Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

# Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie

## Proposition de profil d'activités et de contrôles organisationnels de sécurité et de protection de la vie privée – Incidence moyenne


**Praticien·nes**





Canada

# Avant-propos

Le document *Proposition de profil d'activités et de contrôles organisationnels de sécurité et de protection de la vie privée – Incidence moyenne* (ITSP.10.033-01) est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal, Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

La présente publication remplace l'Annexe 4A – Profil 1 (PROTÉGÉ B/Intégrité moyenne /Disponibilité moyenne).

Pour obtenir de plus amples renseignements ou suggérer des modifications, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca
(613) 949-7048 ou 1-833-CYBER-88.

# Date d'entrée en vigueur

Le présent document entre en vigueur le 1 avril 2026.

# Historique des révisions

| Révision | Modifications | Date |
|---|---|---|
| 1. | Première version. | 1 avril 2026 |
| | | |
| | | |
| | | |

D97-3/10-033-01-2026F-PDF
ISBN 978-0-660-78905-7

# Vue d'ensemble

Le présent document fait partie d'une série de lignes directrices publiées par le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) dans le cadre de la publication du document *Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie*.

Il propose une sélection d'activités, de contrôles et d'améliorations de sécurité collectivement désignés sous le nom « profil d'activités et de contrôles de sécurité et de protection de la vie privée ». Les autorités responsables de la sécurité et de la protection de la vie privée au sein de l'organisation peuvent utiliser ce profil comme référence pour créer des profils propres à l'organisation qui permettent d'assurer la confidentialité, l'intégrité et la disponibilité des biens organisationnels de valeur moyenne contre les auteurs de menace non étatiques. Ce profil a été élaboré au moyen du *Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée* (ITSP.10.033).

Les activités et les contrôles suggérés dans ce profil sont un point de départ et doivent être adaptés au contexte opérationnel, technique, de menace et de risque des activités opérationnelles de chaque organisation et des systèmes d'information qu'ils soutiennent. Les activités et les contrôles de sécurité et de protection de la vie privée sont basés sur les pratiques exemplaires de l'industrie et du gouvernement en matière de sécurité et de protection de la vie privée. Ils tiennent également compte de certaines hypothèses de menace dérivées de l'analyse que le Centre pour la cybersécurité a réalisée de l'environnement de menace avec lequel doivent composer les systèmes d'information dans le contexte opérationnel décrit dans le présent document. Ce profil n'aborde pas les capacités des auteurs de menace dotés de moyens sophistiqués, mais les hypothèses sont décrites de façon plus détaillée à la section 2.3, Contexte de menace.

Ce profil est un outil qui contribue aux efforts déployés par les praticiennes et praticiens de la sécurité et de la protection de la vie privée pour assurer la protection des systèmes d'information en conformité avec les lois du gouvernement du Canada (GC), ainsi que les politiques, les directives et les normes du Secrétariat du Conseil du Trésor du Canada (SCT).

Au moment d'élaborer les profils d'activités et de contrôle de sécurité et de protection de la vie privée de leur organisation, les autorités responsables de la sécurité et de la protection de la vie privée sont tenues de se conformer à toutes les exigences en matière de sécurité et de protection de la vie privée mentionnées dans les lois du GC et les instruments de politique du SCT qui s'appliquent à leurs activités opérationnelles, ainsi qu'à toute autre obligation contractuelle.

# Table des matières



# Liste des tableaux

# 1 Introduction

Un **contrôle de sécurité**, que l'on appelle aussi une protection, est un élément juridique, administratif, opérationnel ou technique d'un système. Il protège la confidentialité, l'intégrité ou la disponibilité d'une activité ou d'un bien opérationnel et des renseignements dont il dépend pour satisfaire aux exigences en matière de sécurité et pour atténuer les risques liés à la cybersécurité. Un **contrôle de protection de la vie privée** est un élément juridique, administratif, opérationnel ou technique d'un système déployé au niveau de l'organisation ou du système afin d'atténuer les risques d'atteinte à la vie privée et d'assurer le respect des exigences applicables en matière de protection de la vie privée.

Une **activité d'assurance**[1] est un groupe de tâches qui assure qu'un contrôle de sécurité ou de protection de la vie privée est adéquatement conçu et mis en œuvre, et qu'il fonctionne comme prévu. Les activités d'assurance comprennent des tâches dont le but est de confirmer que tous les contrôles de sécurité et de protection de la vie privée dans la conception, la mise en œuvre et l'exploitation d'un système sont en mesure de répondre aux besoins opérationnels en matière de sécurité.

Les activités et contrôles de sécurité et de protection de la vie privée sont sélectionnés pour répondre aux exigences de sécurité et de protection de la vie privée imposées à un système ou à une organisation. Les exigences de sécurité et de protection de la vie privée sont issues de lois applicables, de décrets, de directives, de règlements, de politiques, de normes et de besoins opérationnels pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée, stockée ou transmise et pour gérer les risques liés à la vie privée.

## 1.1 Objet

La présente fait partie d'une série de documents publiés par le Centre pour la cybersécurité, conformément à la publication *Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie* du Centre pour la cybersécurité.

Elle propose une sélection d'activités, de contrôles et d'améliorations de sécurité collectivement désignés sous le nom « profil d'activités et de contrôles de sécurité et de protection de la vie privée ». Les autorités responsables de la sécurité et de la protection de la vie privée au sein de l'organisation peuvent utiliser ce profil comme référence pour créer des profils propres à l'organisation qui permettent d'assurer la confidentialité, l'intégrité et la disponibilité des biens organisationnels de valeur moyenne contre les auteurs de menace non étatiques. Ce profil a été élaboré au moyen du *Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée* (ITSP.10.033).

Les profils organisationnels permettent de s'assurer que les fonctions de sécurité et de protection de la vie privée des programmes de sécurité et de protection de la vie privée soient en mesure de :

- réaliser les activités appropriées de gestion des risques liés à la cybersécurité et à la vie privée;
- fournir de l'orientation adéquate pour les projets.

Il importe de souligner qu'un profil n'est qu'une base de référence. Il doit être adapté aux besoins opérationnels de l'organisation en matière de sécurité et de protection de la vie privée selon les objectifs de confidentialité, d'intégrité et de disponibilité de cette dernière.

[1] Dans le présent document, une activité se veut être une activité d'assurance.

## 1.2 Portée et applicabilité

Le profil à confidentialité, intégrité et disponibilité moyennes (incidence moyenne) est destiné essentiellement aux ministères[2] et organismes du GC. Les organisations de l'industrie ou du milieu universitaire qui veulent offrir une protection à un niveau de confidentialité, d'intégrité et de disponibilité moyen peuvent utiliser le profil moyen et adapter les activités et les contrôles selon leur propre contexte.

Les activités et les contrôles de sécurité et de protection de la vie privée suggérés dans ce profil sont un point de départ et doivent être adaptés au contexte opérationnel, technique, de menace et de risque des activités opérationnelles de chaque organisation et des systèmes d'information qu'ils soutiennent (comme il est décrit à la section 2). La sélection des activités et des contrôles de sécurité et de protection de la vie privée est basée sur les pratiques exemplaires du gouvernement et de l'industrie et, sous réserve de certaines hypothèses de menace, est dérivée de l'analyse que le Centre pour la cybersécurité a réalisée de l'environnement de menace avec lequel doivent composer les systèmes d'information dans le contexte opérationnel décrit dans le présent document.

Ce profil ne fournit aucun détail sur la mise en œuvre ou l'utilisation de ces activités et contrôles de sécurité et de protection de la vie privée dans une organisation ou ses systèmes d'information. Les publications *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036) et *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037) du Centre pour la cybersécurité fournissent de l'orientation plus détaillée sur ces sujets. Elles présentent les processus recommandés pour sélectionner, adapter et mettre en œuvre adéquatement les activités d'assurance et les contrôles au niveau de l'organisation et des systèmes, respectivement.

Prière de consulter le site Web du Centre pour la cybersécurité pour de plus amples publications comportant des conseils en matière de cybersécurité.

## 1.3 Public cible

Cette publication vise à aider un public varié, notamment :

- les personnes ayant des responsabilités liées au développement des systèmes, y compris :
  - les propriétaires de la mission ou des activités;
  - les gestionnaires de programme;
  - les ingénieures et ingénieurs de système;
  - les ingénieures et ingénieurs en sécurité des systèmes;
  - les praticiennes et praticiens de la protection de la vie privée;
  - les développeuses et développeurs de matériel et de logiciels;
  - les intégratrices et intégrateurs de systèmes;
  - les responsables et les cadres chargées et chargés de l'acquisition ou de l'approvisionnement;
- les personnes ayant des responsabilités liées à la logistique et à la disposition, y compris :

[2] Dans la présente publication, le terme *ministère* est utilisé pour désigner les ministères, les organismes et les autres organisations du GC assujettis à la *Politique sur la sécurité du gouvernement*.

- les gestionnaires de programme;
- les responsables et les cadres chargées et chargés de l'acquisition;
- les intégratrices et intégrateurs de systèmes;
- les gestionnaires immobilières et immobiliers;

- les personnes ayant des responsabilités liées aux opérations et à la mise en œuvre de la sécurité et de la protection de la vie privée, y compris :
  - les propriétaires de la mission ou des activités;
  - les propriétaires de systèmes;
  - les gardiennes et gardiens de l'information;
  - les administratrices et administrateurs de système;
  - les planificatrices et planificateurs de la continuité;
  - les agentes et agents de la protection des systèmes et de la vie privée;
- les personnes ayant des responsabilités liées à l'évaluation et à la surveillance de la sécurité et de la protection de la vie privée, y compris :
  - les vérificatrices et vérificateurs;
  - les évaluatrices et évaluateurs de systèmes;
  - les évaluatrices et évaluateurs de contrôles;
  - les vérificatrices et vérificateurs indépendants et les responsables de la validation;
  - les analystes;
- les entités commerciales, y compris les partenaires de l'industrie, qui produisent des produits et des systèmes de composants, élaborent des technologies liées à la sécurité et à la protection de la vie privée, ou fournissent des services ou des capacités qui soutiennent la cybersécurité ou la protection de la vie privée.

Dans le GC, la présente publication s'adresse au public cité ci-dessus, ainsi qu'aux personnes qui soutiennent les activités de gestion des risques liés à la cybersécurité et à la vie privée, comme :

- les personnes ayant des responsabilités associées à la gestion et à la surveillance des systèmes, de la sécurité de l'information, de la protection de la vie privée ou des risques, notamment :
  - les responsables de l'autorisation;
  - les dirigeantes principales et dirigeants principaux de l'information;
  - les dirigeantes principales et dirigeants principaux de la sécurité;
  - les hauts fonctionnaires dans la gouvernance de la sécurité du ministère;
  - les agentes et agents désignés pour la cybersécurité;
  - les hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée;
- les personnes qui participent à la définition, à la conception, au développement, à l'installation et à l'exploitation des systèmes d'information et plus particulièrement :
  - les autorisatrices et autorisateurs;
  - les gestionnaires de projet;
  - les architectes en cybersécurité;
  - les ingénieures et ingénieurs de la sécurité;
  - les évaluatrices et évaluateurs de la sécurité;

- les membres des groupes responsables des opérations de cybersécurité.

## 1.4 Hiérarchie de la publication

La présente publication fait partie d'une série de lignes directrices relevant du document *Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie*. Les documents de la série se présentent comme suit :

- *Aperçu de la gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie* (ITSP.10.035)
- *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036)
- *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037)
- *Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée* (ITSP.10.033)
- *Proposition de profil d'activités et de contrôles organisationnels de sécurité et de protection de la vie privée – Incidence moyenne* (ITSP.10.033-01)
- *Évaluation des contrôles et des activités d'assurance de la sécurité et de la protection de la vie privée* (ITSP.10.033-02)

# 2 Contexte et hypothèses

Cette section vise à définir les contextes opérationnels, techniques, de menace et de risque qui conviennent à ce profil d'activités et de contrôles de sécurité et de protection de la vie privée. Lorsqu'elles choisissent ce profil comme point de départ, les autorités organisationnelles responsables de la sécurité et de la protection de la vie privée (appuyées par les praticiennes et praticiens de la sécurité et de la protection de la vie privée) doivent l'adapter de manière à créer des profils d'activités et de contrôles de sécurité et de protection de la vie privée appropriés pour les activités opérationnelles de leur organisation.

## 2.1 Contexte opérationnel

Ce profil convient aux organisations qui utilisent des systèmes d'information pour soutenir une vaste gamme d'activités opérationnelles d'un niveau de sensibilité et de criticité moyen, qui comportent de l'information d'un niveau de sensibilité moyen.

Au GC, ces activités peuvent inclure, sans s'y limiter :

- la prestation de services sociaux;
- la fiscalité;
- les fonctions du receveur général;
- les services financiers et administratifs ministériels;
- les ressources humaines;
- la rémunération et les avantages sociaux;
- l'offre de services de TI communs et partagés à une vaste clientèle.

Au sein de l'industrie, ces activités peuvent inclure, sans s'y limiter :

- les ressources humaines;
- la gestion des finances;
- l'approvisionnement;
- les processus liés à la plupart des dossiers médicaux;
- les dossiers fiscaux.

Les organisations susceptibles d'utiliser ce profil mèneront des activités opérationnelles conformément à une catégorie de sécurité maximale équivalente à un niveau de confidentialité, d'intégrité et de disponibilité moyen, tel qu'il est indiqué dans le document *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036). On peut raisonnablement s'attendre à ce que toute compromission de la confidentialité de cette information et de l'intégrité et la disponibilité des biens connexes[3] cause un préjudice de niveau moyen aux intérêts non nationaux.

[3] Un « bien » est un terme générique utilisé pour désigner les applications administratives, les représentations électroniques d'information (données), ainsi que le matériel, les logiciels et les données système qui composent un système d'information.

Le niveau de robustesse (NR) maximal prévu des contrôles et des améliorations est NR3 et le niveau d'assurance de la sécurité (NAS) maximal prévu est NAS3, tel qu'il est indiqué dans le document *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037).

Le tableau 1 ci-dessous illustre de façon plus détaillée les contextes opérationnels appropriés en fonction des objectifs de confidentialité, d'intégrité et de disponibilité. Il comprend également des exemples de conséquences d'une compromission, des processus opérationnels et de l'information connexe.

### 2.1.1 Conformité aux lois du gouvernement du Canada et aux instruments de politique du Secrétariat du Conseil du Trésor du Canada

Ce profil a été créé comme outil pour faciliter le travail des praticiennes et praticiens de la sécurité et de la protection de la vie privée chargés de la protection des systèmes, conformément aux lois du GC et aux politiques, aux directives et aux normes du SCT applicables.

Lorsqu'elles élaborent les profils d'activités et de contrôle de sécurité et de protection de la vie privée de leur organisation, les autorités responsables de la sécurité et de la protection de la vie privée sont tenues de se conformer à toutes les exigences en matière de sécurité et de protection de la vie privée mentionnées dans les lois du GC et les instruments de politique du SCT qui s'appliquent à leurs activités opérationnelles, ainsi qu'à toute autre obligation contractuelle.

