X			
42	L'organisation **DEVRAIT** mettre en place des outils pour se défendre contre les attaques consistant à rejouer l'authentification et à deviner les secrets pour obtenir accès au réseau. La section sur l'atténuation des menaces du Profil de conformité de l'authentification du CCP fournit des orientations supplémentaires.		X		
43	L'organisation **DOIT** mettre en place des outils pour se défendre contre les attaques consistant à rejouer l'authentification et à deviner les secrets pour obtenir accès au réseau. La section sur l'atténuation des menaces du Profil de conformité de l'authentification du CCP fournit des orientations supplémentaires.			X	

44	L'organisation **PEUT** analyser les changements apportés au système d'information pour déterminer les impacts potentiels sur la sécurité avant de mettre en place des changements.	X			
45	L'organisation **DEVRAIT** analyser les changements apportés au système d'information pour déterminer les impacts potentiels sur la sécurité avant de mettre en place des changements.		X		
46	L'organisation **DOIT** analyser les changements apportés au système d'information pour déterminer les impacts potentiels sur la sécurité avant de mettre en place des changements.			X	
47	L'organisation **PEUT** avoir en place une technologie de détection et de signalement des intrusions pour toutes les composantes technologiques utilisées pour la prestation et la consommation de l'identité numérique.	X			
48	L'organisation **DEVRAIT** avoir en place une technologie de détection et de signalement des intrusions pour toutes les composantes technologiques utilisées pour la prestation et la consommation de l'identité numérique.		X		
49	L'organisation **DOIT** avoir en place une technologie de détection et de signalement des intrusions pour toutes les composantes technologiques utilisées pour la prestation et la consommation de l'identité numérique.			X	
50	L'organisation **PEUT** évaluer et maintenir d'une manière proactive le caractère adéquat des systèmes et services, notamment les niveaux de ressources et l'état à jour des niveaux de correction du matériel et du système d'exploitation.	X			

51	L'organisation **DOIT** évaluer et maintenir d'une manière proactive le caractère adéquat des systèmes et services, notamment les niveaux de ressources et l'état à jour des niveaux de correction du matériel et du système d'exploitation.		X	X	
52	Le système d'information **PEUT** avoir des mécanismes de sécurité pour protéger sa mémoire contre l'exécution de codes non autorisée.	X			
53	Le système d'information **DEVRAIT** avoir des mécanismes de sécurité pour protéger sa mémoire contre l'exécution de codes non autorisée.		X	X	
54	Le système d'information **PEUT** déployer des outils cryptographiques et d'autres méthodes et technologie de protection des données pour faire en sorte que la protection de la vie privée soit maintenue pendant les échanges d'information. Le profil de conformité de la protection de la vie privée du CCP fournit des orientations supplémentaires.	X			
55	Le système d'information **DEVRAIT** déployer des outils cryptographiques et d'autres méthodes et technologie de protection des données pour faire en sorte que la protection de la vie privée soit maintenue pendant les échanges d'information. Le profil de conformité de la protection de la vie privée du CCP fournit des orientations supplémentaires.		X		

56	Le système d'information **DOIT** déployer des outils cryptographiques et d'autres méthodes et technologie de protection des données pour faire en sorte que la protection de la vie privée soit maintenue pendant les échanges d'information. Le profil de conformité de la protection de la vie privée du CCP fournit des orientations supplémentaires.			X	
57	Les outils cryptographiques utilisés pour faire en sorte que la protection de la vie privée soit maintenue pendant les échanges d'information **PEUVENT** remplir une norme de validation reconnue par l'industrie (p. ex., FIPS 140-2 ou l'équivalent).	X			
58	Les outils cryptographiques utilisés pour faire en sorte que la protection de la vie privée soit maintenue pendant les échanges d'information **DEVRAIENT** remplir une norme de validation reconnue par l'industrie (p. ex., FIPS 140-2 ou l'équivalent).		X	X	
	Critères de conformité				
OPS	**Exigences opérationnelles pour les organisations qui desservent l'écosystème de l'identité numérique.**	**LOA1**	**LOA2**	**LOA3**	**LOA4**
1	Il **PEUT** y avoir une norme opérationnelle exigeant que les développeurs suivent un processus de développement documenté qui couvre explicitement les exigences en matière de sécurité, qui identifie les normes et séries d'outils technologiques à utiliser, et qui identifie les configurations spécifiques des outils de travail à utiliser.	X			

2	Il **DEVRAIT** y avoir une norme opérationnelle exigeant que les développeurs suivent un processus de développement documenté qui couvre explicitement les exigences en matière de sécurité, qui identifie les normes et séries d'outils technologiques à utiliser, et qui identifie les configurations spécifiques des outils de travail à utiliser.		X		
3	Il **DOIT** y avoir une norme opérationnelle exigeant que les développeurs suivent un processus de développement documenté qui couvre explicitement les exigences en matière de sécurité, qui identifie les normes et séries d'outils technologiques à utiliser, et qui identifie les configurations spécifiques des outils de travail à utiliser.			X	
4	L'organisation **PEUT** gérer les composantes du système en utilisant le cycle de vie défini pour le développement de son système qui incorpore les préoccupations liées à la sécurité.	X			
5	L'organisation **DEVRAIT** gérer les composantes du système en utilisant le cycle de vie défini pour le développement de son système qui incorpore les préoccupations liées à la sécurité.		X		
6	L'organisation **DOIT** gérer les composantes du système en utilisant le cycle de vie défini pour le développement de son système qui incorpore les préoccupations liées à la sécurité.			X	
7	L'organisation **PEUT** avoir des calendriers officiels de rétention et d'élimination de l'information assujettis à une surveillance et un audit pour assurer la conformité avec son plan de gestion de l'information.	X			

