Ébauche de recommandations pour le profil de conformité « Infrastructure (technologie et opérations) » du CCP V1.0

Cette ébauche de recommandations a été préparée par le Comité d'experts du Cadre de confiance (TFEC) du Conseil canadien de l'identification et de l'authentification numériques (CCIAN). Le TFEC est régi par les politiques du CCIAN en matière de contrôle. Les commentaires soumis par le public sont assujettis à l'entente de contributeur du CCIAN.

Le CCIAN prévoit modifier et améliorer cette ébauche de recommandations en fonction des commentaires du public. Les commentaires ouverts ont pour but d'assurer la transparence de l'élaboration et la diversité d'un apport véritablement pancanadien. Les commentaires effectués pendant l'examen seront pris en considération en vue d'être incorporés dans la prochaine ébauche. Le CCIAN va regrouper les commentaires afin de montrer d'une façon transparente comment chacun a été traité.

Les prochaines versions du Cadre de confiance pancanadien (CCP) vont étoffer, clarifier et peaufiner le contenu de ce document.

Table des matières

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

Ce document spécifie les critères de conformité de la composante « Infrastructure (technologie et opérations) » du CCP, une composante 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 pour la composante « Infrastructure » spécifient les caractéristiques de la technologie et des opérations technologiques qui soutiennent la mise en place des systèmes fournissant des services conformes aux profils du CCP. Les critères sont exprimés dans des termes génériques, sachant que des technologies ou caractéristiques technologiques spécifiques (p. ex. protocoles) sont susceptibles d'être imposées et varieront à l'intérieur de chaque écosystème de l'identité numérique.

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

1.1. 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 que même s'il peut y avoir des raisons valables dans des circonstances particulières pour ignorer l'exigence, toutes les implications devraient être comprises et considérées avec soin avant de décider de ne pas respecter les critères de conformité ou de choisir une autre option tel que spécifié par les critères de conformité.
- **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 apparaissent en caractères **gras** et en MAJUSCULES dans ce profil de conformité.

1.2. Conventions régissant l'infrastructure

Chaque composante du CCP comporte des conventions qui assurent une uniformité d'utilisation et d'interprétation des termes et notions apparaissant dans la composante. **L'aperçu de la composante « Infrastructure (technologie et opérations) » du CCP fournit des conventions pour cette composante**. Ces conventions incluent des définitions et des 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 selon les composantes du CCP. Les lecteurs sont invités à examiner les conventions de chacune des composantes du CCP qu'ils lisent.
- Termes définis – Pour les besoins de ce profil de conformité, les termes et définitions inclus dans l'aperçu de la composante « Infrastructure » et le glossaire du CCP s'appliquent. Les principaux termes et notions décrits et définis dans cette section, l'aperçu de la composante « Infrastructure » du CCP ou le glossaire du CCP sont écrits avec une majuscule initiale dans tout ce document.
- Liens hypertextes – Il se pourrait que les versions électroniques de ce document comportent des liens hypertextes. Tous étaient accessibles au moment de la rédaction.

2. Critères de conformité de la composante « Infrastructure »

Les critères de conformité ci-dessous sont organisés selon trois grandes catégories :

- POL – exigences des politiques et des 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 reliées à la technologie
- OPS – exigences reliées aux opérations technologiques

Par souci de convivialité, les critères sont numérotés à l'intérieur de leur section et peuvent être désignés au moyen de ces identifiants (p. ex. le premier critère dans la section POL peut être appelé POL-1).

On peut tenir pour acquis que la portée des critères ne s'applique qu'aux composantes de la technologie ou des systèmes utilisées par une organisation pour fournir ou consommer un service dans le cadre de l'écosystème de l'identité numérique.

Remarque : Un groupe de travail du CCP sur le niveau d'assurance a été mis sur pied dans le but de définir la façon dont le niveau d'assurance sera traité dans tous les profils du CCP. Le traitement des éventuelles variations dans les critères de conformité en fonction du niveau d'assurance des services a été reporté dans cette version du profil. Veuillez réserver vos commentaires sur le sujet pour une ébauche améliorée de ces documents, une fois que le groupe de travail sur le niveau d'assurance aura publié ses résultats.