**Tableau 1 : Caractérisation des contextes opérationnels applicables**

| Caractéristiques | Descriptions et exemples |
|---|---|
| Objectif de confidentialité | Les activités opérationnelles concernent le traitement, la transmission et le stockage d'information qui doit être protégée adéquatement contre toute divulgation non intentionnelle. |
| Objectif d'intégrité et de disponibilité | On évalue au niveau moyen la gravité de tout préjudice potentiel lié à une compromission de l'intégrité et de la disponibilité des biens. L'intégrité et la disponibilité de ces biens doivent donc être protégées adéquatement contre toute compromission. |
| Exemples de préjudices | Agitation ou désordre civil grave<br>Douleur physique, blessure, traumatisme, difficulté ou maladie touchant des personnes<br>Détresse psychologique ou traumatisme causés à des personnes<br>Perte financière ayant une incidence sur la qualité de vie des personnes<br>Perte financière qui réduit la compétitivité des entreprises canadiennes<br>Incapacité à mener des enquêtes criminelles ou autres obstacles à l'application efficace de la loi<br>Perturbation des activités opérationnelles gouvernementales pouvant causer des inconvénients aux Canadiennes et Canadiens |
| Exemples de processus opérationnels | Paiements de prestations dont la perturbation et le retard peuvent causer des dommages psychologiques aux Canadiennes et Canadiens<br>Processus financiers ou de production de rapports dont la perturbation peut mener à des pertes financières pour les personnes ou les entreprises canadiennes<br>Traitement d'opérations financières et de paiements importants<br>Processus liés à la plupart des dossiers médicaux |
| Exemples de ressources informationnelles | Renseignements médicaux et financiers personnels<br>Renseignements de l'impôt sur le revenu des particuliers<br>Opérations financières et paiements importants<br>Renseignements pouvant servir à des fins criminelles (par exemple, fausse identité ou usurpation d'identité) |

| | |
|---|---|
| | Renseignements relatifs à l'admissibilité d'un individu à des avantages sociaux |

## 2.2 Contexte technique

Ce profil convient aux organisations qui exploitent une vaste gamme d'environnements. De manière générale, les systèmes d'information organisationnels visés par ce profil peuvent être catégorisés selon leur objectif, comme suit :

- systèmes d'information qui offrent des services en ligne (par exemple, sur Internet) aux bénéficiaires de programmes ou de service organisationnels;
- systèmes d'information qui offrent des services de soutien opérationnels aux employées et employés des organisations et aux fournisseurs (par exemple, réseau d'entreprise);
- systèmes d'information qui offrent des services communs ou partagés à l'intérieur et à l'extérieur de l'organisation.

On suppose que ces systèmes seront connectés aux autres organisations et à Internet.

### 2.2.1 Approches architecturales à la sécurité

La sélection des activités et des contrôles de sécurité et de protection de la vie privée documentée à la section 4 a également été influencée par le choix des pratiques exemplaires en matière d'ingénierie de la sécurité qui ont été adoptées lors de la mise en œuvre de systèmes d'information fiables. Ce profil vise à répondre aux besoins en matière de sécurité de cybersécurité d'une vaste gamme d'activités opérationnelles, du travail de bureau quotidien en passant par les applications de prestation de services aux citoyennes et citoyens jusqu'au soutien de l'infrastructure des services communs.

Ce profil est destiné à une catégorisation de confidentialité, d'intégrité et de disponibilité moyennes avec l'acceptation de risques liés à des auteurs de menace de niveau supérieur (Md5, Md6 et Md7). Il suppose une connexion à des réseaux d'une sensibilité moindre (par exemple, l'Internet public) au moyen de produits de sécurité commerciaux, comme un pare-feu. Le profil suggère un ensemble équilibré d'activités et de contrôles de sécurité et de protection de la vie privée pour réduire le risque que les éléments internes compromis d'un système d'information soient utilisés pour compromettre facilement d'autres éléments. Il propose également des activités et des contrôles de sécurité et de protection de la vie privée qui permettent la détection, l'intervention et la reprise des activités à la suite d'incidents de sécurité. Plusieurs de ces activités et contrôles opérationnels sont des activités et des contrôles que tout groupe expérimenté responsable des opérations de cybersécurité devrait instaurer, non seulement aux fins de sécurité et de protection de la vie privée, mais aussi pour assurer l'efficacité et la rentabilité de la gestion quotidienne des systèmes d'information.

Bien que la sélection des activités et des contrôles de sécurité et de protection de la vie privée soit plutôt subjective, le Centre pour la cybersécurité fait le maximum pour inclure des activités et des contrôles qui atténuent les menaces réelles et qui peuvent être mis en œuvre au moyen de produits commerciaux sur étagère (COTS pour *Commercial-Off-the-Shelf*). Il exclut de ce profil suggéré les activités et les contrôles de sécurité et de protection de la vie privée qui définissent une capacité spécialisée ou avancée non nécessaire à tous les systèmes d'information. Ce profil vise de plus à établir un juste équilibre entre la convivialité et la sécurité.

## 2.3 Contexte de menace

Ce profil a été élaboré pour protéger les activités opérationnelles contre les menaces liées à la cybersécurité qui touchent les contextes tant opérationnels que techniques.

Ce profil vise à protéger les systèmes d'information en plus des activités opérationnelles. Cette approche est essentielle puisque les menaces peuvent cibler les biens techniques du GC aux seules fins de les compromettre et de les exploiter, quel que soit le type d'activité opérationnelle que ces biens prennent en charge.

Par exemple, certains auteurs de menace ne sont pas intéressés par l'information du GC et ne cherchent pas à perturber les activités opérationnelles du GC. Ils veulent plutôt compromettre les systèmes d'information du GC de manière à commettre un délit, notamment :

- stocker des données illégales (par exemple, des images ou des films) et les échanger clandestinement avec d'autres criminels;
- lancer des attaques par déni de service visant des sites Web commerciaux;
- extorquer de l'argent;
- envoyer des pourriels;
- infecter les systèmes d'information du GC avec des maliciels.

Le Centre pour la cybersécurité a analysé l'information sur les menaces provenant de plusieurs sources, y compris les rapports d'incidents et de menaces des ministères et du SCT, en plus de procéder à ses propres analyses. Ce profil, lorsqu'il est appliqué correctement (voir la section 4), permet d'atténuer les risques d'exposition aux auteurs de menaces délibérées des catégories Md1 à Md4, ainsi qu'aux menaces accidentelles et aux risques naturels des catégories Ma1 à Ma3, telles qu'elles sont définies dans les tableaux 2 et 3 respectivement. Ce profil sera mis à jour au fil de l'évolution des capacités des auteurs de menace afin d'ajuster de manière appropriée la sélection des activités et des contrôles et d'atténuer l'incidence de ces nouvelles capacités.

Avant de sélectionner et d'adapter le profil, les organisations doivent s'assurer que le contexte de menace correspond à leur environnement. Si ce profil ne convient pas, les organisations devront créer leur propre profil en tenant compte de l'ensemble des activités et des contrôles de sécurité et de protection de la vie privée documentés dans le document *Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée* (ITSP.10.033). Pour plus de détails sur la création de profils d'activités et de contrôles de sécurité et de protection de la vie privée et les évaluations des menaces organisationnelles, prière de consulter le document *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036).

**Tableau 2 : Catégories de menaces délibérées applicables**

| Catégorie de menace | Description des auteurs de menace | Exemples de capacités croissantes des auteurs de menace |
|---|---|---|
| Md1 | Auteur de menace non antagoniste (par exemple, navigation, modification ou destruction non | Capacités de base de l'utilisatrice ou utilisateur d'accéder aux systèmes d'information et au contenu |

| | | |
|---|---|---|
| | malveillante d'information causée par un manque de formation, de sensibilisation ou d'attention) | |
| Md2 | Attaquant occasionnel et passif possédant un minimum de ressources et disposé à prendre de petits risques (par exemple, écoute clandestine, pirates ados) | Exécution d'un scanneur de vulnérabilité accessible au public<br>Exécution de scripts d'attaque de serveurs<br>Tentatives de suppression aléatoire de fichiers système<br>Modification des paramètres de fichiers de configuration |
| Md3 | Attaquant possédant un minimum de ressources et disposé à prendre des risques importants (par exemple, pirates peu sophistiqués) | Utilisation d'outils de piratage accessibles au public pour effectuer différents exploits<br>Employées et employés qui installent des chevaux de Troie et des enregistreurs de frappe dans les systèmes non protégés<br>Recours à des attaques par hameçonnage simples pour compromettre les cibles avec des maliciels<br>Exécution de programmes dans le but de faire planter les ordinateurs et les applications |
| Md4 | Attaquant sophistiqué possédant des ressources moyennes et disposé à prendre de petits risques (par exemple, crime organisé, pirates sophistiqués, organisations internationales) | Utilisation experte d'outils de piratage accessibles au public, incluant les attaques du jour zéro<br>Capacité de créer ses propres outils d'attaque dans le logiciel<br>Attaques par piratage psychologique de base<br>Capacité d'assemblage de matériel avec des composants COTS pour faciliter les attaques<br>Attaques par hameçonnage pour accéder aux cartes de crédit ou aux renseignements personnels |

**Tableau 3 : Catégories de menaces accidentelles applicables**

| Catégorie de menace | Ampleur des événements |
|---|---|
| Ma1 | Événements accidentels mineurs (par exemple, trébucher sur un câble d'alimentation, entrer des données erronées) |
| Ma2 | Événements accidentels moyens (par exemple, rendre un serveur inutilisable, corrompre une base de données, divulguer de l'information à une mauvaise personne ou organisation)<br>Pannes matérielles ou logicielles mineures (par exemple, panne de disque dur)<br>Pannes mécaniques mineures (par exemple, panne de courant dans une section d'une installation)<br>Risques naturels mineurs (par exemple, inondation locale ou tremblement de terre qui compromettent une partie d'une installation) |
| Ma3 | Événements involontaires ou accidentels graves (par exemple, sectionnement des câbles de télécommunications ou d'alimentation d'une installation, incendie dans l'installation, compromission d'information à grande échelle)<br>Pannes mécaniques moyennes (par exemple, panne de courant prolongée dans une installation)<br>Risques naturels moyens (par exemple, inondation locale ou tremblement de terre qui compromettent une installation) |

## 2.4 Relation entre les activités et les contrôles de sécurité et de protection de la vie privée et les objectifs de confidentialité, d'intégrité et de disponibilité

Les activités et les contrôles de sécurité et de protection de la vie privée sélectionnés pour ce profil visent à atténuer de manière appropriée les menaces susceptibles de compromettre la confidentialité, l'intégrité ou la disponibilité des biens utilisés pour soutenir les activités opérationnelles. Le profil ne documente pas la mise en correspondance exacte des

activités et des contrôles de sécurité et de protection de la vie privée aux objectifs spécifiques qu'ils visent à atteindre. Certaines de ces activités et certains de ces contrôles sont associés plus clairement à un objectif particulier (par exemple, le contrôle CP-7, Site de traitement auxiliaire, est associé à un objectif de disponibilité). Cela dit, la plupart de ces activités et de ces contrôles visent plus d'un objectif. Par exemple, la plupart des contrôles de la famille Contrôle d'accès visent directement ou indirectement les trois objectifs de confidentialité, d'intégrité et de disponibilité des biens. L'application adéquate du contrôle d'accès permet d'atténuer les situations de compromission dans le cadre desquelles un auteur de menace :

- exfiltre des documents sensibles contenant des renseignements personnels (objectif de confidentialité);
- modifie des documents ou des enregistrements de base de données (objectif d'intégrité et, habituellement, de disponibilité);
- trafique une application administrative pour nuire à son bon fonctionnement (objectifs d'intégrité et, possiblement, de disponibilité);
- supprime des enregistrements d'une base de données (objectif de disponibilité);
- altère une application administrative pour la rendre inexploitable (objectif de disponibilité).

# 3 Directives de mise en œuvre

Les contrôles de sécurité et de protection de la vie privée doivent être mis en œuvre d'une manière proportionnée aux menaces et aux préjudices éventuels. Ce profil a été élaboré en tenant compte de certaines hypothèses énoncées à la section 2. Par conséquent, la mise en œuvre des activités et des contrôles devrait exiger un niveau moyen d'effort et de diligence, tel qu'il est indiqué dans cette section.

## 3.1 Assurance de la sécurité

Pour satisfaire aux exigences des activités et des contrôles documentées dans ce profil, les organisations doivent définir le niveau d'effort qu'il convient de consacrer à l'élaboration, à la documentation et à l'évaluation de leur mise en œuvre.

Le document *Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée* (ITSP.10.036) décrit le processus que l'on suggère d'entamer pour mettre en œuvre ou mettre à jour les activités et les contrôles de sécurité et de protection de la vie privée de ce profil qui concernent la gestion des risques liés à la cybersécurité, de même que ceux qui ne sont pas déployés dans des systèmes d'information. Le document *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037) fournit des conseils sur le niveau d'effort attendu pour la mise en œuvre de ces activités et contrôles de sécurité et de protection de la vie privée communs (par exemple, la gestion des incidents, les évaluations des risques, le programme de filtrage de sécurité du personnel, le programme de sécurité physique).

Le document *Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes* (ITSP.10.037) décrit un processus suggéré d'ingénierie de la sécurité et de la protection de la vie privée qui permet d'assurer une conception, un développement, une mise à l'essai, une installation et une exploitation rentables de systèmes d'information fiables qui répondent aux besoins opérationnels en matière de sécurité et de protection de la vie privée. L'ITSP.10.037 fournit aux gestionnaires de projet, aux praticiennes et praticiens de la sécurité et de la protection de la vie privée, aux évaluatrices et évaluateurs de la sécurité et de la protection de la vie privée et aux responsables de l'autorisation des conseils sur le niveau d'effort que requièrent les travaux d'ingénierie de sécurité et de protection de la vie privée et les tâches d'évaluation à réaliser pour s'assurer que les mesures de cybersécurité mises en œuvre dans les systèmes d'information répondent aux objectifs de ce profil.

Dans le cas des activités et des contrôles de sécurité et de protection de la vie privée intégrés aux systèmes, le niveau d'effort approprié que requièrent les travaux d'ingénierie de sécurité et de protection de la vie privée et les tâches d'évaluation est défini en termes d'exigences d'assurance de la sécurité. Ces exigences concernent les tâches que les conceptrices, les concepteurs, les développeuses, les développeurs et les responsables de la mise en œuvre des activités et des contrôles de sécurité et de protection de la vie privée doivent accomplir pour avoir la certitude que les travaux et la documentation de l'ingénierie de sécurité sont adéquats. Ces tâches permettent également de s'assurer que les activités et les contrôles ont été mis en œuvre correctement, qu'ils fonctionnent comme prévu et qu'ils produisent les résultats escomptés tout en respectant les objectifs de sécurité définis pour les systèmes d'information. Le Centre pour la cybersécurité suggère que les projets adoptent le NAS2, tel qu'il est indiqué dans l'ITSP.10.037, pour mettre en œuvre la plupart des activités et des contrôles de sécurité et de protection de la vie privée de ce profil.