8	L'organisation **DEVRAIT** avoir des calendriers officiels de rétention et d'élimination de l'information assujettis à une surveillance et un audit pour assurer la conformité avec son plan de gestion de l'information.		X		
9	L'organisation **DOIT** avoir des calendriers officiels de rétention et d'élimination de l'information assujettis à une surveillance et un audit pour assurer la conformité avec son plan de gestion de l'information.			X	
10	Des systèmes et processus officiels de gouvernance technologique (p. ex., risque et conformité de la gouvernance (RCG) ou gestion intégrée du risque (GIR)) **PEUVENT** être en place, lesquels incluent des contrôles continus de la surveillance et de l'audit des activités.	X			
11	Des systèmes et processus officiels de gouvernance technologique (p. ex., risque et conformité de la gouvernance (RCG) ou gestion intégrée du risque (GIR)) **DEVRAIENT** être en place, lesquels incluent des contrôles continus de la surveillance et de l'audit des activités.		X	X	
12	L'organisation **PEUT** tester périodiquement la restauration ou le rétablissement des composantes du système conformément aux exigences définies dans le plan d'urgence.	X			
13	L'organisation **DEVRAIT** tester périodiquement la restauration ou le rétablissement des composantes du système conformément aux exigences définies dans le plan d'urgence.		X		
14	L'organisation **DOIT** tester périodiquement la restauration ou le rétablissement des composantes du système conformément aux exigences définies dans le plan d'urgence.			X	

15	Une mise à l'essai, une évaluation et une mise à jour complète du plan d'urgence **PEUVENT** être effectuées sur une base régulière (p. ex., bisannuelle ou annuelle de préférence).	X			
16	Une mise à l'essai, une évaluation et une mise à jour complète du plan d'urgence **DEVRAIENT** être effectuées sur une base régulière (p. ex., bisannuelle ou annuelle de préférence).		X		
17	Une mise à l'essai, une évaluation et une mise à jour complète du plan d'urgence **DOIVENT** être effectuées sur une base régulière (p. ex., bisannuelle ou annuelle de préférence).			X	
18	Des procédures de sauvegarde automatisées complètes **PEUVENT** être en place. Cela inclut la sauvegarde de : • L'information au niveau des utilisateurs; • L'information au niveau du système; • La documentation sur le système et la sécurité.	X			
19	Des procédures de sauvegarde automatisées complètes **DEVRAIENT** être en place. Cela inclut la sauvegarde de : • L'information au niveau des utilisateurs; • L'information au niveau du système; • La documentation sur le système et la sécurité.		X		

20	Des procédures de sauvegarde automatisées complètes **DOIVENT** être en place. Cela inclut la sauvegarde de : • L'information au niveau des utilisateurs; • L'information au niveau du système; • La documentation sur le système et la sécurité.			X	
21	Les sauvegardes des logiciels et des données opérationnelles essentiels du système **PEUVENT** être entreposées dans une installation qui est physiquement distincte du système opérationnel.	X			
22	Les sauvegardes des logiciels et des données opérationnelles essentiels du système **DEVRAIENT** être entreposées dans une installation qui est physiquement distincte du système opérationnel.		X	X	
23	Des processus et procédures **PEUVENT** être en place pour protéger la confidentialité, l'intégrité et la disponibilité de l'information sauvegardée dans des endroits d'entreposage conformément à la politique de gouvernance et de gestion du risque.	X			
24	Des processus et procédures **DOIVENT** être en place pour protéger la confidentialité, l'intégrité et la disponibilité de l'information sauvegardée dans des endroits d'entreposage conformément à la politique de gouvernance et de gestion du risque.		X	X	
25	Il **PEUT** y avoir un programme visant à tester continuellement la vulnérabilité des composantes du système et des logiciels utilisés pour la prestation de services à l'écosystème de l'identité numérique.	X			

