Ébauche de recommandations pour l'aperçu de la composante « 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.

En examinant cette ébauche, veuillez tenir compte de ce qui suit et noter que les réponses à ces questions sont non contraignantes et vise à améliorer le Cadre de confiance pancanadien. Comme toujours, les commentaires sur n'importe quel aspect de l'ébauche sont les bienvenus. Les éléments ci-dessous visent simplement à mettre en évidence certains aspects pouvant être plus préoccupants.

1. Plusieurs commentaires suggèrent d'ajouter des détails prescriptifs à ce profil de conformité. Certains ajustements ont été apportés, mais des avis supplémentaires sont sollicités pour identifier les secteurs où d'autres détails devraient être inclus. Lorsque des méthodes ou normes spécifiques sont appelées à être développées, veuillez suggérer des méthodes, outils ou éléments de plans ou de politiques qui devraient être ajoutés selon vous.
2. Les critères de conformité sont organisés en trois catégories. Ces catégories sont-elles appropriées et compréhensibles? Dans la négative, veuillez suggérer un autre plan de catégorisation.
3. Nous avons pris soin de trouver un juste milieu entre des critères génériques qui sont définis d'une manière générale et trop prescriptifs. Les critères sont-ils suffisamment prescriptifs pour être utiles et assez génériques pour s'appliquer à la plupart des exemples d'écosystèmes de l'identité numérique?

4. Veuillez noter qu'il y a plusieurs cas de références croisées à des renseignements connexes dans d'autres profils. Y a-t-il d'autres situations où ce serait approprié?
5. Y a-t-il des exigences importantes qui manquent dans cette ébauche? Dans l'affirmative, veuillez indiquer celles qui devraient être incluses selon vous.
6. Nous avons pris soin de ne pas identifier une technologie ou un protocole technologique spécifique, car nous estimons qu'il ne s'agissait pas d'une exigence dans chaque cas. Est-ce exact, ou y a-t-il une technologie ou un protocole spécifique qui devrait être inclus en tant qu'exigence du CCP?
7. **VEUILLEZ NOTER que le 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.

Table des matières

1. Introduction à la composante « Infrastructure (technologie et opérations) » du CCP

Ce document fournit un aperçu de la composante « Infrastructure (technologie et opérations) » du Cadre de confiance pancanadien (CCP). Pour avoir une introduction au CCP, veuillez vous référer au modèle de CCP. L'aperçu du modèle de CCP fournit les buts et objectifs du CCP, un aperçu général du modèle et des renseignements contextuels.

Chaque composante du CCP comprend deux documents :

1. **Aperçu de la composante** – Il introduit le sujet de la composante et fournit des renseignements essentiels pour en comprendre les critères de conformité. Cela inclut des définitions des principaux termes, des notions et des processus de confiance qui font partie de la composante.
2. **Profil de conformité de la composante** – Il spécifie les critères de conformité utilisés pour uniformiser et évaluer l'intégrité des processus de confiance qui font partie de cette composante.

Cet aperçu fournit des renseignements qui sont reliés à la composante « Évaluation » du CCP et nécessaires pour en faire une interprétation uniforme.

1.1. Raison d'être et avantages anticipés

La composante « Infrastructure (technologie et opérations) » du CCP vise à identifier les politiques, les plans, la technologie et les opérations technologiques nécessaires pour soutenir la mise en œuvre des principes des profils du CCP dans le contexte d'un écosystème de l'identité numérique.

Un processus qui a été certifié est un processus de confiance auquel les autres participants du CCP peuvent se fier. Les critères de conformité du CCP visent à compléter les lois et règlements existants; les participants à l'écosystème d'identité numérique certifié par le CCIAN sont tenus de remplir les exigences et les règlements applicables imposés par la loi dans leurs provinces et territoires.

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

- Les artéfacts officiels des politiques et plans qui forment la base d'une installation technologique conforme et de ses opérations de soutien technologique;
- Les capacités générales en termes de technologie et d'outils technologiques nécessaires pour soutenir une infrastructure technologique fournissant des services à un écosystème de l'identité numérique;
- Les outils et caractéristiques opérationnels de soutien technologique pour soutenir une infrastructure technologique installée qui fournit des services à 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 niveau général pour illustrer la portée; les exigences détaillées sont précisées dans le profil de conformité « Infrastructure (technologie et opérations) » du CCP.