Dans le cas des activités et des contrôles critiques, plus particulièrement ceux qui concernent les frontières d'un système d'information et ceux prévus pour contrer des capacités d'auteurs de menace plus importantes, une mise en œuvre adéquate permettra de s'assurer que l'on a consacré davantage d'effort à la conception, au développement, à la mise à l'essai, à l'installation et à l'exploitation de ces activités et de ces contrôles. Le Centre pour la cybersécurité suggère que les projets adoptent le NAS3, tel qu'il est indiqué dans l'ITSP.10.037, pour mettre en œuvre les activités et les contrôles critiques de ce profil. La criticité d'une activité ou d'un contrôle varie selon la conception des systèmes d'information auxquels on l'applique et doit être déterminée par les praticiennes et praticiens de la protection de la vie privée qui ont été désignés.

De plus, concernant les niveaux d'assurance NAS1 à NAS3, les fournisseurs qui participent à la conception, au développement ou à l'exploitation d'un système d'information doivent détenir au moins une vérification d'organisation désignée, comme il est indiqué dans l'ITSP.10.037.

Il importe de souligner que le niveau d'assurance suggéré pour la mise en œuvre appropriée de ce profil ne permet pas d'assurer la protection adéquate d'un système d'information contre les auteurs de menace ayant des capacités supérieures (c'est-à-dire ceux associés aux niveaux de menace Md5, Md6 et Md7 et qui sont très qualifiés, motivés et outillés).

L'ITSP.10.037 fournit aux équipes de projets des directives plus détaillées sur les exigences d'assurance de la sécurité et sur les tâches de développement, de documentation et d'évaluation requises pour y répondre.

Par ailleurs, le Centre pour la cybersécurité recommande d'évaluer les produits commerciaux sélectionnés et dotés de fonctions de sécurité afin de s'assurer qu'ils fonctionnent de la manière prévue et sont suffisamment résilients pour cerner les menaces. Pour faciliter ce processus d'assurance et veiller à ce que les produits soient évalués par rapport aux exigences appropriées en matière de sécurité, le Centre pour la cybersécurité fournit une liste des produits commerciaux disponibles qui ont été évalués dans le cadre du programme de Critères communs (CC). Le Centre pour la cybersécurité a évalué ces produits en partenariat avec certains laboratoires commerciaux[4] et les organisations peuvent les utiliser à leur discrétion. Si les organisations choisissent d'utiliser cette liste de produits validés par le Centre pour la cybersécurité, les processus d'approvisionnement devraient indiquer que les produits de sécurité sélectionnés ont été vérifiés par le programme des CC par rapport à une cible de sécurité appropriée ou à un profil de protection des CC[5]. La cible ou le profil est soit défini par l'organisation dans les normes de sécurité, soit déterminé par les praticiennes et praticiens de la sécurité du projet pour satisfaire aux exigences des sections 2 et 3. Si le produit comporte un module cryptographique, il doit également être vérifié par le Programme de validation des modules cryptographiques[6] (PVMC), un programme conjoint du Centre pour la cybersécurité et du National Institute of Standards and Technology (NIST). On retrouve une base de données des modules cryptographiques validés sur le site Web du NIST (en anglais seulement).

[4] Pour de plus amples renseignements sur la liste des produits certifiés, prière de consulter la page Produits certifiés du Centre pour la cybersécurité.
[5] Pour de plus amples renseignements sur les profils protégés selon les CC, prière de consulter le portail des Critères communs (en anglais seulement).
[6] Pour de plus amples renseignements sur les modules cryptographiques, prière de consulter le site Web du PVMC (en anglais seulement).

## 3.2 Format

Le tableau à la section 4 donne la liste des activités et des contrôles de sécurité et de protection de la vie privée et des améliorations proposées pour ce profil. Chaque activité ou contrôle inclut un identifiant ainsi que les renseignements suivants :

- le nom de l'activité ou du contrôle;
- la liste des améliorations proposées;
- une description générale et des conseils sur la mise en œuvre;
- les valeurs des paramètres substituables documentés dans chaque activité ou contrôle de sécurité du profil;
- des remarques supplémentaires sur les contrôles, les activités et les améliorations dans le contexte de ce profil.

On retrouve une description complète des activités et des contrôles de sécurité et de protection de la vie privée, des améliorations et des paramètres substituables dans le *Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée* (ITSP.10.033). Les colonnes « Valeurs suggérées de paramètres substituables » et « Remarques concernant le profil » sont généralement vides. Votre organisation peut les utiliser comme des outils pour adapter son profil.

Pour faire en sorte qu'il soit plus facile pour les praticiennes et praticiens de la protection de la vie privée d'adapter le profil des activités et des contrôles de sécurité et de protection de la vie privée ou de créer un profil personnalisé, le Centre pour la cybersécurité a créé une feuille de calcul qui contient les activités et les contrôles fournis à la section 4. Envoyez un courriel à contact@cyber.gc.ca pour demander une copie de cette feuille de calcul.