Référence	Critères de conformité
POL	**Exigences relatives aux politiques et plans technologiques nécessaires pour soutenir l'infrastructure utilisée pour fournir des services à l'écosystème de l'identité numérique.**

92		On **DOIT** développer, documenter et disséminer au sein de l'organisation des politiques et des plans qui couvrent : • L'évaluation des risques; • L'audit et la responsabilité; • La planification en cas de catastrophe ou d'urgence; • L'identification et l'autorisation; • La protection des systèmes et des communications; • Les interventions en cas d'incidents; • L'intégrité des systèmes et de l'information; • La gestion de l'information; • La maintenance des systèmes; • Le contrôle de l'accès technique (p. ex. verrouillage des systèmes d'exploitation, détection des intrusions, gestion des mots de passe, cryptage et gestion de l'accès aux réseaux); • Accès physique aux actifs technologiques; et • Gestion des ressources humaines s'appliquant au personnel qui interagit avec l'infrastructure de sécurité.
93		Les politiques et les plans techniques ou de gestion technologique **DOIVENT** être examinés et mis à jour régulièrement, selon un calendrier fixe approprié au contexte opérationnel de l'entreprise. Il se **PEUT** que des ajustements spéciaux soient également apportés si les conditions commerciales l'exigent. Un plan de gestion technologique couvrant l'ensemble des technologies, composantes systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique **DOIT** être élaboré. Ce plan de gestion technologique **DEVRAIT** : • Être conforme à l'architecture d'entreprise de l'organisation; • Définir les pratiques de gestion du cycle de vie des actifs; • Décrire les pratiques de gestion de la capacité et de l'utilisation; • Décrire les pratiques et paramètres d'essai de la gestion de la performance; • Décrire les exigences pour le système d'information et ses relations ou liens avec d'autres systèmes d'information; • S'aligner sur des domaines connexes dans d'autres artéfacts du plan (p. ex. gestion du risque, sécurité, gestion du changement); • Identifier les principaux risques et leurs répercussions commerciales ou opérationnelles; • Démontrer qu'il s'aligne sur un cadre de gestion des services qui est standard dans l'industrie (p. ex. ITIL). Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour faire en sorte que les changements apportés au plan de gestion technologique soient reflétés dans la mise en œuvre des composantes de systèmes connexes.

94		Une architecture de sécurité de l'information pour les systèmes d'information qui fournissent des services à l'écosystème de l'identité numérique **DOIT** être officiellement développée. Elle **DOIT** être examinée et mise à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés à l'architecture de la sécurité de l'information soient reflétés dans les plans de sécurité et opérationnels connexes.
95		On **DOIT** développer un plan de sécurité qui couvre l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan de sécurité **DEVRAIT** : • Être conforme à l'architecture d'entreprise de l'organisation; • Définir la limite d'autorisation pour le système; • Décrire le contexte opérationnel du système d'information; • Fournir la catégorisation de sécurité du système d'information et de ses données; • Décrire l'environnement opérationnel pour le système d'information et les relations ou liens avec d'autres systèmes d'information; • Donner un aperçu des exigences en matière de sécurité pour le système; • Identifier les principaux risques et leurs répercussions commerciales ou opérationnelles; • Décrire les contrôles de sécurité en place ou planifiés pour répondre à ces exigences, notamment une justification pour adapter et compléter les décisions; Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés au plan de sécurité soient reflétés dans la mise en œuvre des composantes de systèmes connexes.

96		On **DOIT** développer un plan d'intervention en cas d'incident qui s'applique à l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan d'intervention en cas d'incident **DEVRAIT** : • Fournir une feuille de route pour la mise en œuvre de cette capacité d'intervention en cas d'incident; • Répondre aux exigences propres à l'organisation qui ont trait à sa mission, sa taille, sa structure et ses fonctions; • Définir les incidents à signaler; • Fournir des paramètres pour mesurer la capacité d'intervention en cas d'incident au sein de l'organisation; • Définir les ressources et le soutien de la gestion nécessaires pour maintenir efficacement la capacité d'intervention en cas d'incident; Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés au plan d'intervention en cas d'incident soient reflétés dans la mise en œuvre des composantes de systèmes connexes.
97		On **DOIT** développer un plan de secours (parfois appelé plan de reprise après catastrophe) qui couvre l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan de secours **DEVRAIT** : • Identifier les missions et fonctions commerciales essentielles et les exigences connexes en matière de secours; • Fournir des objectifs en termes de reprise, des priorités de rétablissement et des paramètres; • Déterminer les rôles, responsabilités et intervenants, avec leurs coordonnées, pour les urgences; • S'occuper de maintenir les missions et fonctions commerciales essentielles même si le système informatique est perturbé, compromis ou en panne; • S'occuper de l'éventuel rétablissement complet du système informatique sans détériorer les mesures de sécurité initialement prévues et mises en place; et • Inclure des descriptions d'autres ressources, notamment l'emplacement physique, les services de télécommunications, l'entreposage et les ressources informatiques. Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés au plan de secours soient reflétés dans la mise en œuvre des composantes de systèmes connexes.