26	Il **DEVRAIT** y avoir un programme visant à tester continuellement la vulnérabilité des composantes du système et des logiciels utilisés pour la prestation de services à l'écosystème de l'identité numérique.		X		
27	Il **DOIT** y avoir un programme visant à tester continuellement la vulnérabilité des composantes du système et des logiciels utilisés pour la prestation de services à l'écosystème de l'identité numérique.			X	
28	Les techniques de balayage des vulnérabilités et les outils qui mettent aussitôt à jour les vulnérabilités à balayer **PEUVENT** être employés et appliqués d'une manière automatisée.	X			
29	Les techniques de balayage des vulnérabilités et les outils qui mettent aussitôt à jour les vulnérabilités à balayer **DEVRAIENT** être employés et appliqués d'une manière automatisée.		X	X	
30	L'organisation **PEUT** mener des essais de pénétration réguliers avec toutes les composantes utilisées pour fournir des services à l'écosystème de l'identité numérique.	X			
31	L'organisation **DEVRAIT** mener des essais de pénétration réguliers avec toutes les composantes utilisées pour fournir des services à l'écosystème de l'identité numérique.		X		
32	L'organisation **DOIT** mener des essais de pénétration réguliers avec toutes les composantes utilisées pour fournir des services à l'écosystème de l'identité numérique.			X	
33	Les méthodes d'accès à distance **PEUVENT** être contrôlées et surveillées.	X			
34	Les méthodes d'accès à distance **DEVRAIENT** être contrôlées et surveillées.		X		

35	Les méthodes d'accès à distance **DOIVENT** être contrôlées et surveillées.			X	
36	L'accès à distance **PEUT** être acheminé par des points de contrôle d'accès au réseau gérés.	X			
37	L'accès à distance **DEVRAIT** être acheminé par des points de contrôle d'accès au réseau gérés.		X		
38	L'accès à distance **DOIT** être acheminé par des points de contrôle d'accès au réseau gérés.			X	
39	Il **PEUT** y avoir des systèmes automatisés (p. ex., approvisionnement, attribution et gestion des droits) pour soutenir la gestion des comptes du système d'information.	X			
40	Il **DEVRAIT** y avoir des systèmes automatisés (p. ex., approvisionnement, attribution et gestion des droits) pour soutenir la gestion des comptes du système d'information.		X	X	
41	Des processus **PEUVENT** être en place pour désactiver automatiquement les comptes inactifs après une période d'inactivité définie basée sur la politique de contrôle du système d'information.	X			
42	Des processus **DEVRAIENT** être en place pour désactiver automatiquement les comptes inactifs après une période d'inactivité définie basée sur la politique de contrôle du système d'information.		X		
43	Des processus **DOIVENT** être en place pour désactiver automatiquement les comptes inactifs après une période d'inactivité définie basée sur la politique de contrôle du système d'information.			X	
44	Il **PEUT** y avoir un dossier système qui est créé automatiquement pour la création, la modification, l'activation, la désactivation et la suppression de comptes.	X			

45	Il **DEVRAIT** y avoir un dossier système qui est créé automatiquement pour la création, la modification, l'activation, la désactivation et la suppression de comptes.		X		
46	Il **DOIT** y avoir un dossier système qui est créé automatiquement pour la création, la modification, l'activation, la désactivation et la suppression de comptes.			X	
47	Des contrôles **PEUVENT** être en place pour obliger les comptes du système à fermer leur session après une période d'inactivité spécifique.	X			
48	Des contrôles **DEVRAIENT** être en place pour obliger les comptes du système à fermer leur session après une période d'inactivité spécifique.		X		
49	Des contrôles **DOIVENT** être en place pour obliger les comptes du système à fermer leur session après une période d'inactivité spécifique.			X	
50	Des comptes d'utilisateurs privilégiés **PEUVENT** être créés et administrés en utilisant un plan d'accès basé sur les rôles.	X			
51	Des comptes d'utilisateurs privilégiés **DEVRAIENT** être créés et administrés en utilisant un plan d'accès basé sur les rôles.		X		
52	Des comptes d'utilisateurs privilégiés **DOIVENT** être créés et administrés en utilisant un plan d'accès basé sur les rôles.			X	
53	Des composantes technologiques de surveillance et d'alarme **PEUVENT** être configurées pour générer des notifications en temps réel et amorcer des processus pour atténuer les menaces en temps opportun.	X			
54	Des composantes technologiques de surveillance et d'alarme **DEVRAIENT** être configurées pour générer des notifications en temps réel et amorcer des processus pour atténuer les menaces en temps opportun.		X		

55	Des composantes technologiques de surveillance et d'alarme **DOIVENT** être configurées pour générer des notifications en temps réel et amorcer des processus pour atténuer les menaces en temps opportun.			X	
56	Des processus automatisés ou manuels **PEUVENT** être en place pour annuler des justificatifs partagés ou de groupe quand des membres quittent le groupe.	X			
57	Des processus automatisés ou manuels **DEVRAIENT** être en place pour annuler des justificatifs partagés ou de groupe quand des membres quittent le groupe.		X		
58	Des processus automatisés ou manuels **DOIVENT** être en place pour annuler des justificatifs partagés ou de groupe quand des membres quittent le groupe.			X	
59	Des processus automatisés **PEUVENT** être en place pour limiter les tentatives de connexion infructueuses et verrouiller le compte ou le nœud jusqu'à ce qu'il soit libéré par un administrateur ou un processus administratif (p. ex., réinitialisation forcée des mots de passe).	X			
60	Des processus automatisés **DEVRAIENT** être en place pour limiter les tentatives de connexion infructueuses et verrouiller le compte ou le nœud jusqu'à ce qu'il soit libéré par un administrateur ou un processus administratif (p. ex., réinitialisation forcée des mots de passe).		X		
61	Des processus automatisés **DOIVENT** être en place pour limiter les tentatives de connexion infructueuses et verrouiller le compte ou le nœud jusqu'à ce qu'il soit libéré par un administrateur ou un processus administratif (p. ex., réinitialisation forcée des mots de passe).			X	