# 4 Suggestion d'activités, de contrôles et d'améliorations

**Tableau 4 : Suggestion d'activités et de contrôles de sécurité et de protection de la vie privée et d'améliorations**

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| AC | 01 | Politique et procédures de contrôle d'accès | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de contrôle d'accès [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, à la jurisprudence, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de contrôle d'accès et des contrôles d'accès connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées au contrôle d'accès<br>C. Passer en revue et mettre à jour, par rapport au contrôle d'accès,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | C.1 C.2 fréquence [au moins une fois par année] | s.o. |
| AC | 02 | Gestion des comptes | A. Définir et consigner les types de comptes permis et dont l'utilisation est interdite dans le système<br>B. Affecter des gestionnaires de comptes et des responsables des données<br>C. Exiger [Affectation : prérequis et critères ayant été définis par l'organisation] en ce qui concerne l'appartenance au groupe et au rôle<br>D. Préciser :<br>1. les utilisatrices et utilisateurs autorisés du système<br>2. les membres des groupes et des rôles<br>3. les autorisations d'accès (par exemple, droits d'accès ou privilèges) et [Affectation : attributs définis par l'organisation (selon les besoins)] pour chaque compte<br>E. Obtenir l'approbation de [Affectation : personnel ou rôles définis par l'organisation] pour les demandes de création de comptes<br>F. Créer, activer, modifier, désactiver et retirer les comptes du système conformément aux [Affectation : stratégies, procédures, conditions préalables et critères définis par l'organisation]<br>G. Surveiller l'utilisation des comptes | Contrôle | Sélectionné | (J) fréquence [au moins une fois par mois] | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | H. Aviser les gestionnaires de compte et [Affectation : personnel ou rôles définis par l'organisation] dans<br>1. [Affectation : délais définis par l'organisation] lorsque les comptes ne sont plus requis ou en état de latence<br>2. [Affectation : délais définis par l'organisation] lorsque les utilisatrices et utilisateurs quittent leur emploi ou sont transférés<br>3. [Affectation : délais définis par l'organisation] lorsque l'utilisation du système ou le besoin de connaître d'une personne change<br>I. Autoriser l'accès au système en fonction de ce qui suit<br>1. une autorisation d'accès valide<br>2. l'utilisation prévue du système<br>3. [Affectation : attributs définis par l'organisation (selon les besoins)]<br>J. Examiner périodiquement les comptes pour s'assurer qu'ils sont conformes aux exigences en matière de gestion des comptes tous les [Affectation : fréquence définie par l'organisation]<br>K. Établir et mettre en œuvre un processus de changement des authentifiants de compte partagé ou de groupe (s'ils sont déployés) lorsque des utilisatrices et utilisateurs sont retirés du groupe<br>L. Aligner les processus de gestion des comptes avec les processus de cessation d'emploi et de mutation de personnel | | | | |
| AC | 02(01) | Gestion des comptes | Gestion des comptes : Gestion automatisée des comptes système<br>Appuyer la gestion des comptes système au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 02(02) | Gestion des comptes | Gestion des comptes : Gestion automatisée des comptes temporaires et des comptes d'urgence<br>Automatiquement, le système [Sélection (un choix) : supprime; désactive] les comptes temporaires et d'urgence après [Affectation : délais définis par l'organisation pour chaque type de compte]. | Contrôle | Sélectionné | délai [au plus 48 heures après que le compte n'est plus requis] | s.o. |
| AC | 02(03) | Gestion des comptes | Gestion des comptes : Désactivation des comptes<br>Désactiver les comptes dans [Affectation : délais définis par l'organisation] lorsque les comptes :<br>a. ont expiré<br>b. ne sont plus associés à une utilisatrice ou un utilisateur, ou à une personne<br>c. contreviennent à une politique organisationnelle<br>d. sont inactifs depuis [Affectation : délais définis par l'organisation] | Contrôle | Sélectionné | a. b. délai [au plus 30 jours]<br>c. délai [au plus 24 heures] | s.o. |
| AC | 02(04) | Gestion des comptes | Gestion des comptes : Opérations automatisées de vérification<br>Vérification automatique des activités de création, de modification, d'activation, de désactivation et de retrait des comptes. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 02(05) | Gestion des comptes | Gestion des comptes : Fermeture de session en cas d'inactivité<br>Exiger des utilisatrices et utilisateurs qu'ils ferment leur session après [Affectation : délai d'inactivité prévu ou description du moment de la fermeture de session définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 02(06) | Gestion des comptes | Gestion des comptes : Gestion dynamique des droits d'accès<br>Mettre en œuvre des [Affectation : capacités de gestion dynamique des droits d'accès définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 02(07) | Gestion des comptes | Gestion des comptes : Comptes d'utilisateur privilégiés<br>a. Établir et administrer des comptes d'utilisateur privilégiés conformément à un [Sélection (un choix) : plan de contrôle d'accès basé sur les rôles; plan d'accès basés sur les attributs]<br>b. Surveiller les attributions de rôles privilégiés ou d'attributs | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | c. Surveiller les changements aux rôles ou aux attributs<br>d. Révoquer l'accès lorsque les attributions de rôles privilégiés ou d'attributs ne conviennent plus | | | | |
| AC | 02(08) | Gestion des comptes | Gestion des comptes : Gestion dynamique des comptes<br>Créer, activer, gérer et désactiver [Affectation : comptes du système définis par l'organisation] de manière dynamique. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 02(09) | Gestion des comptes | Gestion des comptes : Restrictions liées à l'utilisation de comptes partagés et de groupe<br>Autoriser uniquement l'utilisation des comptes partagés et de groupe qui répondent aux [Affectation : conditions relatives à l'établissement de comptes partagés et de groupe définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 02(10) | Gestion des comptes | Gestion des comptes : Changement de justificatifs d'identité de comptes partagés et de groupe<br>Annulé : Intégré au contrôle AC-2K. | s.o. | Sélectionné | s.o. | s.o. |
| AC | 02(11) | Gestion des comptes | Gestion des comptes : Conditions d'utilisation<br>Appliquer [Affectation : circonstances et/ou conditions d'utilisation définies par l'organisation] aux [Affectation : comptes du système définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 02(12) | Gestion des comptes | Gestion des comptes : Surveillance des comptes pour utilisation irrégulière<br>a. Surveiller les comptes de système afin de détecter [Affectation : utilisation irrégulière définie par l'organisation]<br>b. Signaler une utilisation irrégulière des comptes de système à [Affectation : personnel ou rôles définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 02(13) | Gestion des comptes | Gestion des comptes : Désactivation des comptes des personnes à risque élevé<br>Désactiver des comptes du personnel dans les [Affectation : délais définis par l'organisation] après la découverte des [Affectation : risques importants définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 03 | Application de l'accès | Appliquer les autorisations approuvées pour l'accès logique à l'information et aux ressources système conformément aux stratégies de contrôle d'accès applicables. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 03(01) | Application de l'accès | Application de l'accès : Restriction de l'accès aux fonctions privilégiées<br>Annulé : Intégré au contrôle AC-06. | s.o. | s.o. | s.o. | s.o. |
| AC | 03(02) | Application de l'accès | Application de l'accès : Double autorisation<br>Appliquer une double autorisation pour [Affectation : commandes privilégiées ou autres mesures définies par l'organisation]. | Contrôle | Sélectionné | [1] commandes privilégiées [création et suppression de comptes d'agentes et agents d'ICP, d'administratrices et d'administrateur]<br>[2] actions [par exemple : changements d'ICP pour des administratrices, des administrateurs, des agentes et des agents de la sécurité; actions des administratrices et administrateurs globaux dans les architectures infonuagiques; actions | Les organisations doivent évaluer quelles actions administratives peuvent causer de graves préjudices. Ces actions sont sujettes à une double autorisation. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | des administratrices et administrateurs de domaine dans des systèmes à forêt unique. | |
| AC | 03(03) | Application de l'accès | Application de l'accès : Contrôle d'accès obligatoire<br>Appliquer la [Affectation : stratégie de contrôle d'accès non discrétionnaire définie par l'organisation] à l'ensemble de sujets et objets couverts qui sont définis dans la stratégie, quand la stratégie<br>a. est appliquée de façon uniforme pour tous les sujets et objets dans le système<br>b. précise qu'un sujet ayant reçu l'accès à l'information est contraint<br>1) d'acheminer l'information à des sujets ou à des objets non autorisés<br>2) d'octroyer ses droits d'accès à d'autres sujets<br>3) de changer un ou plusieurs attributs de sécurité (précisés par la stratégie) pour des sujets, des objets, le système ou des composants du système<br>4) de choisir les attributs de sécurité et les valeurs d'attribut (précisés par la stratégie) qui seront associés aux objets nouvellement créés ou modifiés<br>5) de changer les règles régies par le contrôle d'accès<br>c. précise que les [Affectation : sujets définis par l'organisation] peuvent accorder explicitement [Affectation : droits d'accès définis par l'organisation, de façon à ce qu'ils ne soient pas limités par les contraintes ci-dessus | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(04) | Application de l'accès | Application de l'accès : Contrôle d'accès discrétionnaire<br>Appliquer la [Affectation : stratégie de contrôle d'accès non discrétionnaire définie par l'organisation] aux ensembles de sujets et d'objets couverts qui ont été précisés dans la stratégie, et quand la stratégie précise qu'un sujet à qui l'accès à l'information a été accordé peut réaliser l'un ou l'autre des aspects suivants<br>a. acheminer l'information à d'autres sujets ou objets<br>b. octroyer ses droits d'accès à d'autres sujets<br>c. changer des attributs de sécurité de sujets, d'objets, du système ou de composants du système<br>d. choisir les attributs de sécurité qui seront associés aux objets nouvellement créés ou modifiés; par le contrôle d'accès<br>e. changer les règles régies par le contrôle d'accès | Contrôle | Sélectionné | s.o. | L'amélioration (04) clarifie le contrôle d'application de l'accès en donnant des détails sur la stratégie qui devrait être utilisée pour accéder à l'information cotée PROTÉGÉ B. Autrement dit, le système peut être autorisé à traiter cette information, mais toute l'information n'est pas nécessairement de ce type. On doit donc exercer un contrôle d'accès discrétionnaire (DAC) pour établir et appliquer à cette information le principe du besoin de savoir.<br>Exemples de DAC : les groupes Windows (au niveau d'objet fichier) et les systèmes de gestion de documents qui permettent à la ou au |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | propriétaire de modifier les permissions d'accès aux documents. |
| AC | 03(05) | Application de l'accès | Application de l'accès : Information pertinente en matière de sécurité<br>Empêcher l'accès à [Affectation : information pertinente en matière de sécurité définie par l'organisation] sauf lorsque le système est en état de non-fonctionnement sécurisé. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(06) | Application de l'accès | Application de l'accès : Protection de l'information du système, des utilisatrices et utilisateurs<br>Annulé : Intégré aux contrôles MP-04 et SC-28. | s.o. | s.o. | s.o. | s.o. |
| AC | 03(07) | Application de l'accès | Application de l'accès : Contrôle d'accès basé sur les rôles<br>Appliquer une stratégie de contrôle d'accès basé sur les rôles à des sujets et objets définis, et il contrôle l'accès en fonction des [Affectation : rôles et du personnel autorisé à assumer ces rôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(08) | Application de l'accès | Application de l'accès : Révocation des autorisations d'accès<br>Appliquer la révocation des autorisations d'accès à la suite de changements apportés aux attributs de sécurité des sujets et des objets en fonction des [Affectation : règles régissant le moment de la révocation des autorisations d'accès définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(09) | Application de l'accès | Application de l'accès : Diffusion contrôlée<br>Diffuser de l'information hors du système uniquement si<br>a. le [Affectation : système ou composant du système désigné par l'organisation] destinataire fournit les [Affectation : contrôles définis par l'organisation]<br>b. les [Affectation : contrôles définis par l'organisation] sont utilisés pour valider la pertinence de l'information désignée à des fins de diffusion | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 03(10) | Application de l'accès | Application de l'accès : Dérogation vérifiée aux mécanismes de contrôle d'accès<br>Utiliser une dérogation vérifiée aux mécanismes automatisés de contrôle d'accès en vertu des [Affectation : conditions définies par l'organisation] par les [Affectation : rôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(11) | Application de l'accès | Application de l'accès : Accès restreint à des types d'information spécifiques<br>Accès restreint à des référentiels contenant des [Affectation : types d'information définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(12) | Application de l'accès | Application de l'accès : Assurer et appliquer l'accès aux applications<br>a. Exiger des applications pour assurer, dans le cadre du processus d'installation, l'accès nécessaire aux applications et fonctions de systèmes suivantes : [Affectation : applications et fonctions de systèmes définies par l'organisation]<br>b. Fournir un mécanisme d'application de l'accès pour empêcher les accès non autorisés<br>c. Approuver les changements d'accès après l'installation initiale de l'application | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(13) | Application de l'accès | Application de l'accès : Contrôle d'accès basé sur les attributs<br>Appliquer une stratégie de contrôle d'accès basé sur les attributs des sujets et objets définis, et contrôler l'accès en fonction des [Affectation : attributs définis par l'organisation pour assumer les autorisations d'accès]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 03(14) | Application de l'accès | Application de l'accès : Accès individuel<br>Fournir les [Affectation : mécanismes définis par l'organisation] pour permettre aux personnes d'avoir accès aux éléments suivants des renseignements personnels : [Affectation : éléments définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 03(15) | Application de l'accès | Application de l'accès : Contrôle d'accès discrétionnaire et obligatoire<br>a. Appliquer la [Affectation : stratégie de contrôle d'accès non discrétionnaire définie par l'organisation] à l'ensemble de sujets et objets couverts qui sont définis dans la stratégie<br>b. Appliquer la [Affectation : stratégie de contrôle d'accès discrétionnaire définie par l'organisation] à l'ensemble de sujets et objets couverts qui sont définis dans la stratégie | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04 | Application du contrôle de flux d'information | Appliquer des autorisations approuvées pour contrôler le flux d'information dans le système et entre les systèmes reconnectés en fonction des [Affectation : stratégies de contrôle de flux d'information définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 04(01) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Attributs de sécurité et de protection de la vie privée des objets<br>Utiliser des [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] associés aux [Affectation : objets d'information, de source et de destination définis par l'organisation] pour appliquer les [Affectation : stratégies de contrôle de flux d'information définies par l'organisation] comme base pour les décisions concernant le contrôle de flux. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(02) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Domaines de traitement<br>Utiliser des domaines de traitement protégés pour appliquer les [Affectation : stratégies de contrôle de flux d'information définies par l'organisation] comme base pour les décisions concernant le contrôle de flux. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(03) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Contrôle dynamique de flux d'information<br>Appliquer les [Affectation : stratégies de contrôle de flux d'information définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(04) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Contrôle de flux de l'information chiffrée<br>Le système empêche l'information chiffrée de contourner les [Affectation : mécanismes de vérification de contenu] en [Sélection (un choix ou plus) : déchiffrant l'information; bloquant le flux d'information chiffrée; en mettant fin aux sessions de communication qui tentent d'acheminer l'information chiffrée; [Affectation : procédure ou méthode définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(05) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Types de données intégrés<br>Appliquer [Affectation : restrictions définies par l'organisation] concernant l'intégration de types de données dans d'autres types de données. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(06) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Métadonnées<br>Appliquer le contrôle de flux d'information en fonction des [Affectation : métadonnées définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(07) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Mécanismes de flux unidirectionnels<br>Appliquer des flux unidirectionnels d'information par des mécanismes de contrôle de flux matériel. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(08) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Filtres de stratégie de sécurité et protection de la vie privée<br>a. Appliquer le contrôle de flux d'information en utilisant des [Affectation : filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation] comme base pour les décisions de contrôle de flux pour les [Affectation : flux d'information définis par l'organisation]<br>b. [Sélection (un choix ou plus) : Bloquer; retirer; modifier; mettre en quarantaine] les données après l'échec d'un | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | traitement de filtre conformément à [Affectation : stratégie de sécurité ou de protection de la vie privée définie par l'organisation] | | | | |
| AC | 04(09) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Vérifications manuelles<br>Appliquer l'utilisation de vérifications manuelles pour les [Affectation : flux d'information définis par l'organisation] selon les modalités suivantes : [Affectation : modalités définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(10) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Activer et désactiver les filtres de stratégie de sécurité et de protection de la vie privée<br>Permettre à une administratrice ou à un administrateur privilégié d'activer ou de désactiver les [Affectation : filtres de la stratégie de sécurité définis par l'organisation] selon les modalités suivantes : [Affectation : modalités définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(11) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Configuration des filtres de stratégie de sécurité et de protection de la vie privée<br>Permettre à des administratrices et administrateurs privilégiés de configurer [Affectation : filtres de la stratégie de sécurité ou de protection de la vie privée définis par l'organisation] pour appuyer les différentes stratégies de sécurité ou de protection de la vie privée. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(12) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Identifiants de type de données<br>Lors du transfert d'information entre différents domaines de sécurité, utiliser des [Affectation : identifiants de type de données définis par l'organisation] pour valider les données essentielles aux décisions liées au flux d'information. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(13) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Décomposition en sous-composantes pertinentes<br>Lors du transfert d'information entre différents domaines de sécurité, décomposer l'information en [Affectation : sous-composantes pertinentes définies par l'organisation] pour la présenter aux mécanismes d'application de la stratégie. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(14) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Contraintes liées aux filtres de stratégie de sécurité ou de protection de la vie privée<br>Lors du transfert d'information entre différents domaines de sécurité, appliquer des [Affectation : filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation] qui exigent des formats entièrement énumérés limitant le contenu et la structure des données. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(15) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Détection de l'information non autorisée<br>Lors du transfert d'information entre différents domaines de sécurité, examiner l'information afin de détecter la présence de [Affectation : information non autorisée définie par l'organisation] et interdire le transfert de cette information, conformément à la [Affectation : stratégie de sécurité ou de conformité définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(16) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Transferts d'information sur des systèmes interconnectés<br>Annulé : Intégré au contrôle AC-04. | s.o. | s.o. | s.o. | s.o. |