1.2.1. Inclus dans la portée

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

- La sécurité TI (d'un point de vue général);
- La supervision de la collecte, la validation, l'entreposage et l'accessibilité des données;
- L'audit et la journalisation;
- La prévention et le traitement des incidents TI qui compromettent la fiabilité de l'écosystème de l'identité numérique;
- Les politiques et les plans qui soutiennent la gestion fiable de la technologie et des opérations technologiques.

1.2.2. Exclus de la portée

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

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

1.3. Relations avec le CCP

Le CCP est un ensemble de composantes modulaires ou fonctionnelles qui peuvent être évaluées et certifiées indépendamment pour être prises en considération comme composantes de confiance. Le CCP, qui se fonde sur une approche pancanadienne, permet aux secteurs public et privé de collaborer pour protéger les identités numériques en uniformisant les processus et les pratiques à l'échelle de l'écosystème numérique canadien.

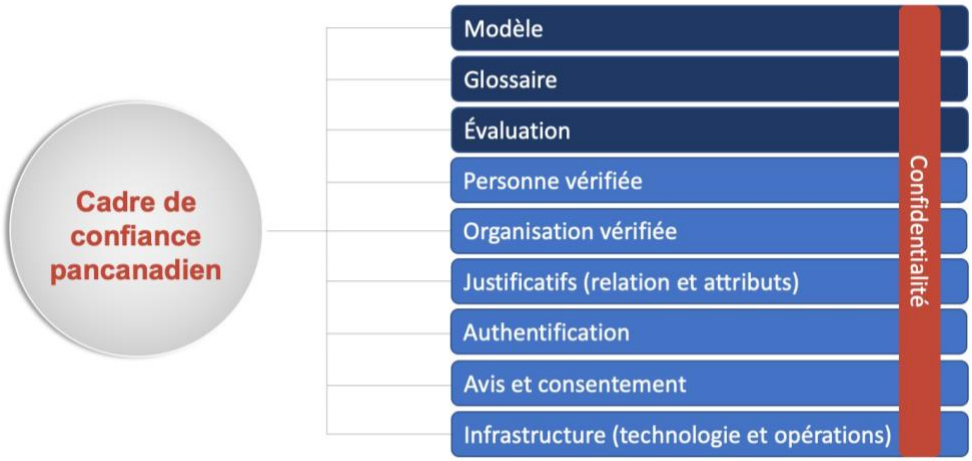

Figure 1 - Composantes de l'ébauche du Cadre de confiance pancanadien

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

2. Conventions régissant l'infrastructure (technologie et opérations)

Cette section décrit et définit les principaux termes et notions utilisés 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 invités à examiner les conventions de chacune des composantes du CCP qu'ils lisent.
- Termes définis - Les principaux termes et concepts décrits et définis dans cette section et le glossaire du CCP sont écrits avec une majuscule initiale dans ce document.
- Liens hypertextes – Des liens hypertextes peuvent être intégrés dans les versions électroniques de ce document pour fournir des références au lecteur. Tous les liens étaient accessibles au moment de la rédaction.

1.4. Terms et définitions

Pour les besoins de cette composante du CCP, les termes et définitions du glossaire du CCP et ceux qui figurent 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 – Système interconnecté pour l'échange et la vérification de renseignements sur l'identité numérique faisant intervenir des organisations des secteurs public et privé qui se conforment à un cadre de confiance commun pour la gestion et l'utilisation des identités numériques, et les sujets de ces identités numériques.
    - Exemples : écosystème de l'identité numérique canadien endossé par le CCIAN; écosystème de l'identité numérique d'un autre pays; écosystème provincial consistant en un fournisseur d'identité et plusieurs parties utilisatrices qui fournissent un ensemble de services pour les citoyens suivant un cadre d'identité provincial commun.

1.5. Acronymes

Les acronymes suivants sont utilisés tout au long de la présente composante du CCP :

- CCO – Cadre de confiance pancanadien
- CCIAN – Conseil canadien de l'identification et de l'authentification numériques

3. Couverture des critères de conformité

Les critères de conformité sont élaborés en détail dans le profil de conformité « Infrastructure » du CCP. Les exigences ont été conçues pour refléter les capacités et les caractéristiques qu'on retrouve dans les opérations technologiques et les normes de gouvernance (p. ex. ITIL, COBIT) sans être prescriptifs au point d'exiger une norme spécifique.