62	Le système **PEUT** empêcher son accès après une période d'inactivité définie et exige que l'utilisateur rétablisse l'accès à l'aide de procédures d'identification et d'authentification établies. Le profil d'authentification du CCP fournit des orientations supplémentaires.	X			
63	Le système **DEVRAIT** empêcher son accès après une période d'inactivité définie et exige que l'utilisateur rétablisse l'accès à l'aide de procédures d'identification et d'authentification établies. Le profil d'authentification du CCP fournit des orientations supplémentaires.		X		
64	Le système **DOIT** empêcher son accès après une période d'inactivité définie et exige que l'utilisateur rétablisse l'accès à l'aide de procédures d'identification et d'authentification établies. Le profil d'authentification du CCP fournit des orientations supplémentaires.			X	
65	Si les systèmes d'information permettent des sessions simultanées, des processus **PEUVENT** être en place pour limiter le nombre de sessions simultanées pour chaque type de compte défini conformément à la politique de sécurité et d'accès de l'organisation.	X			
66	Si les systèmes d'information permettent des sessions simultanées, des processus **DEVRAIENT** être en place pour limiter le nombre de sessions simultanées pour chaque type de compte défini conformément à la politique de sécurité et d'accès de l'organisation.		X		

67	Si les systèmes d'information permettent des sessions simultanées, des processus **DOIVENT** être en place pour limiter le nombre de sessions simultanées pour chaque type de compte défini conformément à la politique de sécurité et d'accès de l'organisation.			X	
68	Les organisations **PEUVENT** affecter des gestionnaires de comptes aux comptes des systèmes d'information et établir des conditions officielles pour les membres de groupes et de rôles accordant des autorisations d'accès.	X			
69	Les organisations **DEVRAIENT** affecter des gestionnaires de comptes aux comptes des systèmes d'information et établir des conditions officielles pour les membres de groupes et de rôles accordant des autorisations d'accès.		X		
70	Les organisations **DOIVENT** affecter des gestionnaires de comptes aux comptes des systèmes d'information et établir des conditions officielles pour les membres de groupes et de rôles accordant des autorisations d'accès.			X	
71	Il **PEUT** y avoir en place des processus documentés qui exigent des approbations pour la création de comptes et ont des procédures documentées pour surveiller l'utilisation des comptes du système d'information.	X			
72	Il **DEVRAIT** y avoir en place des processus documentés qui exigent des approbations pour la création de comptes et ont des procédures documentées pour surveiller l'utilisation des comptes du système d'information.		X		

73	Il **DOIT** y avoir en place des processus documentés qui exigent des approbations pour la création de comptes et ont des procédures documentées pour surveiller l'utilisation des comptes du système d'information.			X	
74	L'organisation **PEUT** adhérer au principe du droit d'accès minimal qui permet uniquement des accès autorisés pour les utilisateurs (ou les processus agissant pour le compte des utilisateurs) qui sont nécessaires pour accomplir les tâches assignées conformément aux missions et fonctions commerciales. Cela inclut : • La configuration des produits logiciels pour refléter le mode le plus restrictif conformément aux exigences opérationnelles; • L'accès limité aux données de l'identité numérique à l'aide de configuration qui fournissent un accès explicite uniquement aux données requises par la personne ou le système qui en a besoin; et • Les configurations de réseaux et d'appareils de communication qui limitent l'accès aux seules composantes de systèmes ou services nécessaires.	X			

75	L'organisation **DEVRAIT** adhérer au principe du droit d'accès minimal qui permet uniquement des accès autorisés pour les utilisateurs (ou les processus agissant pour le compte des utilisateurs) qui sont nécessaires pour accomplir les tâches assignées conformément aux missions et fonctions commerciales. Cela inclut : • La configuration des produits logiciels pour refléter le mode le plus restrictif conformément aux exigences opérationnelles; • L'accès limité aux données de l'identité numérique à l'aide de configuration qui fournissent un accès explicite uniquement aux données requises par la personne ou le système qui en a besoin; et • Les configurations de réseaux et d'appareils de communication qui limitent l'accès aux seules composantes de systèmes ou services nécessaires.		X		

76	L'organisation **DOIT** adhérer au principe du droit d'accès minimal qui permet uniquement des accès autorisés pour les utilisateurs (ou les processus agissant pour le compte des utilisateurs) qui sont nécessaires pour accomplir les tâches assignées conformément aux missions et fonctions commerciales. Cela inclut : • La configuration des produits logiciels pour refléter le mode le plus restrictif conformément aux exigences opérationnelles; • L'accès limité aux données de l'identité numérique à l'aide de configuration qui fournissent un accès explicite uniquement aux données requises par la personne ou le système qui en a besoin; et • Les configurations de réseaux et d'appareils de communication qui limitent l'accès aux seules composantes de systèmes ou services nécessaires.			X	
77	L'organisation **PEUT** maintenir la disponibilité de l'information si des utilisateurs perdent des clés cryptographiques.	X			
78	L'organisation **DEVRAIT** maintenir la disponibilité de l'information si des utilisateurs perdent des clés cryptographiques.		X	X	
79	Le système d'information **PEUT** mettre en place des mécanismes cryptographiques pour empêcher la divulgation non autorisée de renseignements et déceler les changements à l'information sur l'identité numérique pendant la transmission.	X			