| AC | 04(17) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Authentification des domaines<br>Identifier de façon unique et authentifier les points source et destination par [sélection (un choix ou plus) : organisation, système, application, service, personne] à des fins de transfert d'information. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 04(18) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Liaison d'attribut de sécurité<br>Annulé : Intégré au contrôle AC-16. | s.o. | s.o. | s.o. | s.o. |
| AC | 04(19) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Validation des métadonnées<br>Lors du transfert de l'information entre différents domaines de sécurité, mettre en œuvre les [Affectation : filtres de stratégie de sécurité ou de protection de la vie privée définis par l'organisation] en fonction des métadonnées. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(20) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Solutions approuvées<br>Utiliser des [Affectation : solutions définies par l'organisation dans les configurations approuvées] pour contrôler le flux de [Affectation : l'information définie par l'organisation] dans les domaines de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(21) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Séparation physique ou logique des flux d'information<br>Séparer les flux d'information de façon logique ou physique au moyen de [Affectation : mécanismes et/ou techniques définis par l'organisation] pour accomplir les [Affectation : séparations requises par type d'information définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(22) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Accès seulement<br>Fournir à un seul dispositif l'accès aux plateformes informatiques, aux applications ou aux données contenues dans des domaines de sécurité différents tout en empêchant le flux d'information entre les différents domaines de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(23) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Modifier l'information non communicable<br>Lors du transfert d'information entre différents domaines de sécurité, modifier l'information non communicable en mettant en œuvre une [Affectation : mesure modifiable définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(24) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Format normalisé interne<br>Lors du transfert d'information entre différents domaines de sécurité, analyser des données entrantes dans un format normalisé interne et régénérer les données pour qu'elles soient conformes aux spécifications prévues. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(25) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Nettoyage des données<br>Lors du transfert d'information entre différents domaines de sécurité, nettoyer les données pour minimiser la [Sélection (un choix ou plus) : livraison de contenu malveillant, la commande et le contrôle de code malveillant, l'augmentation de code malveillant, et les données codées par stéganographie; fuite d'information sensible] conformément à la [Affectation : stratégie définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(26) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Mesures de filtrage de vérification<br>Lors du transfert d'information entre différents domaines de sécurité, enregistrer et vérifier les mesures de filtrage de contenu ainsi que les résultats pour l'information faisant l'objet du filtrage. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(27) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Mécanismes de filtrage redondants et indépendants<br>Lors du transfert d'information entre différents domaines de sécurité, mettre en œuvre des solutions de filtrage de contenu qui offrent des mécanismes de filtrage de contenu redondants et indépendants pour chaque type de données. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(28) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Pipelines de filtre linéaire<br>Lors du transfert d'information entre différents domaines de sécurité, mettre en œuvre un pipeline de filtre de contenu linéaire qui est appliqué avec contrôle d'accès discrétionnaire et obligatoire. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 04(29) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Moteurs d'orchestration de filtre<br>Lors du transfert d'information entre différents domaines de sécurité, utiliser des moteurs d'orchestration de filtre de contenu pour s'assurer de ce qui suit<br>a. les mécanismes de filtrage de contenu ont réussi l'exécution sans présenter d'erreurs<br>b. les opérations de filtrage de contenu sont exécutées dans le bon ordre et sont conforment à la [Affectation : stratégie définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(30) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Mécanismes de filtrage à l'aide de plusieurs processus<br>Lors du transfert d'information entre différents domaines de sécurité, mettre en œuvre des mécanismes de filtrage de contenu à l'aide de plusieurs processus. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(31) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Prévenir l'échec d'un transfert de contenu<br>Lors du transfert d'information entre différents domaines de sécurité, prévenir l'échec d'un transfert de contenu vers le domaine destinataire. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 04(32) | Application du contrôle de flux d'information | Application du contrôle de flux d'information : Exigences des processus pour le transfert d'information<br>Lors du transfert d'information entre différents domaines de sécurité, le processus qui transfert l'information entre les pipelines de filtre<br>a. ne filtre pas le contenu du message<br>b. valide les métadonnées de filtrage<br>c. assure que le contenu associé aux métadonnées de filtrage a effectué avec succès le filtrage<br>d. transfert le contenu au pipeline de filtre de destination | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 05 | Séparation des tâches | A. Identifier et consigner les [Affectation : tâches assumées par le personnel définies par l'organisation nécessitant une séparation]<br>B. Définir les autorisations d'accès au système afin d'appuyer la séparation des tâches | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06 | Droit d'accès minimal | Utiliser le principe du droit d'accès minimal, ce qui autorise l'accès uniquement aux utilisatrices et utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées par l'organisation. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06(01) | Droit d'accès minimal | Droit d'accès minimal : Autorisation de l'accès aux fonctions de sécurité<br>Autoriser l'accès à [Affectation : personnel et rôles définis par l'organisation] pour<br>a. les [Affectation : fonctions de sécurité définies par l'organisation (déployées dans le matériel, les logiciels et les micrologiciels)]<br>b. [Affectation : information liée à la sécurité définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06(02) | Droit d'accès minimal | Droit d'accès minimal : Accès non privilégié aux fonctions non liées à la sécurité<br>Exiger que les utilisatrices et utilisateurs de comptes ou de rôles de système qui ont accès aux [Affectation : fonctions de sécurité et informations sur la sécurité définies par l'organisation] utilisent des comptes ou des rôles non privilégiés pour accéder à des fonctions qui ne sont pas liées à la sécurité. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06(03) | Droit d'accès minimal | Droit d'accès minimal : Accès réseau aux commandes privilégiées<br>Autoriser l'accès réseau aux [Affectation : commandes privilégiées définies par l'organisation] seulement pour [Affectation : répondre à des besoins opérationnels urgents définis par l'organisation] et consigner les motifs d'un tel accès dans le plan de sécurité pour le système. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 06(04) | Droit d'accès minimal | Droit d'accès minimal : Domaines de traitement séparés<br>Fournir des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès d'utilisatrice et utilisateur. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 06(05) | Droit d'accès minimal | Droit d'accès minimal : Comptes privilégiés<br>Restreindre les comptes privilégiés sur le système à [Affectation : personnel ou rôles définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06(06) | Droit d'accès minimal | Droit d'accès minimal : Accès privilégié des utilisatrices et utilisateurs ne faisant pas partie de l'organisation<br>Interdire tout accès privilégié au système aux utilisatrices et utilisateurs ne faisant pas partie de l'organisation. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 06(07) | Droit d'accès minimal | Droit d'accès minimal : Examen des privilèges d'utilisateur<br>a. Examiner les [Affectation : droits d'accès attribués aux [Affectation : rôles ou classes d'utilisateur définis par l'organisation] tous les [Affectation : fréquence définie par l'organisation] pour valider la nécessité de détenir ces droits d'accès<br>b. Réattribuer ou retirer les droits d'accès, au besoin, pour bien refléter les besoins organisationnels liés à la mission et aux opérations | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06(08) | Droit d'accès minimal | Droit d'accès minimal : Niveaux de droits d'accès pour une exécution de code<br>Empêcher les logiciels d'être exécutés à des niveaux de droits d'accès plus élevés que ceux des utilisatrices et utilisateurs qui exécutent les logiciels : [Affectation : logiciels définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 06(09) | Droit d'accès minimal | Droit d'accès minimal : Journalisation de l'utilisation des fonctions privilégiées<br>Journaliser l'exécution de fonctions privilégiées. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 06(10) | Droit d'accès minimal | Droit d'accès minimal : Interdiction aux utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées<br>Empêcher les utilisatrices et utilisateurs non privilégiés d'exécuter des fonctions privilégiées. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 07 | Tentatives d'ouverture de session infructueuses | A. Appliquer une limite de [Affectation : nombre défini par l'organisation] tentatives d'ouverture de session non valides consécutives par l'utilisatrice ou utilisateur sur une période de [Affectation : délais définis par l'organisation]<br>B. [Sélection (un choix ou plus) : Verrouiller le compte ou le nœud pendant [Affectation : délais définis par l'organisation]; verrouiller le compte ou le nœud jusqu'à ce qu'une administratrice ou un administrateur le libère; retarder la prochaine invite d'ouverture de session selon [Affectation : algorithme de temporisation défini par l'organisation]; aviser l'administratrice ou administrateur de système; effectuer une autre [Affectation : opération définie par l'organisation] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé | Contrôle | Sélectionné | A. nombre [maximum de cinq]<br>A. délai [au moins cinq minutes] | s.o. |
| AC | 07(01) | Tentatives d'ouverture de session infructueuses | Tentatives d'ouverture de session infructueuses : Verrouillage automatique du compte<br>Annulé : Intégré au contrôle AC-07. | s.o. | s.o. | s.o. | s.o. |
| AC | 07(02) | Tentatives d'ouverture de session infructueuses | Tentatives d'ouverture de session infructueuses : Purge ou nettoyage d'appareils mobiles<br>Le système purge ou nettoie l'information des [Affectation : appareils mobiles définis par l'organisation] en fonction des [Affectation : techniques ou exigences en matière de purge ou de nettoyage définies par l'organisation] après [Affectation : nombre défini par l'organisation] tentatives infructueuses d'ouverture de session consécutives sur les appareils. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 07(03) | Tentatives d'ouverture de session infructueuses | Tentatives d'ouverture de session infructueuses : Limitation des tentatives par biométrie<br>Limiter le nombre de tentatives d'ouvertures de session infructueuses par biométrie à [Affectation : nombre défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 07(04) | Tentatives d'ouverture de session infructueuses | Tentatives d'ouverture de session infructueuses : Utilisation d'un autre facteur d'authentification<br>a. Permettre l'utilisation de [Affectation : facteurs d'authentification définis par l'organisation] qui sont différents des facteurs d'authentification principaux après que le nombre de tentatives d'ouverture de session non valides consécutives définies par l'organisation ait été dépassé<br>b. Appliquer une limite de [Affectation : nombre défini par l'organisation] tentatives d'ouverture de session non valides consécutives au moyen d'autres facteurs par l'utilisatrice ou utilisateur sur une période de [Affectation : délais définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 08 | Avis d'utilisation système | A. Afficher aux utilisatrices et utilisateurs [Affectation : message ou bannière d'avis d'utilisation du système défini par l'organisation], qui comprend des énoncés de protection de la vie privée et de sécurité conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables, et stipule ce qui suit<br>1. les utilisatrices et utilisateurs accèdent à un système du gouvernement du Canada<br>2. l'utilisation du système peut être surveillée, enregistrée et faire l'objet d'une vérification<br>3. l'utilisation non autorisée du système est interdite et passible à des amendes administratives et à des sanctions pénales<br>4. les fichiers de renseignements personnels pertinents, le cas échéant<br>5. l'autorité légale pour la collecte de renseignements personnels<br>6. les conséquences juridiques et administratives de tout refus de fournir des renseignements personnels<br>7. le droit de protection des renseignements personnels et le droit d'y accéder et de faire des demandes de correction<br>8. la manière dont les renseignements seront utilisés<br>9. le droit de déposer une plainte auprès du Commissariat à la protection de la vie privée du Canada concernant le traitement par les institutions des renseignements personnels des gens<br>B. Afficher le message ou la bannière d'avis jusqu'à ce que l'utilisatrice ou utilisateur accepte les modalités d'utilisation et opter d'ouvrir une session ou d'accéder au système<br>C. Dans le cas de systèmes accessibles au public<br>1. afficher l'information sur l'utilisation du système selon les [Affectation : modalités définies par l'organisation] avant d'accorder l'accès<br>2. afficher, au besoin, des mises en garde concernant la surveillance, l'enregistrement et la vérification conformes aux dispositions sur la protection des renseignements personnels pour de tels systèmes qui interdisent généralement ces activités<br>3. comprendre une description des utilisations autorisées du système | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 09 | Avis d'ouverture de session précédente | Indiquer à l'utilisatrice ou utilisateur qui vient d'ouvrir une session sur le système la date et l'heure de sa dernière ouverture de session. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 09(01) | Avis d'ouverture de session précédente | Avis d'ouverture de session précédente : Ouvertures de session infructueuses<br>Indiquer à l'utilisatrice ou utilisateur qui vient d'ouvrir une session le nombre de tentatives d'ouverture de session infructueuses depuis sa dernière tentative réussie. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 09(02) | Avis d'ouverture de session précédente | Avis d'ouverture de session précédente : Tentatives fructueuses et infructueuses d'ouverture de session<br>Indiquer à l'utilisatrice ou utilisateur qui vient d'ouvrir une session le nombre de [Sélection (un choix) : tentatives d'ouverture de session fructueuses; tentatives d'ouverture de session infructueuses; tentatives d'ouverture de session fructueuses et infructueuses] pendant [Affectation : délais définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 09(03) | Avis d'ouverture de session précédente | Avis d'ouverture de session précédente : Avis de changements au compte<br>Aviser l'utilisatrice ou utilisateur qui vient d'ouvrir une session des changements apportés aux [Affectation : caractéristiques ou paramètres liés à la sécurité appliqués au compte de l'utilisatrice ou utilisateur définis par l'organisation] pendant [Affectation : délai défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 09(04) | Avis d'ouverture de session précédente | Avis d'ouverture de session précédente : Information supplémentaire sur l'ouverture de session<br>Aviser l'utilisatrice ou utilisateur qui vient d'ouvrir une session de l'information supplémentaire suivante : [Affectation : information supplémentaire définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 10 | Contrôle de sessions simultanées | Limiter le nombre de sessions simultanées pour chaque [Affectation : type de compte et/ou compte défini par l'organisation] à [Affectation : nombre défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 11 | Verrouillage d'appareil | A. Empêcher d'autres accès au système [Sélection (un choix ou plus) : en procédant à un verrouillage d'appareil après [Affectation : délai défini par l'organisation] d'inactivité; en exigeant que l'utilisatrice ou utilisateur procède à un verrouillage d'appareil avant de laisser le système sans surveillance]<br>B. Préserver le verrouillage d'appareil jusqu'à ce que l'utilisatrice ou utilisateur rétablisse l'accès au moyen des procédures d'identification et d'authentification établies | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 11(01) | Verrouillage d'appareil | Verrouillage d'appareil : Masquage de l'affichage au moyen d'une image<br>Masquer, au moyen d'un verrouillage d'appareil, l'information auparavant visible à l'écran en utilisant une image visible. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 12 | Fin de session | Mettre automatiquement fin à une session utilisateur après [Affectation : conditions ou événements déclenchant une déconnexion définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 12(01) | Fin de session | Fin de session : Fermetures de session exécutées par les utilisatrices et utilisateurs<br>Fournir une capacité de fermeture de session pour les sessions de communication lancées par les utilisatrices et utilisateurs lorsque l'authentification est utilisée pour accéder aux [Affectation : ressources d'information désignées par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 12(02) | Fin de session | Fin de session : Message d'interruption<br>Afficher un message explicite de fermeture de session pour indiquer aux utilisatrices et utilisateurs l'interruption des sessions de communication authentifiées. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 12(03) | Fin de session | Fin de session : Message d'avertissement de délai d'expiration<br>Afficher un message explicite aux utilisatrices et utilisateurs pour indiquer que la session prendra fin [Affectation : d'ici la fin de session définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 13 | Surveillance et examen – Contrôle d'accès | Annulé : Intégré aux contrôles AC-02 et AU-06. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 14 | Opérations permises sans identification ni authentification | A. Identifier les [Affectation : opérations de l'utilisatrice ou utilisateur définies par l'organisation] que l'utilisatrice ou utilisateur peut exécuter dans le système sans devoir s'identifier ni s'authentifier, conformément aux fonctions opérationnelles et à la mission de l'organisation<br>B. Consigner et expliquer dans le plan de sécurité du système la logique sous-jacente qui permet à l'utilisatrice ou utilisateur d'effectuer des opérations qui ne nécessitent ni identification ni authentification | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 14(01) | Opérations permises sans identification ni authentification | Opérations permises sans identification ni authentification : Usages indispensables<br>Annulé : Intégré au contrôle AC-14. | s.o. | s.o. | s.o. | s.o. |