De même, les organes de normalisation du secteur public et leurs consignes de mise en œuvre ont été mis à contribution pour aider à définir certaines des exigences détaillées des critères de conformité. Il s'agit notamment du National Institute of Standards and Technology (NIST) et du Federal Risk and Authorization Management Program (FEDRAMP) aux États-Unis, de l'Agence européenne de cybersécurité (ENISA) en Europe et de diverses directives du gouvernement fédéral au Canada. L'approche a consisté à s'inspirer de certaines consignes 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 n'importe quel domaine du secteur public ou privé.

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

Les critères sont organisés selon trois grandes catégories :

- Politiques et planification – cette catégorie définit les principaux artéfacts officiels qui élaborent l'approche constante de l'organisation pour ce qui est de l'instanciation et de la gestion des composantes technologie et systèmes qui remplissent le rôle que cette organisation joue dans l'écosystème de l'identité numérique.
- Technologie – cette catégorie détermine les caractéristiques et les capacités que doivent avoir les composantes technologiques.
- Opérations – cette catégorie détermine les caractéristiques et capacités que doivent avoir le cadre opérationnel et l'ensemble d'outils utilisés pour jouer un rôle défini au sein de l'écosystème de l'identité numérique.

2.1. Politique et plans

La composante technologique d'une architecture d'entreprise se fonde sur un ensemble complet de politiques et de plans organisationnels clairement axés sur les objectifs commerciaux identifiés dans les composantes commerciales de l'architecture d'entreprise. Ce profil identifie les exigences en ce qui concerne les artéfacts officiels et leur gestion continue dans les domaines suivants :

- Évaluation des risques;
- Audit et responsabilité;
- Évaluation de la sécurité;
- Planification des catastrophes ou urgences;
- Identification et autorisation;
- Protection des systèmes et des communications;
- Intervention en cas d'incident;
- Intégrité des systèmes et de l'information;
- Maintenance des systèmes;
- Contrôle de l'accès technique; et
- Accès physique aux actifs technologiques

Précisons que ces critères représentent les capacités à prendre en compte et ne devraient pas être interprétés comme une politique ou des artéfacts d'un plan en particulier. Bon nombre de ces capacités sont généralement combinées et couvertes dans un seul artéfact. D'une façon générale, il faut surtout en retenir le besoin d'avoir une planification ordonnée qui commence par la détermination des objectifs dans les énoncés de politiques, avec des plans officiels qui régissent la mise en œuvre et le fonctionnement de la technologie.

2.2. Critères technologiques

Ces critères consistent surtout à identifier les outils génériques et les capacités technologiques nécessaires pour soutenir une infrastructure opérationnelle qui fournit des services conformes au CCP. Des produits ou protocoles technologiques spécifiques ne sont pas identifiés, car ils tendent à varier selon le processus de confiance spécifique qui est suivi dans 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 seront imposées par l'écosystème de l'identité numérique dans lequel elles souhaitent fonctionner.

De plus, les capacités 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, lorsque c'est approprié.

2.3. Critères des opérations technologiques

La troisième catégorie des 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 identifiés plus tôt, représentent le soutien technologique continu et les caractéristiques opérationnelles nécessaires pour fournir les capacités d'entreprise identifiées dans les politiques et les plans associés à une architecture d'entreprise complète.

4. Références

Ce profil s'est inspiré des normes ou des organes de normalisation ci-dessous. Chacune des organisations mentionnées inclut un référentiel contenant de multiples documents ayant trait à l'établissement et au fonctionnement d'une infrastructure technique nécessaire pour soutenir la prestation de services, dans ce cas-ci, à un écosystème de l'identité numérique.

Remarque : Le cas échéant, seul le numéro de version spécifié dans ce document s'applique à la présente composante du CCP.

Les profils de conformité de la composante du CCP (les versions publiques seront publiées dans leur état final à www.diacc.ca) ont été mentionnés dans leur ébauche :

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

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

Gouvernement du Canada. *Profil du secteur public du Cadre de confiance pancanadien du gouvernement du Canada V1.1*. https://github.com/canada-ca/PCTF-CCP/tree/master/Version1_1

Département du Commerce des États-Unis. 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

Département du Commerce des États-Unis. National Institute of Standards and Technology. *Assessing Security and Privacy Controls (NIST Special Publication 800-53)*. 2014. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

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/fr/standard/50341.html

Gouvernement fédéral des États-Unis, programme fédéral de gestion des risques et des autorisations (FedRAMP). Voir le lien menant au référentiel. www.fedramp.gov

Agence européenne pour la cybersécurité (ENISA). Voir le lien menant au référentiel. https://www.enisa.europa.eu/