98		On **DOIT** développer un plan de gestion de la configuration qui couvre l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan de gestion de la configuration **DEVRAIT** : • Déterminer les rôles, responsabilités, et processus et procédures de gestion de la configuration; • Établir un processus pour identifier les éléments de configuration tout au long du cycle de vie du développement des systèmes et pour gérer la configuration des éléments de configuration; • Définir les éléments de configuration, et les bases connexes, à gérer dans le cadre du plan. Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés au plan de gestion de la configuration soient reflétés dans la gestion des composantes de systèmes connexes.
99		Il **DEVRAIT** y avoir un plan et un programme de surveillance permanente qui incluent : • La détermination des paramètres à surveiller; • L'établissement de la fréquence de la surveillance; • La surveillance de l'état de la sécurité; • Les mesures d'intervention pour faire suite aux résultats de l'analyse de l'information reliée à la sécurité; et • Le signalement de l'état de la sécurité de l'organisation et du système d'information.

100		On **DOIT** développer un plan d'évaluation de la sécurité et de la protection de la vie privée qui couvre l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan d'évaluation de la sécurité **DEVRAIT** : • Déterminer les contrôles de sécurité et les améliorations des contrôles en cours d'évaluation; • Définir les procédures d'évaluation à utiliser pour déterminer l'efficacité des contrôles de sécurité; • Identifier l'environnement d'évaluation, l'équipe d'évaluation, et les rôles et responsabilités liés à l'évaluation; • Définir les paramètres à évaluer; • Définir un rapport d'évaluation de la sécurité qui documente les résultats de l'évaluation; et • Identifier les mesures de protection de la vie privée qui sont en place et leurs contrôles (se reporter à la section Mesures de protection du profil de conformité « Respect de la vie privée » du CCP pour obtenir plus détails sur la question). Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés au plan d'évaluation de la sécurité et de la protection de la vie privée soient reflétés dans la configuration des composantes de systèmes connexes.
101		Il **DOIT** y avoir une norme opérationnelle obligeant les développeurs à suivre un processus de développement documenté qui consiste explicitement à répondre aux exigences en matière de sécurité, à déterminer les normes technologiques et les ensembles d'outils à utiliser, et à définir les configurations d'outils de travail spécifiques à employer.
102		Il **DEVRAIT** exister une élaboration officielle d'une architecture de capacités commerciales-services qui est examinée et mise à jour.
103		Il **DEVRAIT** y avoir des politiques documentées établissant les restrictions d'utilisation, les exigences en matière de configuration et de connexion, et les consignes de mise en œuvre pour : • l'accès sans fil; • l'accès mobile; et • l'accès à distance.

104		On **DOIT** développer un plan d'audit de la sécurité et des activités commerciales qui couvre l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan d'audit **DEVRAIT** : • Identifier les événements pour lesquels des renseignements sur les audits doivent être recueillis; • Déterminer que les composantes de systèmes sont capables de saisir des évévenements vérifiables; et • Expliquer pourquoi les événements vérifiables sont jugés adéquats pour soutenir des enquêtes sur les incidents de sécurité menées après coup. Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles. Enfin, il **DOIT** y avoir un processus pour s'assurer que les changements apportés au plan d'audit correspondent à l'évolution des composantes des systèmes connexes.
105		On **DOIT** développer un plan d'audit de l'évaluation des risques qui couvre l'ensemble des technologies, composantes de systèmes, intégrations et échanges d'information utilisés pour fournir des services à l'écosystème de l'identité numérique. Le plan d'évaluation des risques **DEVRAIT** : • Gouverner l'évaluation des risques, notamment la probabilité et l'ampleur des torts résultant de l'accès, l'utilisation, la divulgation, la perturbation, la modification ou la destruction non autorisées du système d'information et des renseignements qu'il traite, entrepose ou transmet; • Déterminer la documentation des résultats de l'évaluation des risques; • Définir les rôles et responsabilités pour la diffusion des résultats de l'évaluation des risques. Ce plan **DOIT** être examiné et mis à jour en permanence pour refléter l'évolution des exigences commerciales ou opérationnelles.
106	**TECH**	**Exigences technologiques des organisations qui fournissent des services à l'écosystème de l'identité numérique**
107		L'organisation **DOIT** déployer et gérer les outils, les logiciels, les dispositifs et protocoles de sécurité, l'architecture de réseau et les protocoles de communication spécifiques exigés par l'écosystème de l'identité numérique dans lequel elle souhaite fonctionner.