| AC | 15 | Marquage automatique | Annulé : Intégré au contrôle MP-03. | s.o. | s.o. | s.o. | s.o. |
| AC | 16 | Attributs de sécurité et de protection de la vie privée | A. Fournir les moyens permettant d'associer les [Affectation : types d'attribut de sécurité et de protection de la vie privée définis par l'organisation] avec les [Affectation : valeurs des attributs de sécurité définies par l'organisation] pour l'information pendant qu'elle est stockée, traitée et/ou transmise<br>B. S'assurer que toutes les associations d'attribut de sécurité sont effectuées et conservées avec l'information<br>C. Établir les attributs de sécurité et de protection de la vie privée autorisés suivants à partir des attributs définis dans le contrôle AC-16A pour [Affectation : systèmes définis par l'organisation] : [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation]<br>D. Déterminer les valeurs ou les plages autorisées des attributs suivants pour chacun des attributs définis : [Affectation : valeurs des attributs ou des plages définies par l'organisation pour les attributs définis]<br>E. Vérifier les changements apportés aux attributs<br>F. Examiner les [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] aux fins d'applicabilité [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | Dans le contexte de ce profil, l'objectif du contrôle et d'assurer l'étiquetage uniforme du matériel PROTÉGÉ B au niveau maximal permis par les mécanismes automatisés existants (par exemple, le système de courrier électronique qui applique les étiquettes de classification). Puisque toute l'information contenue dans le système ne sera pas de nature sensible, l'étiquetage permettra d'empêcher la distribution accidentelle d'information cotée PROTÉGÉ B en offrant des mécanismes de filtrage dotés d'un différentiateur. |
| AC | 16(01) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Association dynamique d'attribut<br>Associer de manière dynamique les attributs de sécurité et de protection de la vie privée aux [Affectation : sujets et objets définis par l'organisation] conformément aux stratégies de sécurité et de protection de la vie privée suivantes au moment où l'information est créée et combinée : [Affectation : stratégies de sécurité et de protection de la vie privée définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 16(02) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Changements aux valeurs d'attribut par des personnes autorisées<br>Fournir à des personnes autorisées (ou à des processus exécutés au nom des personnes) la capacité de définir ou de changer la valeur des attributs de sécurité et de protection de la vie privée connexes. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 16(03) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Maintenance des associations d'attributs par système<br>Maintenir l'intégrité des [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] et l'association de ceux-ci aux [Affectation : sujets et objets définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 16(04) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Association d'attributs par personnes autorisées<br>Fournir les moyens d'associer des [Affectation : Attributs de sécurité et de protection de la vie privée définies par l'organisation] aux [Affectation : sujets et objets définis par l'organisation] effectuée par des personnes autorisées (ou par des processus exécutés en leur nom). | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 16(05) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Affichage d'attributs des objets transmis à des dispositifs de sortie<br>Afficher sous forme lisible les attributs de sécurité et de protection de la vie privée de chaque objet que le système transmet à des dispositifs de sortie afin d'identifier les [Affectation : instructions spéciales de diffusion, de traitement ou de distribution définies par l'organisation] conformément aux [Affectation : conventions d'appellation standard, en langage lisible, définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 16(06) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Maintien des associations d'attributs<br>Permettre au personnel d'associer les [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] aux [Affectation : sujets et objets définis par l'organisation] et de maintenir cette association, conformément aux [Affectation : stratégies de sécurité et de sécurité définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 16(07) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Interprétation uniforme des attributs<br>Fournir une interprétation uniforme des attributs de sécurité et de protection de la vie privée transmis entre les composants du système distribués. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 16(08) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Techniques et technologies d'association<br>Mettre en œuvre des [Affectation : techniques et technologies définies par l'organisation] en associant des attributs de sécurité et de protection de la vie privée à l'information. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 16(09) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Réaffectation d'attribut – Mécanismes remaniés<br>Changer les attributs de sécurité et de protection de la vie privée associés à l'information uniquement par des mécanismes remaniés validés au moyen de [Affectation : techniques ou procédures définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 16(10) | Attributs de sécurité et de protection de la vie privée | Attributs de sécurité et de protection de la vie privée : Configuration d'attribut par des personnes autorisées<br>Fournir aux personnes autorisées la capacité de définir ou de changer le type et la valeur des attributs de sécurité et de protection de la vie privée disponibles pouvant être associés à des sujets et à des objets. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 17 | Accès à distance | A. Définir et consigner les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre de chaque type d'accès à distance autorisé<br>B. Autoriser chaque type d'accès sans fil au système avant d'autoriser de telles connexions | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 17(01) | Accès à distance | Accès à distance : Surveillance et contrôle<br>Utiliser des mécanismes automatisés pour faciliter la surveillance et le contrôle des méthodes d'accès à distance. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 17(02) | Accès à distance | Accès à distance : Protection de la confidentialité et de l'intégrité au moyen du chiffrement<br>Mettre en œuvre des mécanismes cryptographiques pour protéger la confidentialité et l'intégrité des sessions d'accès à distance. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 17(03) | Accès à distance | Accès à distance : Points de contrôle d'accès gérés<br>Acheminer l'accès distant au moyen de points de contrôle d'accès réseau autorisés et gérés. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 17(04) | Accès à distance | Accès à distance : Commandes et accès privilégiés<br>a. Autorise l'exécution de commandes privilégiées et de l'accès à l'information liée à la sécurité au moyen de l'accès à distance seulement dans un format qui fournit des preuves justificatives de confiance, et ce, pour les besoins suivants : [Affectation : besoins définis par l'organisation]<br>b. Consigner la justification pour cet accès dans le plan de sécurité du système | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 17(05) | Accès à distance | Accès à distance : Surveillance pour connexions non autorisées<br>Annulé : Intégré au contrôle SI-04. | s.o. | s.o. | s.o. | s.o. |
| AC | 17(06) | Accès à distance | Accès à distance : Protection de l'information sur les mécanismes<br>Protéger l'information sur les mécanismes d'accès à distance contre toute utilisation et divulgation non autorisée. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 17(07) | Accès à distance | Accès à distance : Protection supplémentaire pour l'accès aux fonctions de sécurité<br>Annulé : Intégré au contrôle AC-03(10). | s.o. | s.o. | s.o. | s.o. |
| AC | 17(08) | Accès à distance | Accès à distance : Désactiver les protocoles réseau non sécurisés<br>Annulé : Intégré au contrôle CM-07. | s.o. | s.o. | s.o. | s.o. |
| AC | 17(09) | Accès à distance | Accès à distance : Déconnecter ou désactiver l'accès<br>Fournir la capacité de déconnecter ou de désactiver l'accès à distance au système dans un délai de [Affectation : délai défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 17(10) | Accès à distance | Accès à distance : Authentification des commandes à distance<br>Mettre en place les [Affectation : mécanismes définis par l'organisation] pour authentifier [Affectation : commandes à distance définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 17(400) | Accès à distance | Accès à distance : Accès à distance à des comptes privilégiés<br>L'accès à distance à des comptes privilégiés s'effectue à partir de consoles de gestion spécialisées utilisées exclusivement à cette fin. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 18 | Accès sans fil | A. Établir les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre pour chaque type d'accès sans fil<br>B. Autoriser chaque type d'accès sans fil au système avant d'autoriser de telles connexions | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 18(01) | Accès sans fil | Accès sans fil : Authentification et chiffrement<br>Protéger l'accès sans fil au système au moyen de l'authentification des [Sélection (un choix ou plus) : utilisatrices et utilisateurs; dispositifs] et du chiffrement. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 18(02) | Accès sans fil | Accès sans fil : Surveillance des connexions non autorisées<br>Annulé : Intégré au contrôle SI-04. | s.o. | s.o. | s.o. | s.o. |
| AC | 18(03) | Accès sans fil | Accès sans fil : Désactivation du réseautage sans fil<br>Désactiver, lorsqu'on ne prévoit pas les utiliser, les capacités de réseautage sans fil intégrées aux composants du système avant leur remise et leur déploiement. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 18(04) | Accès sans fil | Accès sans fil : Restriction des configurations par les utilisatrices et utilisateurs<br>Identifier les utilisatrices et utilisateurs et les autoriser explicitement à configurer eux-mêmes les capacités de réseautage sans fil. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 18(05) | Accès sans fil | Accès sans fil : Antennes et puissance de transmission<br>Sélectionner des antennes radio et calibrer la puissance de transmission afin de réduire la probabilité que les signaux puissent être reçus en dehors des frontières que contrôle l'organisation. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 19 | Contrôle d'accès pour les appareils mobiles | A. Établir les restrictions d'utilisation, les exigences en matière de configuration et de connexion, ainsi que les directives de mise en œuvre des appareils mobiles contrôlés par l'organisation de manière à inclure de tels appareils lorsqu'ils se trouvent à l'extérieur des zones contrôlées<br>B. Autoriser les connexions d'appareils mobiles aux systèmes organisationnels | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 19(01) | Contrôle d'accès pour les appareils mobiles | Contrôle d'accès pour les appareils mobiles : Utilisation d'appareils mobiles<br>Annulé : Intégré au contrôle MP-07. | s.o. | s.o. | s.o. | s.o. |
| AC | 19(02) | Contrôle d'accès pour les appareils mobiles | Contrôle d'accès pour les appareils mobiles : Utilisation de dispositifs de stockage portatifs appartenant à des particuliers<br>Annulé : Intégré au contrôle MP-07. | s.o. | s.o. | s.o. | s.o. |
| AC | 19(03) | Contrôle d'accès pour les appareils mobiles | Contrôle d'accès pour les appareils mobiles : Utilisation de dispositifs de stockage portatifs sans propriétaire identifiable<br>Annulé : Intégré au contrôle MP-07. | s.o. | s.o. | s.o. | s.o. |
| AC | 19(04) | Contrôle d'accès pour les | Contrôle d'accès pour les appareils mobiles : Restrictions liées à l'information classifiée<br>a. Interdire l'utilisation d'appareils mobiles non classifiés dans les installations qui hébergent des systèmes qui traitent, stockent ou transmettent de l'information classifiée, sauf si l'autorité responsable le permet | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | appareils mobiles | b. Appliquer par le biais de l'autorité responsable les restrictions ci-après aux personnes autorisées à utiliser des appareils mobiles non classifiés dans les installations hébergeant des systèmes qui traitent, stockent ou transmettent de l'information classifiée<br>1) il est interdit de connecter des appareils mobiles non classifiés à des systèmes classifiés<br>2) la connexion d'appareils mobiles non classifiés à des systèmes non classifiés requiert l'approbation de l'autorité responsable<br>3) il est interdit d'utiliser des modems internes ou externes, ou des interfaces sans fil, avec les appareils mobiles non classifiés<br>4) les appareils mobiles non classifiés et l'information qui y est stockée peuvent faire l'objet d'examens ou d'inspections aléatoires par [Affectation : agentes et agents de sécurité définis par l'organisation]; si l'inspection confirme la présence d'information classifiée, la stratégie de traitement des incidents est appliquée<br>c. Limiter la connexion d'appareils mobiles classifiés à des systèmes classifiés conformément aux [Affectation : stratégies de sécurité définies par l'organisation] | | | | |
| AC | 19(05) | Contrôle d'accès pour les appareils mobiles | Contrôle d'accès pour les appareils mobiles : Chiffrement complet des appareils ou chiffrement des contenants<br>Employer le [Sélection (un choix ou plus) : chiffrement complet des appareils; chiffrement des contenants] pour protéger la confidentialité et l'intégrité de l'information sur les [Affectation : appareils mobiles définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 19(400) | Contrôle d'accès pour les appareils mobiles | Contrôle d'accès pour les appareils mobiles : Appareils sans fil<br>Annulé : Transféré sous le contrôle SC-42(400). | s.o. | s.o. | s.o. | s.o. |
| AC | 20 | Utilisation de systèmes externes | A. [Sélection (un choix ou plus) : Établir les [Affectation : conditions générales d'utilisation définies par l'organisation]; identifier les [Affectation : contrôles définis par l'organisation dont la mise en place est présumée sur les systèmes externes]], conformément aux relations d'approbation établies avec les autres organisations qui possèdent, exploitent et/ou maintiennent les systèmes externes, de manière à ce que les personnes autorisées puissent faire ce qui suit<br>1. accéder au système à partir des systèmes externes<br>2. traiter, stocker ou transmettre de l'information contrôlée par l'organisation au moyen de systèmes externes<br>B. Interdire l'utilisation de [Affectation : types de systèmes externes définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 20(01) | Utilisation de systèmes externes | Utilisation de systèmes externes : Limites relatives à l'utilisation autorisée<br>Permettre aux personnes autorisées d'utiliser un système externe afin d'accéder au système ou afin de traiter, de stocker ou de transmettre de l'information contrôlée par l'organisation seulement après les opérations suivantes<br>a. vérifier que les contrôles ont été mis en œuvre dans le système externe tel qu'il est stipulé dans les stratégies de sécurité et de protection de la vie privée et les plans de sécurité et de protection de la vie privée<br>b. conserver les ententes approuvées de connexion au système ou de traitement avec l'entité organisationnelle qui héberge le système externe | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 20(02) | Utilisation de systèmes externes | Utilisation de systèmes externes : Dispositifs de stockage portatifs – Utilisation restreinte<br>Restreindre l'utilisation de dispositifs de stockage portatifs contrôlés par l'organisation aux personnes autorisées pour les systèmes externes conformément aux [Affectation : restrictions définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AC | 20(03) | Utilisation de systèmes externes | Utilisation de systèmes externes : Systèmes ne faisant pas partie de l'organisation – Utilisation restreinte<br>Limiter l'utilisation de systèmes ne faisant pas partie de l'organisation ou de composants de systèmes afin de traiter, de stocker ou de transmettre de l'information de l'organisation au moyen de [Affectation : restrictions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 20(04) | Utilisation de systèmes externes | Utilisation de systèmes externes : Dispositifs de stockage accessibles par réseau – Utilisation restreinte<br>Interdire l'utilisation de [Affectation : dispositifs de stockage accessibles par réseau, définis par l'organisation] dans des systèmes externes. | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 20(05) | Utilisation de systèmes externes | Utilisation de systèmes externes : Dispositifs de stockage portatifs – Utilisation interdite<br>Interdire l'utilisation de dispositifs de stockage portatifs contrôlés par l'organisation aux personnes autorisées pour les systèmes externes. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 21 | Échange d'information | A. Permettre aux utilisatrices et utilisateurs autorisés de déterminer si les autorisations d'accès accordées aux partenaires d'échange respectent les restrictions d'accès à l'information et d'utilisation en tenant compte de [Affectation : circonstances d'échange d'information définies par l'organisation où l'utilisateur doit faire preuve de discrétion]<br>B. Employer des [Affectation : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisatrices et utilisateurs à prendre des décisions concernant l'échange d'information et la collaboration | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 21(01) | Échange d'information | Échange d'information : Application des décisions automatisées<br>Utiliser des [Affectation : mécanismes automatisés définis par l'organisation] pour appliquer des décisions sur l'échange d'information par une utilisatrice ou un utilisateur autorisé en fonction des autorisations d'accès des partenaires d'échange et des restrictions d'accès à l'information à échanger. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 21(02) | Échange d'information | Échange d'information : Recherche et récupération d'information<br>Le système d'information met en œuvre des services de recherche et de récupération de l'information qui appliquent des [Affectation : restrictions liées à l'échange d'information définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 21(400) | Échange d'information | Échange d'information : Accord d'échange de renseignements<br>Veiller, à la suite des accords écrits, à prendre les mesures de protection appropriées de l'information sensible échangée avec des entités du secteur public externes et des organisations. | Contrôle | Sélectionné | s.o. | Propre au GC |
| AC | 21(401) | Échange d'information | Échange d'information : Entente d'échange de renseignements<br>Veiller, à la suite des ententes écrites, à prendre les mesures de protection appropriées de l'information sensible échangée entre et au sein des institutions fédérales. | Contrôle | Sélectionné | s.o. | Propre au GC |
| AC | 22 | Contenu accessible au public | A. Désigner les personnes qui sont autorisées à rendre l'information accessible au public<br>B. Former les personnes autorisées afin de s'assurer que l'information accessible au public ne contient pas d'information non publique<br>C. Examiner le contenu d'information proposé avant de l'afficher sur le système accessible au public pour s'assurer qu'il ne contient aucune information non publique<br>D. Examiner le contenu du système accessible au public tous les [Affectation : fréquence définie par l'organisation] pour vérifier s'il contient de l'information non publique et pour la supprimer, le cas échéant | Contrôle | Sélectionné | s.o. | s.o. |