80	Le système d'information **DEVRAIT** mettre en place des mécanismes cryptographiques pour empêcher la divulgation non autorisée de renseignements et déceler les changements à l'information sur l'identité numérique pendant la transmission.		X		
81	Le système d'information **DOIT** mettre en place des mécanismes cryptographiques pour empêcher la divulgation non autorisée de renseignements et déceler les changements à l'information sur l'identité numérique pendant la transmission.			X	
82	L'organisation **PEUT** autoriser des connexions extérieures entre les systèmes d'information basées sur des ententes de sécurité officielles comme définies dans la politique de sécurité de l'organisation.	X			
83	L'organisation **DEVRAIT** autoriser des connexions extérieures entre les systèmes d'information basées sur des ententes de sécurité officielles comme définies dans la politique de sécurité de l'organisation.		X		
84	L'organisation **DOIT** autoriser des connexions extérieures entre les systèmes d'information basées sur des ententes de sécurité officielles comme définies dans la politique de sécurité de l'organisation.			X	
85	Pour chaque connexion externe entre des systèmes d'information, les caractéristiques de l'interface, les exigences de sécurité et la nature de l'information **PEUVENT** être documentées.	X			
86	Pour chaque connexion externe entre des systèmes d'information, les caractéristiques de l'interface, les exigences de sécurité et la nature de l'information **DEVRAIENT** être documentées.		X		

87	Pour chaque connexion externe entre des systèmes d'information, les caractéristiques de l'interface, les exigences de sécurité et la nature de l'information **DOIVENT** être documentées.			X	
88	Un historique des changements apportés à l'entente ou aux caractéristiques de l'interface **PEUT** être maintenu pour les connexions externes entre des systèmes d'information.	X			
89	Un historique des changements apportés à l'entente ou aux caractéristiques de l'interface **DEVRAIT** être maintenu pour les connexions externes entre des systèmes d'information.		X	X	
90	Des connexions internes entre les composantes des systèmes d'information **PEUVENT** être documentées en saisissant les caractéristiques, des interfaces, les exigences de sécurité et la nature de l'information communiquée.	X			
91	Des connexions internes entre les composantes des systèmes d'information **DEVRAIENT** être documentées en saisissant les caractéristiques, des interfaces, les exigences de sécurité et la nature de l'information communiquée.		X		
92	Des connexions internes entre les composantes des systèmes d'information **DOIVENT** être documentées en saisissant les caractéristiques, des interfaces, les exigences de sécurité et la nature de l'information communiquée.			X	
93	Un historique des changements apportés aux caractéristiques de l'interface, aux exigences de sécurité et à la nature de l'information communiquée **PEUT** être maintenu pour les connexions internes entre les composantes des systèmes d'information.	X			

94	Un historique des changements apportés aux caractéristiques de l'interface, aux exigences de sécurité et à la nature de l'information communiquée **DEVRAIT** être maintenu pour les connexions internes entre les composantes des systèmes d'information.		X	X	
95	Des processus **PEUVENT** être en place pour avoir des autorisations approuvées pour contrôler le flux d'information à l'intérieur du système et entre des systèmes interconnectés basés sur la politique de sécurité de l'organisation.	X			
96	Des processus **DEVRAIENT** être en place pour avoir des autorisations approuvées pour contrôler le flux d'information à l'intérieur du système et entre des systèmes interconnectés basés sur la politique de sécurité de l'organisation.		X		
97	Des processus **DOIVENT** être en place pour avoir des autorisations approuvées pour contrôler le flux d'information à l'intérieur du système et entre des systèmes interconnectés basés sur la politique de sécurité de l'organisation.			X	
98	L'organisation **PEUT** employer des mécanismes automatisés pour que le personnel de sécurité autorisé ait accès aux alertes de sécurité et aux avis.	X			
99	L'organisation **DEVRAIT** employer des mécanismes automatisés pour que le personnel de sécurité autorisé ait accès aux alertes de sécurité et aux avis.		X	X	
100	L'organisation **PEUT** recevoir sur une base permanente des alertes, avis et directives de sécurité provenant d'autorités externes reconnues (p. ex., fournisseurs, partenaires d'affaires, partenaires de la chaîne d'approvisionnement, autorités de sécurité externes, etc.) et générer au besoin des alertes, avis et directives de sécurité internes.	X			