108		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-feu, portes d'accès, systèmes de détection d'intrusion au niveau de l'hôte) pour détecter et supprimer les codes malveillants. Ces outils **DEVRAIENT** mettre automatiquement à jour les mécanismes de protection contre les codes malveillants.
109		Le système d'information **DOIT** assurer la confidentialité et l'intégrité des renseignements sur l'identité numérique qui sont stationnaires et en transit. Veuillez vous référer au profil de conformité « Respect de la vie privée » du CCP pour obtenir d'autres exigences connexes dans ce domaine.
110		Le système d'information **DOIT** assurer l'authenticité des séances de communication (p. ex. identifiants de sessions aléatoires uniques, invalidation des identifiants à la fermeture des sessions, application appropriée de certificats de cryptage approuvés basés sur la politique d'entreprise).
111		Le système d'information **DOIT** invalider les identifiants de sessions une fois que les utilisateurs se déconnectent ou lors de toute autre interruption de session. Veuillez vous référer également à la section Fin de session du profil de conformité « Authentification » du CCP pour obtenir plus de contexte.
112		L'organisation **DOIT** émettre des certificats de clés publiques conformément à la politique sur les certificats définie par l'organisation ou obtenir des certificats de clés publiques auprès d'une autorité pilier en matière de certificats qui est bien connue et jouit de la confiance du public.
113		Le système d'information **DOIT** mettre fin à la connexion réseau associée à une session utilisateur ou à une session de communication de réseau à réseau, à la fin de la session ou après une période d'inactivité prédéfinie.
114		L'organisation **DEVRAIT** employer des outils de vérification de l'intégrité pour détecter les changements non autorisés apportés aux logiciels, aux micrologiciels et à l'information.
115		Des outils **DOIVENT** être en place pour surveiller les communications entrantes et sortantes pour des activités ou conditions inhabituelles ou non autorisées.
116		On **DOIT** utiliser des outils, appareils et techniques de surveillance et d'alerte pour surveiller le système d'information afin de détecter : • Les attaques et indications d'attaques potentielles; et • Les connexions locales, réseau et à distance non autorisées. Voir aussi la section Surveillance du profil de conformité « Authentification » du CCP pour plus de renseignements.

117		Les systèmes d'information qui fournissent collectivement un service de résolution des noms et adresses pour une organisation **DOIVENT** être insensibles aux défaillances et instaurer une séparation des rôles internes et externes.
118		L'organisation **DOIT** établir et gérer des clés cryptographiques répondant aux normes de cryptage requises qui sont utilisées dans le système d'information.
119		Des outils, appareils et techniques de protection des frontières **DOIVENT** être utilisés pour : • Surveiller et contrôler les communications à la frontière externe du système et aux principales frontières internes de celui-ci; • Mettre en place des sous-réseaux pour les composantes système d'accès public qui sont logiquement séparées des réseaux organisationnels internes; et • Se relier à des réseaux ou systèmes d'information externes uniquement par des interfaces gérées consistant en des appareils de protection des frontières arrangés conformément à une architecture de sécurité organisationnelle.
120		L'organisation **DOIT** employer des outils et techniques pour se protéger contre les effets des attaques par déni de service ou les limiter.
121		Le système d'information **DOIT** identifier et authentifier de manière unique les utilisateurs non organisationnels (ou les processus agissant pour le compte d'utilisateurs non organisationnels).
122		L'organisation **DOIT** s'assurer que des authentifiants statiques non cryptés ne sont pas intégrés dans des applications ou des scripts d'accès ou entreposés sur des touches de fonction. Veuillez vous référer aux sections Attribution et authentification des justificatifs du profil de conformité « Authentification » du CCP.
123		L'organisation **DEVRAIT** utiliser des outils automatisés pour déterminer si les authentifiants de mots de passe sont suffisamment robustes pour remplir les exigences de la politique de sécurité de l'organisation. Veuillez vous référer aux sections Attribution et authentification des justificatifs du profil de conformité « Authentification » du CCP.
124		L'organisation **DOIT** mettre en place une authentification multifacteurs pour l'accès à distance à des comptes privilégiés et non privilégiés de sorte qu'un des facteurs est fourni par un appareil distinct du système qui obtient l'accès.
125		L'organisation **DOIT** mettre en place des outils pour se défendre contre des attaques consistant à rejouer l'authentification et à deviner des secrets pour obtenir accès au réseau. Voir aussi la section Atténuation des menaces du profil de conformité « Authentification » du CCP.
126		L'organisation **DOIT** analyser les changements apportés au système d'information afin de déterminer les impacts potentiels pour la sécurité avant leur mise en œuvre.