| AC | 23 | Protection contre | Employer des [Affectation : techniques de détection et de prévention de l'exploration de données définies par l'organisation] pour les [Affectation : objets de stockage de données définis par l'organisation] pour détecter l'exploration de données et protéger les systèmes contre celle-ci. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | l'exploration de données | | | | | |
| AC | 24 | Décisions de contrôle d'accès | [Sélection (un choix) : Établir les procédures; mettre en œuvre des mécanismes pour s'assurer que les [Affectation : décisions de contrôle d'accès définies par l'organisation] sont appliquées à chacune des demandes d'accès avant l'application de l'accès. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 24(01) | Décisions de contrôle d'accès | Décisions de contrôle d'accès : Transmission de l'information sur l'autorisation d'accès<br>Transmettre [Affectation : information d'autorisation d'accès définie par l'organisation] au moyen de [Affectation : contrôles définis par l'organisation] aux [Affectation : systèmes désignés par l'organisation] qui appliquent les décisions de contrôle d'accès. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 24(02) | Décisions de contrôle d'accès | Décisions de contrôle d'accès : Aucune identité d'utilisatrices, utilisateurs ou processus<br>Le système applique les décisions de contrôle d'accès en fonction des [Affectation : attributs de sécurité ou de protection de la vie privée définis par l'organisation] qui ne contiennent pas l'identité d'utilisatrices ou utilisateurs ni le processus exécuté en leur nom. | Contrôle | Non sélectionné | s.o. | s.o. |
| AC | 25 | Moniteur de référence | Mettre en œuvre un moniteur de référence pour les [Affectation : stratégies de contrôle d'accès définies par l'organisation] qui est résistant aux intrusions, systématiquement appelé et suffisamment simple pour faire l'objet d'une analyse et de tests dont l'exhaustivité peut être assurée. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| AT | 01 | Politique et procédures de sensibilisation et de formation | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de sensibilisation et de formation [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. Procédures pour faciliter la mise en œuvre de la politique de sensibilisation et de formation ainsi que des contrôles de sensibilisation et de formation connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de sensibilisation et de formation.<br>C. Passer en revue et mettre à jour, par rapport à la sensibilisation et à la formation,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AT | 02 | Formation et sensibilisation en matière de sécurité | A. Fournir une formation sur la sécurité et la protection de la vie privée aux utilisatrices et utilisateurs du système (y compris les gestionnaires, les cadres supérieures et supérieurs et les entrepreneures et entrepreneurs)<br>1. dans le cadre d'une formation de base pour les nouvelles utilisatrices et nouveaux utilisateurs, et tous les [Affectation : fréquence définie par l'organisation] par la suite<br>2. lors de changements apportés au système ou à la suite de [Affectation : événements définis par l'organisation]<br>B. Utiliser les techniques suivantes pour accroître la sensibilisation à la sécurité et à la protection de la vie privée des utilisatrices et utilisateurs du système [Affectation : techniques de sensibilisation définies par l'organisation]<br>C. Mettre à jour le contenu de la formation et sensibilisation en matière de sécurité tous les [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>D. Incorporer les leçons apprises des incidents ou des violations de sécurité internes ou externes dans les techniques de formation et sensibilisation en matière de sécurité | Contrôle | Sélectionné | s.o. | s.o. |
| AT | 02(01) | Formation et sensibilisation en matière de sécurité | Formation et sensibilisation en matière de sécurité : Exercices pratiques<br>Fournir des exercices pratiques en formation en matière de sécurité qui simulent des événements et des incidents. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 02(02) | Formation et sensibilisation en matière de sécurité | Formation et sensibilisation en matière de sécurité : Menace interne<br>Fournir une formation en matière de sécurité pour que le personnel sache reconnaître les indicateurs potentiels de menace interne et pour qu'il les signale. | Contrôle | Sélectionné | s.o. | s.o. |
| AT | 02(03) | Formation et sensibilisation en matière de sécurité | Formation et sensibilisation en matière de sécurité : Piratage psychologique et exploration de données<br>Fournir une formation en matière de sécurité pour que le personnel sache reconnaître les indicateurs potentiels et réels de piratage psychologique et de l'exploration de données dans les médias sociaux. | Contrôle | Sélectionné | s.o. | s.o. |
| AT | 02(04) | Formation et sensibilisation en matière de sécurité | Formation et sensibilisation en matière de sécurité : Communications suspectes et comportements anormaux de systèmes<br>Fournir une formation en matière de sécurité sur la façon de reconnaître les communications suspectes et les comportements anormaux dans les systèmes organisationnels au moyen [Affectation : indicateurs de programmes malveillants définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 02(05) | Formation et sensibilisation en matière de sécurité | Formation et sensibilisation en matière de sécurité : Menaces persistantes avancées<br>Fournir une formation en matière de sécurité sur les menaces persistantes avancées. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 02(06) | Formation et sensibilisation en matière de sécurité | Formation et sensibilisation en matière de sécurité : Environnement de cybermenaces<br>a. Fournir une formation en matière de sécurité sur l'environnement de cybermenaces<br>b. Refléter l'information actuelle sur les cybermenaces dans les opérations du système | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 03 | Formation selon le rôle | A. Fournir une formation en sécurité et en protection de la vie privée basée sur les rôles au personnel détenant les rôles et responsabilités suivants : [Affectation : rôles et responsabilités définis par l'organisation]<br>1. avant d'autoriser l'accès au système ou à de l'information, ou avant la réalisation des tâches attribuées et tous les | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | [Affectation : fréquence définie par l'organisation] par la suite<br>2. lorsque des changements apportés au système l'exigent<br>B. Mettre à jour le contenu de la formation offerte selon le rôle tous les [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>C. Incorporer les leçons apprises des incidents ou des violations de sécurité internes ou externes dans la formation axée sur les rôles | | | | |
| AT | 03(01) | Formation selon le rôle | Formation selon le rôle : Contrôles environnementaux<br>Offrir à [Affectation : personnel ou rôles définis par l'organisation] la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 03(02) | Formation selon le rôle | Formation selon le rôle : Contrôles de sécurité physiques<br>Offrir à [Affectation : personnel ou rôles définis par l'organisation] la formation initiale sur l'utilisation et le fonctionnement des contrôles environnementaux [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 03(03) | Formation selon le rôle | Formation selon le rôle : Exercices pratiques<br>Inclure dans la formation à la sécurité et protection de la vie privée des exercices pratiques qui renforcent les objectifs de formation. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 03(04) | Formation selon le rôle | Formation selon le rôle : Communications suspectes et comportements anormaux de systèmes<br>Annulé : Transféré sous le contrôle AT-02(04). | s.o. | s.o. | s.o. | s.o. |
| AT | 03(05) | Formation selon le rôle | Formation selon le rôle : Traitement des renseignements personnels<br>Offrir à [Affectation : personnel ou rôles définis par l'organisation] la formation initiale sur l'utilisation et le fonctionnement des contrôles de traitement des renseignements personnels et de transparence [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AT | 04 | Dossiers de formation | A. Consigner et surveiller les activités de formation en matière de sécurité de l'information et de protection de la vie privée, y compris la formation sur la sensibilisation à la sécurité et à la protection de la vie privée, et la formation en sécurité et en protection de la vie privée basée sur des rôles spécifiques<br>B. Conserver les dossiers de formation individuels pendant [Affectation : délai défini par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| AT | 05 | Contacts avec les groupes et associations de sécurité | Annulé : Intégré au contrôle PM-15. | s.o. | s.o. | s.o. | s.o. |
| AT | 06 | Rétroaction sur les formations suivies | Fournir une rétroaction sur les résultats de la formation organisationnelle au personnel suivant [Affectation : fréquence définie par l'organisation] : [Affectation : personnel désigné par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| AU | 01 | Politique et procédures de vérification et de responsabilisation | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de vérification et de responsabilisation [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de vérification et de responsabilisation ainsi que des contrôles connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de vérification et de responsabilisation.<br>C. Passer en revue et mettre à jour, par rapport à la vérification et la responsabilisation,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| AU | 02 | Journalisation d'événements | A. Déterminer les types d'événements que le système est en mesure de journaliser pour soutenir la fonction de vérification : [Affectation : types d'événements définis par l'organisation que le système est en mesure de journaliser]<br>B. Coordonner la fonction de journalisation avec d'autres entités organisationnelles qui nécessitent de l'information en matière de vérification afin d'orienter et d'éclairer la sélection des critères pour les événements à journaliser<br>C. Préciser les types d'événements suivants pour la journalisation dans le système [Affectation : types d'événements définis par l'organisation (sous-ensemble de types d'événements défini dans le contrôle AU-02A) et fréquence de journalisation (ou la situation qui la justifie) de chaque type d'événement]<br>D. Expliquer pourquoi les types d'événements sélectionnés pour la journalisation sont jugés adéquats pour soutenir les enquêtes après coup des incidents<br>E. Vérifier et mettre à jour les types d'événements sélectionnés pour la journalisation tous les [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 02(01) | Journalisation d'événements | Journalisation d'événements : Compilation d'enregistrements de vérification provenant de sources multiples<br>Annulé : Intégré au contrôle AU-12. | s.o. | s.o. | s.o. | s.o. |
| AU | 02(02) | Journalisation d'événements | Journalisation d'événements : Sélection d'événements de vérification par composant<br>Annulé : Intégré au contrôle AU-12. | s.o. | s.o. | s.o. | s.o. |
| AU | 02(03) | Journalisation d'événements | Journalisation d'événements : Examens et mises à jour<br>Annulé : Intégré au contrôle AU-02. | s.o. | s.o. | s.o. | s.o. |
| AU | 02(04) | Journalisation d'événements | Journalisation d'événements : Fonctions privilégiées<br>Annulé : Intégré au contrôle AC-06(09). | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AU | 03 | Contenu des enregistrements de vérification | S'assurer que les enregistrements de vérification contiennent l'information nécessaire pour établir<br>A. le type d'événement qui s'est produit<br>B. le moment auquel l'événement s'est produit<br>C. l'endroit où l'événement s'est produit<br>D. la source de l'événement<br>E. le résultat de l'événement<br>F. l'identité des personnes, des sujets, des objets ou des entités associés à l'événement | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 03(01) | Contenu des enregistrements de vérification | Contenu des enregistrements de vérification : Information de vérification supplémentaire<br>Générer des enregistrements de vérification comportant l'information supplémentaire suivante : [Affectation : information supplémentaire définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 03(02) | Contenu des enregistrements de vérification | Contenu des enregistrements de vérification : Gestion centralisée du contenu des enregistrements de vérification<br>Annulé : Intégré au contrôle PL-09. | s.o. | s.o. | s.o. | s.o. |
| AU | 03(03) | Contenu des enregistrements de vérification | Contenu des enregistrements de vérification : Limitation des éléments liés aux renseignements personnels<br>Limiter les renseignements personnels contenus dans les enregistrements de vérification aux éléments suivants identifiés dans l'évaluation des facteurs relatifs à la vie privée : [Affectation : éléments définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 04 | Capacité de stockage des journaux de vérification | Attribuer une capacité de stockage de journaux de vérification en fonction des [Affectation : exigences de conservation des journaux de vérification]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 04(01) | Capacité de stockage des journaux de vérification | Capacité de stockage des journaux de vérification : Transfert vers une capacité de stockage secondaire<br>Transférer les journaux de vérification [Affectation : fréquence définie par l'organisation] à un système, composant du système ou un support différent du système ou du composant du système faisant l'objet de la journalisation. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 05 | Intervention en cas d'échec du processus de journalisation des données de vérification | A. Alerter [Affectation : personnel ou rôles désignés de l'organisation] dans [Affectation : délais définis par l'organisation] en cas d'échec d'un processus de journalisation des données de vérification<br>B. Prendre les mesures supplémentaires suivantes : [Affectation : mesures supplémentaires définies par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 05(01) | Intervention en cas d'échec du processus de journalisation des données de vérification | Intervention en cas d'échec du processus de journalisation des données de vérification : Avertissement de capacité de stockage<br>Avertir [Affectation : personnel, rôles et/ou emplacements définis par l'organisation] dans un délai de [Affectation : délai défini par l'organisation] lorsque le volume de stockage des journaux de vérification attribué aux enregistrements de journaux vérification atteint [Affectation : pourcentage défini par l'organisation] de sa capacité maximale. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 05(02) | Intervention en cas d'échec du | Intervention en cas d'échec du processus de journalisation des données de vérification : Alertes en temps réel<br>Fournir une alerte [Affectation : personnel, rôles et/ou emplacements définis par l'organisation] en [Affectation : délais en | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | processus de journalisation des données de vérification | temps réel définis par l'organisation] lorsque les événements d'échec de vérification suivants se produisent : [Affectation : événements d'échec de journalisation des données de vérification définis par l'organisation qui nécessitent une alerte en temps réel]. | | | | |
| AU | 05(03) | Intervention en cas d'échec du processus de journalisation des données de vérification | Intervention en cas d'échec du processus de journalisation des données de vérification : Seuils de volume de trafic configurables<br>Appliquer des seuils de volume de trafic configurables aux communications réseau, qui représentent les limites de la capacité de vérification et [Sélection (un choix) : rejette; retarde] tout trafic réseau supérieur à ces seuils. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 05(04) | Intervention en cas d'échec du processus de journalisation des données de vérification | Intervention en cas d'échec du processus de journalisation des données de vérification : Interruption en cas d'échec<br>Évoquer une [Sélection (un choix) : interruption complète du système; interruption partielle du système; détérioration des opérations en limitant les fonctions associées à la mission ou aux activités] en cas de [Affectation : échecs de la journalisation des données de vérification définis par l'organisation], sauf s'il existe une capacité de journalisation des données de vérification de substitution. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 05(05) | Intervention en cas d'échec du processus de journalisation des données de vérification | Intervention en cas d'échec du processus de journalisation des données de vérification : Capacité de journalisation des données de vérification secondaire<br>Prévoir une capacité de journalisation des données de vérification secondaire en vue de parer à l'impossibilité d'avoir recours à la capacité de journalisation des données de vérification principale, et de mettre en œuvre [Affectation : autres fonctions de journalisation des données de vérification définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 06 | Examen, analyse et production de rapports liés aux enregistrements de vérification | A. Examiner et analyser les enregistrements de vérification du système tous les [Affectation : fréquence définie par l'organisation] pour déceler toute indication de [Affectation : activités inappropriées ou inhabituelles définies par l'organisation] et les répercussions potentielles d'activités inappropriées ou inhabituelles<br>B. Faire rapport des résultats à [Affectation : personnel ou rôles définis par l'organisation]<br>C. Ajuster le niveau d'examen, d'analyse et de rapports d'enregistrements de vérification dans le système lorsqu'un changement fondé sur des renseignements relatifs au maintien de l'ordre, du renseignement brut ou d'autres sources crédibles d'information est apporté au risque | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 06(01) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Intégration de processus automatisés<br>Intégrer des processus d'examen, d'analyse et de production de rapports liés aux enregistrements de vérification au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 06(02) | Examen, analyse et production de rapports liés | Examen, analyse et production de rapports liés aux enregistrements de vérification : Alertes de sécurité automatisées<br>Annulé : Intégré au contrôle SI-04. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | aux enregistrements de vérification | | | | | |
| AU | 06(03) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Correspondance des référentiels pour les enregistrements de vérification<br>Analyser et mettre en correspondance les enregistrements de vérification provenant de différents référentiels afin d'établir une connaissance de la situation à l'échelle de l'organisation. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 06(04) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Analyses et examens centralisés<br>Fournir et mettre en œuvre la capacité de centraliser les examens et les analyses des enregistrements de vérification provenant de plusieurs composants du système. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 06(05) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Analyse intégrée des enregistrements de vérification<br>Intégrer l'analyse des enregistrements de vérification et l'analyse de [Sélection (un choix ou plus) : l'information liée au balayage des vulnérabilités; les données de rendement; l'information sur la surveillance du système d'information; [Affectation : données ou information recueillies par d'autres sources définies par l'organisation]] pour accroître sa capacité de détecter les activités inappropriées ou inhabituelles. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 06(06) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Corrélation avec la surveillance physique<br>Mettre en corrélation l'information des enregistrements de vérification avec celle obtenue lors de la surveillance de l'accès physique pour accroître la capacité d'identification des activités suspectes, inappropriées, inhabituelles ou malveillantes. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 06(07) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Opérations autorisées<br>Préciser les opérations qui sont autorisées concernant chaque [Sélection (un choix ou plus) : processus de système; rôle; utilisateur] associé à l'examen, à l'analyse et aux rapports de l'information de vérification. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 06(08) | Examen, analyse et | Examen, analyse et production de rapports liés aux enregistrements de vérification : Analyse plein texte des commandes privilégiées | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | production de rapports liés aux enregistrements de vérification | Mener une analyse plein texte des commandes privilégiées enregistrées dans un composant de système ou un sous-système physiquement distinct du système ou dans un autre système conçu pour mener cette analyse. | | | | |