101	L'organisation **DEVRAIT** recevoir sur une base permanente des alertes, avis et directives de sécurité provenant d'autorités externes reconnues (p. ex., fournisseurs, partenaires d'affaires, partenaires de la chaîne d'approvisionnement, autorités de sécurité externes, etc.) et générer au besoin des alertes, avis et directives de sécurité internes.		X	X	
102	L'organisation **PEUT :** • Déceler, signaler et corriger les failles du système d'information; • Tester les mises à jour des logiciels et micrologiciels reliées à la correction des failles pour déterminer l'efficacité et les éventuels effets secondaires avant l'installation; • Installer des mises à jour de logiciels et micrologiciels ayant trait à la sécurité dans une certaine période, suivant le lancement, définie par la politique sur la sécurité de l'organisation; et • Incorporer la correction des failles dans le processus de gestion de la configuration organisationnelle.	X			

103	L'organisation **DEVRAIT :** • Déceler, signaler et corriger les failles du système d'information; • Tester les mises à jour des logiciels et micrologiciels reliées à la correction des failles pour déterminer l'efficacité et les éventuels effets secondaires avant l'installation; • Installer des mises à jour de logiciels et micrologiciels ayant trait à la sécurité dans une certaine période, suivant le lancement, définie par la politique sur la sécurité de l'organisation; et • Incorporer la correction des failles dans le processus de gestion de la configuration organisationnelle.		X		
104	L'organisation **DOIT :** • Déceler, signaler et corriger les failles du système d'information; • Tester les mises à jour des logiciels et micrologiciels reliées à la correction des failles pour déterminer l'efficacité et les éventuels effets secondaires avant l'installation; • Installer des mises à jour de logiciels et micrologiciels ayant trait à la sécurité dans une certaine période, suivant le lancement, définie par la politique sur la sécurité de l'organisation; et • Incorporer la correction des failles dans le processus de gestion de la configuration organisationnelle.			X	

105	Des processus officiels de gestion des changements technologiques **PEUVENT** être en place pour évaluer et gérer le risque associé à l'évolution technologique.	X			
106	Des processus officiels de gestion des changements technologiques **DEVRAIENT** être en place pour évaluer et gérer le risque associé à l'évolution technologique.		X		
107	Des processus officiels de gestion des changements technologiques **DOIVENT** être en place pour évaluer et gérer le risque associé à l'évolution technologique.			X	
108	L'organisation **PEUT** définir, documenter, approuver, et appliquer les restrictions d'accès physique et logique associées aux changements apportés au système d'information.	X			
109	L'organisation **DEVRAIT** définir, documenter, approuver, et appliquer les restrictions d'accès physique et logique associées aux changements apportés au système d'information.		X		
110	L'organisation **DOIT** définir, documenter, approuver, et appliquer les restrictions d'accès physique et logique associées aux changements apportés au système d'information.			X	

111	Les processus de gestion des changements technologiques **PEUVENT :** • Déterminer les types de changements apportés au système d'information qui sont contrôlés par la configuration; • Examiner les changements proposés au système qui sont contrôlés par la configuration et approuver ou désapprouver ces changements en tenant explicitement compte des analyses d'impact • Documenter les décisions concernant les changements de configuration associées au système d'information; • Mettre en œuvre les changements au système d'information qui sont approuvés; • Garder des dossiers des changements apportés aux systèmes d'information pour le temps spécifié dans la politique de contrôle des changements; et • Coordonner et superviser les activités de contrôle des changements de configuration par l'intermédiaire d'un organe de gouvernance constitué officiellement.	X			

112	Les processus de gestion des changements technologiques **DEVRAIENT :** • Déterminer les types de changements apportés au système d'information qui sont contrôlés par la configuration; • Examiner les changements proposés au système qui sont contrôlés par la configuration et approuver ou désapprouver ces changements en tenant explicitement compte des analyses d'impact • Documenter les décisions concernant les changements de configuration associées au système d'information; • Mettre en œuvre les changements au système d'information qui sont approuvés; • Garder des dossiers des changements apportés aux systèmes d'information pour le temps spécifié dans la politique de contrôle des changements; et • Coordonner et superviser les activités de contrôle des changements de configuration par l'intermédiaire d'un organe de gouvernance constitué officiellement.		X	X	
113	Des installations de surveillance de l'activité et de pistes d'audit **PEUVENT** être en place pour avoir un dossier de toutes les transactions reliées à l'identité numérique au sein de l'écosystème de l'identité numérique.	X			
114	Des installations de surveillance de l'activité et de pistes d'audit **DEVRAIENT** être en place pour avoir un dossier de toutes les transactions reliées à l'identité numérique au sein de l'écosystème de l'identité numérique.		X		