127			L'organisation **DOIT** avoir une technologie automatisée de détection et d'alerte des intrusions en place pour toutes les composantes technologiques utilisées pour la prestation ou la consommation de l'identité numérique.
128			L'organisation **DOIT** évaluer d'une manière proactive et maintenir le caractère adéquat des systèmes et services, notamment les niveaux des ressources du système et l'état à jour des niveaux de correctifs du matériel et du système d'exploitation.
129			Le système d'information **DEVRAIT** avoir des mécanismes de sécurité pour protéger sa mémoire contre l'exécution non autorisée des codes.
130			Le système d'information **DOIT** déployer des outils cryptographiques et d'autres méthodes et technologies de protection des données de façon à maintenir la protection de la vie privée pendant les échanges d'information. Veuillez vous référer au profil de conformité « Respect de la vie privée » du CCP pour plus de renseignements. Les outils cryptographiques **DEVRAIENT** répondre à une norme de validation reconnue dans l'industrie (p. ex. FIPS 140-2 ou l'équivalent).
131	**OPS**		**Exigences opérationnelles pour les organisations qui desservent l'écosystème de l'identité numérique**
132			L'organisation **DOIT** gérer les composantes de systèmes en utilisant son cycle défini de développement de systèmes qui intègre les préoccupations liées à la sécurité.
133			L'organisation **DOIT** avoir des calendriers officiels de rétention et disposition de l'information assujettis à une surveillance et un audit afin d'assurer la conformité.
134			Des systèmes et processus officiels de gouvernance technologique de l'entreprise (p. ex. gestion des tâches et des flux de travaux de gouvernance, gestion des changements) **DEVRAIENT** être en place. Ils **DEVRAIENT** inclure des contrôles continus de la surveillance et de l'audit des activités afin d'assurer la conformité.
135			L'organisation **DOIT** être capable de restaurer les composantes des systèmes d'information à l'intérieur des périodes de restauration définies dans le plan d'urgence. Cette capacité **DOIT** englober le rétablissement et la reconstitution du système d'information à un état connu après une interruption, une compromission ou une panne.
136			Le plan d'urgence **DOIT** faire régulièrement l'objet de tests, d'une évaluation et d'une mise à jour complets (p. ex. tous les deux ans, idéalement tous les ans).