115	Des installations de surveillance de l'activité et de pistes d'audit **DOIVENT** être en place pour avoir un dossier de toutes les transactions reliées à l'identité numérique au sein de l'écosystème de l'identité numérique.			X	
116	Les dossiers de toutes les transactions reliées à l'identité numérique à l'intérieur de l'écosystème de l'identité numérique **PEUVENT** être protégés contre une altération et les politiques limitant l'accès appliquées.	X			
117	Les dossiers de toutes les transactions reliées à l'identité numérique à l'intérieur de l'écosystème de l'identité numérique **DEVRAIENT** être protégés contre une altération et les politiques limitant l'accès appliquées.		X		
118	Les dossiers de toutes les transactions reliées à l'identité numérique à l'intérieur de l'écosystème de l'identité numérique **DOIVENT** être protégés contre une altération et les politiques limitant l'accès appliquées.			X	
119	Les renseignements et les outils d'audit **PEUVENT** être protégés contre l'accès, la modification et la suppression non autorisés.	X			
120	Les renseignements et les outils d'audit **DEVRAIENT** être protégés contre l'accès, la modification et la suppression non autorisés.		X		
121	Les renseignements et les outils d'audit **DOIVENT** être protégés contre l'accès, la modification et la suppression non autorisés.			X	
122	Le système d'information **PEUT** avoir des mécanismes en place qui protègent contre une personne (ou un processus agissant pour le compte d'une personne) niant faussement avoir commis des actes pour être couvert par la non-répudiation.	X			

123	Le système d'information **DEVRAIT** avoir des mécanismes en place qui protègent contre une personne (ou un processus agissant pour le compte d'une personne) niant faussement avoir commis des actes pour être couvert par la non-répudiation.		X		
124	Le système d'information **DOIT** avoir des mécanismes en place qui protègent contre une personne (ou un processus agissant pour le compte d'une personne) niant faussement avoir commis des actes pour être couvert par la non-répudiation.			X	
125	Les dossiers d'audit **PEUVENT** être conservés d'une manière sécuritaire pendant la période stipulée dans la politique de l'organisation sur la rétention de l'information afin de soutenir les enquêtes après coup sur les incidents de sécurité et de répondre aux exigences réglementaires et organisationnelles en matière de rétention de l'information.	X			
126	Les dossiers d'audit **DEVRAIENT** être conservés d'une manière sécuritaire pendant la période stipulée dans la politique de l'organisation sur la rétention de l'information afin de soutenir les enquêtes après coup sur les incidents de sécurité et de répondre aux exigences réglementaires et organisationnelles en matière de rétention de l'information.		X		
127	Les dossiers d'audit **DOIVENT** être conservés d'une manière sécuritaire pendant la période stipulée dans la politique de l'organisation sur la rétention de l'information afin de soutenir les enquêtes après coup sur les incidents de sécurité et de répondre aux exigences réglementaires et organisationnelles en matière de rétention de l'information.			X	

128	Des dossiers d'audit **PEUVENT** être générés pour les transactions d'identité numérique qui contiennent de l'information déterminant le type d'événement qui est survenu, le moment où l'événement est survenu, l'endroit où l'événement est survenu, la provenance de l'événement, le résultat de l'événement et l'identité des personnes ou sujets associés à l'événement.	X			
129	Des dossiers d'audit **DEVRAIENT** être générés pour les transactions d'identité numérique qui contiennent de l'information déterminant le type d'événement qui est survenu, le moment où l'événement est survenu, l'endroit où l'événement est survenu, la provenance de l'événement, le résultat de l'événement et l'identité des personnes ou sujets associés à l'événement.		X		
130	Des dossiers d'audit **DOIVENT** être générés pour les transactions d'identité numérique qui contiennent de l'information déterminant le type d'événement qui est survenu, le moment où l'événement est survenu, l'endroit où l'événement est survenu, la provenance de l'événement, le résultat de l'événement et l'identité des personnes ou sujets associés à l'événement.			X	
131	Des dossiers d'audit **PEUVENT** être générés pour l'exécution des fonctions système privilégiées.	X			
132	Des dossiers d'audit **DEVRAIENT** être générés pour l'exécution des fonctions système privilégiées.		X		
133	Des dossiers d'audit **DOIVENT** être générés pour l'exécution des fonctions système privilégiées.			X	

134	Des processus **PEUVENT** être en place pour faire en sorte que seul le personnel autorisé puisse exécuter des fonctions privilégiées, notamment désactiver, contourner ou altérer les protections ou contre-mesures de sécurité en place.	X			
135	Des processus **DEVRAIENT** être en place pour faire en sorte que seul le personnel autorisé puisse exécuter des fonctions privilégiées, notamment désactiver, contourner ou altérer les protections ou contre-mesures de sécurité en place.		X		
136	Des processus **DOIVENT** être en place pour faire en sorte que seul le personnel autorisé puisse exécuter des fonctions privilégiées, notamment désactiver, contourner ou altérer les protections ou contre-mesures de sécurité en place.			X	
137	L'utilisation des comptes du système d'information **PEUT** être surveillée pour les signalements d'utilisation atypique et de tendances d'utilisation atypiques et/ou les comptes désactivés compte tenu du risque associé à l'utilisation atypique.	X			
138	L'utilisation des comptes du système d'information **DEVRAIT** être surveillée pour les signalements d'utilisation atypique et de tendances d'utilisation atypiques et/ou les comptes désactivés compte tenu du risque associé à l'utilisation atypique.		X		
139	L'utilisation des comptes du système d'information **DOIT** être surveillée pour les signalements d'utilisation atypique et de tendances d'utilisation atypiques et/ou les comptes désactivés compte tenu du risque associé à l'utilisation atypique.			X	