137		Des procédures complètes de sauvegarde automatisée **DOIVENT** être en place. Cela inclut la sauvegarde : • Des renseignements au niveau des utilisateurs • Des renseignements au niveau des systèmes • De la documentation sur le système et la sécurité
138		Les procédures de sauvegarde automatisée pour l'ensemble du système en fonctionnement **DOIVENT** s'aligner sur le plan d'urgence.
139		Les sauvegardes des logiciels et des données opérationnelles essentiels **DEVRAIENT** être entreposées dans un endroit qui est physiquement séparé du système d'exploitation. Des processus et procédures **DOIVENT** être en place pour protéger la confidentialité, l'intégrité et la disponibilité des renseignements sauvegardés dans les lieux d'entreposage conformément à la politique de gouvernance et de gestion du risque.
140		Il **DOIT** y avoir un programme d'essai continu de la vulnérabilité des composantes du système et des logiciels utilisés pour fournir des services à l'écosystème de l'identité numérique. Des techniques de balayage des vulnérabilités et des outils qui mettent aussitôt à jour les vulnérabilités à balayer **DEVRAIENT** être utilisés et exploités d'une manière automatisée.
141		L'organisation **DOIT** mener régulièrement des essais de pénétration sur toutes les composantes utilisées pour fournir des services à l'écosystème de l'identité numérique.
142		Les méthodes d'accès à distance **DOIVENT** être contrôlées et surveillées.
143		L'accès à distance **DOIT** se faire par des points de contrôle d'accès réseau gérés.
144		IL **DEVRAIT** y avoir des systèmes automatisés (p. ex. provisionnement, attribution et gestion des droits) pour soutenir la gestion des comptes du système d'information.
145		Des processus **DOIVENT** être en place pour désactiver automatiquement des comptes inactifs après une période spécifique d'inactivité basée sur la politique de contrôle du système d'information.
146		Un dossier système **DOIT** être automatiquement créé pour les actions consistant à créer, modifier, activer, désactiver et supprimer des comptes.
147		Des contrôles **DOIVENT** être en place pour obliger les comptes système à se déconnecter après une période d'inactivité spécifique.
148		Des comptes d'utilisateurs privilégiés **DOIVENT** être établis et administrés selon un mécanisme d'accès basé sur les rôles.
149		Une politique documentée **DOIT** être en place et la conformité à celle-ci doit être surveillée pour l'utilisation des groupes ou comptes partagés.

150		Des processus automatisés **DOIVENT** être en place pour résilier les justificatifs des comptes partagés ou de groupes lorsque des membres quittent le groupe.
151		Des processus automatisés **DOIVENT** être en place pour faire respecter une limite de 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 du mot de passe).
152		Le système **DOIT** empêcher l'accès après une période d'inactivité définie et exiger que l'utilisateur rétablisse l'accès à l'aide de procédures d'identification et d'authentification établies. Veuillez vous référer également aux critères d'annulation de session définis dans le profil « Authentification » du CCP pour plus de renseignements.
153		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 établie de l'organisation.
154		Les organisations **DOIVENT** affecter des gestionnaires aux comptes de systèmes d'information et établir des conditions officielles pour l'appartenance à des groupes et des rôles qui accorde des autorisations d'accès. Il **DOIT** y avoir en place des processus documentés exigeant des approbations pour la création de comptes et des procédures automatisées pour surveiller l'utilisation des comptes du système d'information.
155		L'organisation **DOIT** utiliser le principe du droit d'accès minimal, qui limite l'accès aux utilisateurs (ou processus agissant pour le compte des utilisateurs) qui sont nécessaires pour accomplir des tâches assignées conformément aux missions organisationnelles et fonctions commerciales. Cela inclut : • La configuration de logiciels pour refléter le mode le plus restrictif conformément aux besoins opérationnels; • L'accès restreint aux données d'identité numérique en utilisant des configurations qui fournissent un accès explicite uniquement aux données requises par la personne ou le système qui en a besoin; et • Les configurations des appareils du réseau et de communications limitant l'accès aux composantes de systèmes ou aux services nécessaires.
156		L'organisation **DOIT** maintenir l'information disponible au cas où des utilisateurs perdraient les clés cryptographiques.
157		Le système d'information **DOIT** mettre en place des mécanismes cryptographiques pour empêcher la divulgation non autorisée de l'information et détecter les changements apportés aux renseignements sur l'identité numérique pendant la transmission.

158			L'organisation **DOIT** autoriser les connexions externes entre les systèmes d'information basés sur des ententes de sécurité officielles telles que définies dans sa politique sur la sécurité. Pour chaque connexion individuelle, les caractéristiques de l'interface, les exigences en matière de sécurité et la nature de l'information communiquée **DOIVENT** être documentées. On **DEVRAIT** tenir un historique des changements apportés à l'entente ou aux caractéristiques de l'interface.
159	e		Les connexions internes entre les composantes des systèmes d'information **DOIVENT** être documentées, en saisissant les caractéristiques des interfaces, les exigences en matière de sécurité et la nature des renseignements communiqués. On **DEVRAIT** tenir un historique des changements apportés aux caractéristiques des interfaces.
160			Des processus **DOIVENT** être en place pour assurer des autorisations approuvées pour contrôler le flux de l'information à l'intérieur du système et entre des systèmes interconnectés selon la politique de sécurité de l'organisation.
161			L'organisation **DEVRAIT** utiliser des mécanismes automatisés pour que des renseignements sur les alertes et avis de sécurité soient disponibles dans toute l'organisation.
162			L'organisation **DEVRAIT** recevoir continuellement d'une autorité reconnue des alertes, avis et directives à propos de la sécurité du système d'information, et générer des alertes, avis et directives de sécurité internes si elle le juge nécessaire.
163			L'organisation **DOIT :** • Identifier, signaler et corriger les lacunes du système d'information; • Tester les mises à jour de logiciels et micrologiciels reliées à la correction des lacunes pour en vérifier l'efficacité et les éventuels effets secondaires avant leur installation; • Installer les mises à jour des logiciels et micrologiciels ayant trait à la sécurité dans un certain délai, après leur diffusion, qui est déterminé par la politique de sécurité de l'organisation; et • Incorporer les corrections des lacunes dans un processus de gestion de la configuration organisationnelle.
164			Des processus officiels de gestion des changements technologiques **DOIVENT** être en place pour évaluer et gérer les risques associés à l'évolution de la technologie.
165			L'organisation **DOIT** définir, documenter, approuver, et faire respecter les restrictions d'accès physique et logique associées aux changements apportés au système d'information.

166		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 contrôlés par la configuration qu'on se propose d'apporter au système d'information et approuver ou désapprouver ces changements en tenant explicitement compte des analyses d'impact sur la sécurité; • Documenter les décisions d'apporter des changements de configuration qui sont associées au système d'information; • Mettre en place les changements approuvés au système d'information; • Garder les dossiers des changements apportés au système d'information pendant la période spécifiée dans la politique de contrôle des changements; et • Coordonner et superviser les activités de contrôle des changements de configuration par le biais d'un organe de gouvernance du contrôle des changements officiellement constitué.
167		Des installations de surveillance des activités et de trace d'audits **DOIVENT** être en place pour fournir un registre de toutes les transactions reliées à l'identité numérique au sein de l'écosystème de l'identité numérique. En outre, ces traces d'audits doivent être protégées contre les modifications et les politiques qui limitent l'accès doivent être observées.
168		Les renseignements et les outils des audits **DOIVENT** être protégés contre les accès, les modifications et les suppressions non autorisés.
169		Le système d'information **DOIT** avoir des mécanismes en place qui le protègent contre toute personne (ou tout processus agissant pour le compte d'une personne) niant faussement avoir effectué des actions pour être couverte par la non-répudiation.
170		Les dossiers d'audit **DOIVENT** être conservés d'une manière sécuritaire pendant le temps stipulé par la politique de rétention des renseignements de l'organisation afin de fournir un soutien lors des enquêtes menées à la suite d'incidents de sécurité et de remplir les exigences réglementaires et organisationnelles en matière de rétention de l'information.
171		Des dossiers d'audit **DOIVENT** être régénérés pour les transactions liées à l'identité numérique qui contiennent de l'information établissant le type d'événement qui s'est produit, à quel moment et à quel endroit, la source de l'événement, le résultat de l'événement et l'identité des personnes ou sujets associés à l'événement.
172		Des dossiers d'audit **DOIVENT** être générés pour éxécuter des fonctions privilégiées du système.

173			Des processus **DOIVENT** être en place pour empêcher des utilisateurs non privilégiés d'exécuter des fonctions privilégiées consistant notamment à désactiver, contourner ou modifier des mesures ou des contre-mesures de sécurité en place.
174			L'utilisation des comptes du système d'information **DOIT** être surveillée pour voir s'il y a une utilisation et des habitudes d'utilisation atypiques signalées et/ou des comptes désactivés qui dépendent des risques associés à l'utilisation atypique observée.
175			Des processus **DOIVENT** être en place pour faire appliquer les autorisations approuvées pour l'accès logique aux ressources d'information et du système conformément aux politiques de contrôle d'accès applicables.
176			L'organisation **DEVRAIT** avoir des intendants de données et d'information clairement identifiés.
177			L'organisation **DEVRAIT** avoir une norme API documentée.