140	Des processus **PEUVENT** être en place pour appliquer les autorisations approuvées pour un accès logique aux ressources liées à l'information et aux systèmes conformément aux politiques de contrôle d'accès applicables.	X			
141	Des processus **DEVRAIENT** être en place pour appliquer les autorisations approuvées pour un accès logique aux ressources liées à l'information et aux systèmes conformément aux politiques de contrôle d'accès applicables.		X		
142	Des processus **DOIVENT** être en place pour appliquer les autorisations approuvées pour un accès logique aux ressources liées à l'information et aux systèmes conformément aux politiques de contrôle d'accès applicables.			X	
143	L'organisation **PEUT** avoir clairement identifié les intendants de données.	X			
144	L'organisation **DEVRAIT** avoir clairement identifié les intendants de données.		X	X	
145	L'organisation **PEUT** avoir une norme API documentée.	X			
146	L'organisation **DEVRAIT** avoir une norme API documentée.		X	X	

6. Références

Ce profil a été influencé par les normes ou les organes de normalisation indiqués ci-dessous. Chacune des organisations mentionnées inclut un référentiel qui contient de multiples documents ayant trait à l'établissement et au fonctionnement d'une infrastructure technique requise pour soutenir la prestation du service, dans ce cas-ci, un écosystème de l'identité numérique.

Remarque : Lorsque c'est applicable, l'unique numéro de version spécifié dans ce document s'applique à cette composante du CCP.

Les profils de conformité des composantes du CCP (les versions publiques seront publiées une fois rendues au stade final au www.diacc.ca) ont été mentionnés au stade d'ébauche :

- Profil de conformité de la composante « Authentification »
- Profil de conformité de la composante « Justificatifs (relations et attributs) »
- Profil de conformité de la composante « Avis et consentement »
- Profil de conformité de la composante « Respect de la vie privée »
- Profil de conformité de la composante « Organisation vérifiée »
- Profil de conformité de la composante « Personne vérifiée »

Gouvernement du Canada. *Directive du Conseil du Trésor du gouvernement du Canada sur les services et le numérique.* https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32601

Gouvernement du Canada. *Version 1.1 du profil du CCP lié à la fonction publique.* https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_1

United States Department of Commerce. National Institute of Standards and Technology. *Digital Identity Guidelines (NIST Special Publication 800-63 – 5 documents).* 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html

United States Department of Commerce. National Institute of Standards and Technology. *Assessing Security and Privacy Controls (NIST Special Publication 800-53 Rev. 5).* September 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ISACA. *Control Objectives for Information Technology (COBIT)*. www.isaca.org

Axelos. *IT Infrastructure Library (ITIL).* www.axelos.com

Organisation internationale de normalisation (ISO). *Critères d'évaluation pour la sécurité TI*. https://www.iso.org/standard/50341.html

US Federal Government, *Federal Risk and Authorization Management Program (FedRAMP). Voir le lien menant au référentiel*. www.fedramp.gov

Agence de l'Union européenne pour la cybersécurité (ENISA). *Voir le lien menant vers le référentiel.* https://www.enisa.europa.eu/

7. Historique des révisions

Version	Date	Auteur	Commentaire
0.01	2019-12-15	Équipe de rédaction du CCP	Ébauche initiale du cadre
0.02	2020-02-14	Équipe de rédaction du CCP	Ébauche initiale avec tout le contenu
0.03	2020-03-03	Équipe de rédaction du CCP	Ajustements basés sur une étude et un examen supplémentaires des ébauches des composantes du CCP
0.04	2020-03-30	Équipe de rédaction du CCP	Ajustements finaux pour la publication de la version préliminaire
0.05	2020-06-05	Équipe de rédaction du CCP	Mises à jour basées sur les commentaires des membres du TFEC
0.06	2020-06-29	Équipe de rédaction du CCP	Mises à jour faisant suite à une brève période d'examen supplémentaire du TFEC
1.0	2020-07-08	Équipe de rédaction du CCP	Approbation du TFEC comme recommandation préliminaire V1.0
1.1	2020-09-18	Équipe de rédaction du CCP	Mises à jour d'après les commentaires reçus pendant la période d'examen public de l'ébauche de recommandation
1.0	2020-09-30	Équipe de rédaction du CCP	Approbation du TFEC comme candidat pour une recommandation finale V1.0
1.1	2022-08-09	Rédacteur et équipe de conception de l'infrastructure du CCP	Recommandation finale V1.1 destinée à incorporer la rétroaction des essais alpha
1.1	2022-09-14	Rédacteur et équipe de conception de l'infrastructure du CCP	Approbation du TFEC comme recommandation finale V1.1

1.1.1	2023-01-19	Rédacteur et équipe de conception de l'infrastructure du CCP	Mises à jour d'après les commentaires reçus pendant la période d'examen public de la recommandation finale V1.1
1.2	2023-02-01	Rédacteur et équipe de conception de l'infrastructure du CCP	Approbation du TFEC comme candidat pour une recommandation finale V1.2
1.2	2023-04-19	Rédacteur et équipe de conception de l'infrastructure du CCP	Approuvé en tant que recommandation finale V1.0 par vote du membre de soutien du CCIAN