| AU | 06(09) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Corrélation avec l'information provenant de sources non techniques<br>Mettre en corrélation l'information provenant de sources non techniques et l'information d'enregistrement de vérification afin d'acquérir une connaissance globale de sa situation. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 06(10) | Examen, analyse et production de rapports liés aux enregistrements de vérification | Examen, analyse et production de rapports liés aux enregistrements de vérification : Ajustement du niveau d'examen<br>Annulé : Intégré au contrôle AU-06. | s.o. | s.o. | s.o. | s.o. |
| AU | 07 | Réduction des enregistrements de vérification et génération de rapports | Fournir et mettre en œuvre une capacité de réduction des enregistrements de vérification et de génération de rapports qui<br>A. prend en charge les exigences en matière d'examen, d'analyse et de production de rapports liés aux enregistrements de vérification sur demande et les enquêtes après coup sur les incidents<br>B. ne change pas le contenu original ni le classement chronologique des enregistrements de vérification | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 07(01) | Réduction des enregistrements de vérification et génération de rapports | Réduction des enregistrements de vérification et génération de rapports : Traitement automatique<br>Permettre et mettre en œuvre le tri et la recherche des enregistrements de vérification liés à des événements d'intérêt selon le contenu suivant : [Affectation : champs d'enregistrements de vérification définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 07(02) | Réduction des enregistrements de vérification et génération de rapports | Réduction des enregistrements de vérification et génération de rapports : Triage et recherche automatisés<br>Annulé : Intégré au contrôle AU-07(01). | s.o. | s.o. | s.o. | s.o. |
| AU | 08 | Horodatage | A. Utiliser les horloges internes du système pour horodater les enregistrements de vérification<br>B. Consigner l'horodatage des enregistrements de vérification correspondant à [Affectation : granularité de mesure du temps définie par l'organisation] et utilisant le temps universel coordonné (UTC), un décalage fixe par rapport à l'UTC correspondant à l'heure locale, ou encore en incluant le décalage local dans les données d'horodatage | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 08(01) | Horodatage | Horodatage : Synchronisé avec une source de temps faisant autorité | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | Annulé : Transféré sous le contrôle SC-45(01). | | | | |
| AU | 08(02) | Horodatage | Horodatage : Deuxième source de temps qui fait autorité<br>Annulé : Transféré sous le contrôle SC-45(02). | s.o. | s.o. | s.o. | s.o. |
| AU | 09 | Protection de l'information de vérification | A. Protéger l'information de vérification et les outils de journalisation des données de vérification contre les accès non autorisés, les modifications et les suppressions<br>B. Alerter [Affectation : personnel ou rôles définis par l'organisation] advenant la détection d'une modification ou d'une suppression non autorisée de l'information de vérification, ou d'un accès non autorisé à celle-ci | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 09(01) | Protection de l'information de vérification | Protection de l'information de vérification : Supports matériels non réinscriptibles<br>Consigner les enregistrements de vérification sur des supports matériels non réinscriptibles. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 09(02) | Protection de l'information de vérification | Protection de l'information de vérification : Stockage sur des systèmes ou des composants physiques séparés<br>Stocker les enregistrements de vérification [Affectation : fréquence définie par l'organisation] dans un référentiel faisant partie d'un système ou d'un composant de système qui est physiquement différent du système ou du composant faisant l'objet de la vérification. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 09(03) | Protection de l'information de vérification | Protection de l'information de vérification : Protection cryptographique<br>Utiliser des mécanismes cryptographiques pour protéger l'intégrité de l'information de vérification et des outils de vérification. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 09(04) | Protection de l'information de vérification | Protection de l'information de vérification : Accès par un sous-ensemble d'utilisateurs privilégiés<br>Autoriser l'accès pour la gestion de la fonctionnalité de journalisation des données de vérification uniquement à [Affectation : sous-ensemble d'utilisatrices et utilisateurs ou de rôles privilégiés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 09(05) | Protection de l'information de vérification | Protection de l'information de vérification : Double autorisation<br>Appliquer le principe de double autorisation pour [Sélection (un choix ou plus) : déplacement; suppression] de [Affectation : information de vérification définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 09(06) | Protection de l'information de vérification | Protection de l'information de vérification : Accès en lecture seule<br>Autoriser l'accès en lecture seule pour l'information de vérification à [Affectation : sous-ensemble d'utilisatrices et utilisateurs ou de rôles privilégiés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 09(07) | Protection de l'information de vérification | Protection de l'information de vérification : Stockage sur composant avec un système d'exploitation différent<br>Stocker de l'information de vérification sur un composant exécutant un système d'exploitation différent du système ou du composant faisant l'objet de la vérification. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 10 | Non-répudiation | Fournir une preuve irréfutable qu'une personne (ou un processus exécuté en son nom) a effectué [Affectation : opérations de non-répudiation définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 10(01) | Non-répudiation | Non-répudiation : Association avec les identités<br>a. Associer l'identité de l'auteure ou auteur d'une information avec l'information de [Affectation : robustesse du lien définie par l'organisation]<br>b. Permettre aux personnes autorisées de déterminer l'identité de l'auteure ou auteur de l'information | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AU | 10(02) | Non-répudiation | Non-répudiation : Validité du lien avec l'identité de l'auteure ou auteur de l'information<br>a. Valider le lien entre l'identité de l'auteure ou auteur de l'information et l'information [Affectation : fréquence définie par l'organisation]<br>b. Effectuer [Affectation : opérations définies par l'organisation] en cas d'erreur de validation | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 10(03) | Non-répudiation | Non-répudiation : Chaîne de possession<br>Conserver, dans la chaîne de possession établie, l'identité et les justificatifs d'identité de l'examinatrice ou examinateur ou de l'émettrice ou émetteur pour l'information examinée ou diffusée. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 10(04) | Non-répudiation | Non-répudiation : Validité du lien avec l'identité de l'examinatrice ou examinateur de l'information<br>a. Valider le lien entre l'identité de l'examinatrice ou examinateur et l'information au point de transfert ou de diffusion, avant que l'information ne soit transférée ou diffusée [Affectation : d'un domaine de sécurité à un autre définis par l'organisation]<br>b. Effectuer [Affectation : opérations définies par l'organisation] en cas d'erreur de validation | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 10(05) | Non-répudiation | Non-répudiation : Signatures numériques<br>Annulé : Intégré au contrôle SI-07. | s.o. | s.o. | s.o. | s.o. |
| AU | 11 | Conservation des enregistrements de vérification | Conserver les enregistrements de vérification pendant [Affectation : délais définis par l'organisation et conformément à la stratégie de conservation des dossiers] pour appuyer les enquêtes après coup sur les incidents et satisfaire aux exigences réglementaires et organisationnelles de conservation de l'information. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 11(01) | Conservation des enregistrements de vérification | Conservation des enregistrements de vérification : Capacité de récupération à long terme<br>Recourir à [Affectation : mesures définies par l'organisation] pour s'assurer que les enregistrements de vérification à long terme que génère le système sont récupérables. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 12 | Génération d'enregistrements de vérification | A. Fournir une capacité de génération d'enregistrements de vérification pour les types d'événements que le système est en mesure de vérifier conformément au contrôle AU-02A sur [Affectation : composants du système désignés par l'organisation]<br>B. Permettre à [Affectation : personnel ou rôles définis par l'organisation] de sélectionner les types d'événements qui doivent être journalisés par des composants de système particuliers<br>C. Générer des enregistrements de vérification pour les types d'événements définis au contrôle AU-02C dont le contenu des enregistrements de vérification est défini au contrôle AU-03 | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 12(01) | Génération d'enregistrements de vérification | Génération d'enregistrements de vérification : Piste de vérification à l'échelle du système et corrélée dans le temps<br>Compiler les enregistrements de vérification provenant de [Affectation : composants du système définis par l'organisation] en une piste de vérification (logique ou physique) globale qui est corrélée dans le temps, en-dedans de [Affectation : niveau de tolérance défini par l'organisation pour les relations entre les estampilles temporelles des enregistrements individuels de la piste de vérification]. | Contrôle | Sélectionné | s.o. | s.o. |
| AU | 12(02) | Génération d'enregistrements | Génération d'enregistrements de vérification : Formats normalisés<br>Produire une piste de vérification (logique ou physique) globale composée d'enregistrements de vérification dans un format normalisé. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | ts de vérification | | | | | |
| AU | 12(03) | Génération d'enregistrements de vérification | Génération d'enregistrements de vérification : Modifications par des personnes autorisées<br>Permettre et mettre en œuvre à [Affectation : liste des personnes ou des rôles définie par l'organisation] de modifier la journalisation à effectuer sur [Affectation : composants de système définis par l'organisation] en fonction de [Affectation : critères d'événement sélectionnables définis par l'organisation] dans un délai de [Affectation : délai défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 12(04) | Génération d'enregistrements de vérification | Génération d'enregistrements de vérification : Vérifications des paramètres d'interrogation des renseignements personnels<br>Fournir et mettre en œuvre la capacité de vérifier les paramètres des événements d'interrogation d'utilisatrices et utilisateurs pour des jeux de données comportant des renseignements personnels. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 13 | Surveillance de la divulgation d'information | A. Surveiller [Affectation : sites d'information ou sites d'information de source ouverte définis par l'organisation] [Affectation : fréquence définie par l'organisation] pour veiller à ce qu'il n'y ait aucune divulgation non autorisée d'information liée à l'organisation<br>B. Si une divulgation d'information est découverte<br>1. informer [Affectation : personnel ou rôles définis par l'organisation]<br>2. prendre les mesures supplémentaires suivantes : [Affectation : mesures supplémentaires définies par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 13(01) | Surveillance de la divulgation d'information | Surveillance de la divulgation d'information : Utilisation d'outils automatisés<br>Surveiller des sites d'information de source ouverte ou des sites d'information au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 13(02) | Surveillance de la divulgation d'information | Surveillance de la divulgation d'information : Examen des sites surveillés<br>Examiner la liste des sites d'information de source ouverte faisant l'objet d'une surveillance [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 13(03) | Surveillance de la divulgation d'information | Surveillance de la divulgation d'information : Duplication non autorisée d'information<br>Employer des techniques, des processus et des outils de découverte pour déterminer si des entités externes reproduisent l'information de l'organisation de façon non autorisée. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 14 | Vérification des sessions | A. Permettre et mettre en œuvre la capacité pour les [Affectation : utilisatrices et utilisateurs ou rôles définis par l'organisation] de [Sélection (un choix ou plus) : enregistrer; afficher; écouter; journaliser] le contenu d'une session d'utilisatrice ou utilisateur pour des [Affectation : circonstances définies par l'organisation]<br>B. Mettre au point, intégrer et utiliser les activités de vérification des sessions après consultation avec des conseillères et conseillers juridiques, conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 14(01) | Vérification des sessions | Vérification des sessions : Démarrage du système<br>Lancer la vérification des sessions automatiquement au démarrage du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 14(02) | Vérification des sessions | Vérification des sessions : Contenu de la saisie et de l'enregistrement<br>Annulé : Intégré au contrôle AU-14. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AU | 14(03) | Vérification des sessions | Vérification des sessions : Visualisation et écoute à distance<br>Fournir et mettre en œuvre la capacité qui permet aux utilisatrices et utilisateurs autorisés de visualiser ou d'écouter à distance et en temps réel tout le contenu d'une session utilisateur établie. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 15 | Capacité de journalisation des données de vérification secondaire | Annulé : Transféré sous le contrôle AU-05(05). | s.o. | s.o. | s.o. | s.o. |
| AU | 16 | Journalisation des données de vérification transorganisationnelle | Utiliser [Affectation : méthodes définies par l'organisation] pour coordonner [Affectation : information de contrôle définie par l'organisation] avec d'autres organisations lorsque l'information de contrôle est transmise au-delà des frontières organisationnelles. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 16(01) | Journalisation des données de vérification transorganisationnelle | Journalisation des données de vérification transorganisationnelle : Préservation de l'identité<br>Préserver l'identité des personnes dans des pistes de vérification transorganisationnelles. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 16(02) | Journalisation des données de vérification transorganisationnelle | Journalisation des données de vérification transorganisationnelle : Échange d'information de vérification<br>Fournir de l'information de vérification trans-organisationnelle aux [Affectation : organisations définies par l'organisation] en vertu des [Affectation : accords liés à l'échange transorganisationnel définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| AU | 16(03) | Journalisation des données de vérification transorganisationnelle | Journalisation des données de vérification transorganisationnelle : Dissociabilité<br>Mettre en œuvre des [Affectation : mesures définies par l'organisation] pour dissocier des individus de l'information de vérification transmise au-delà des frontières organisationnelles. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| CA | 01 | Politique et procédures d'évaluation, | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique d'évaluation, d'autorisation et de surveillance [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | d'autorisation et de surveillance | organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique d'évaluation, d'autorisation et de surveillance ainsi que des contrôles de surveillance connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'évaluation d'autorisation et de surveillance<br>C. Passer en revue et mettre à jour, par rapport à l'évaluation, l'autorisation et la surveillance,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | | | | |
| CA | 02 | Évaluations de contrôle | A. Sélectionner l'évaluatrice ou évaluateur ou l'équipe d'évaluation qui convient pour le type d'évaluation à effectuer<br>B. Élaborer un plan d'évaluations de contrôle qui décrit la portée de l'évaluation, y compris<br>1. les contrôles et les améliorations de contrôle faisant l'objet d'une évaluation<br>2. les procédures d'évaluation à utiliser pour déterminer l'efficacité des contrôles<br>3. l'environnement d'évaluation, l'équipe d'évaluation et les rôles et responsabilités liés à l'évaluation<br>C. S'assurer que le plan d'évaluation des contrôles est examiné et approuvé par l'autorité responsable ou une représentante ou un représentant désigné avant d'effectuer l'évaluation<br>D. Évaluer les contrôles du système et l'environnement dans lequel il est exploité [Affectation : fréquence définie par l'organisation] pour déterminer dans quelle mesure les contrôles ont été mis en œuvre correctement, s'ils fonctionnent comme prévu et s'ils produisent les résultats escomptés tout en respectant les exigences relatives à la sécurité et à la protection de la vie privée<br>E. Produire un rapport d'évaluation de contrôle, une évaluation des facteurs relatifs à la vie privée ou un protocole de protection de la vie privée qui documente les résultats de l'évaluation<br>F. Remettre les résultats de l'évaluation des contrôles à [Affectation : personnel et rôles définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| CA | 02(01) | Évaluations de contrôle | Évaluations de contrôle : Évaluatrices et évaluateurs indépendants<br>Utiliser des évaluatrices et évaluateurs ou des équipes d'évaluatrices et évaluateurs indépendants pour mener des évaluations de contrôle. | Activité | Sélectionné | s.o. | s.o. |
| CA | 02(02) | Évaluations de contrôle | Évaluations de contrôle : Évaluations spécialisées<br>Comprendre dans le cadre des évaluations de contrôle, [Affectation : fréquence définie par l'organisation], [Sélection (un choix) : annoncé; non annoncé], [Sélection (un choix ou plus) : une surveillance approfondie; une instrumentation de sécurité; des cas de tests de sécurité automatisés; une analyse des vulnérabilités; des tests liés aux utilisatrices et utilisateurs malveillants; une évaluation des menaces internes; des tests de charge et de performance; une évaluation des fuites de données ou des pertes de données; [Affectation : autres formes d'évaluation de sécurité définies par l'organisation]]. | Activité | Non sélectionné | s.o. | s.o. |
| CA | 02(03) | Évaluations de contrôle | Évaluations de contrôle : Tirer parti des résultats d'évaluation provenant d'organisations externes<br>Tirer parti des résultats des évaluations de contrôle menées par [Affectation : organisation externe désignée par l'organisation] sur le [Affectation : système désigné par l'organisation] lorsque l'évaluation respecte [Affectation : exigences définies par l'organisation]. | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CA | 03 | Échange d'information | A. Approuver et gérer l'échange d'information entre le système et d'autres systèmes au moyen de [Sélection (un choix ou plus) : ententes sur la sécurité des interconnexions; ententes sur la sécurité de l'échange d'information; ententes ou protocoles d'entente; accords d'échange de renseignements; ententes d'échange de renseignements; accords sur les niveaux de service; ententes avec les utilisatrices et utilisateurs; accords de non-divulgation; [Affectation : type d'entente défini par l'organisation]]<br>B. Consigner, dans le cadre des ententes d'échange, les caractéristiques d'interface, les exigences de sécurité et de protection de la vie privée ainsi que les responsabilités liées à chacun des systèmes, et le niveau d'incidence de l'information communiquée<br>C. Examiner et tenir à jour les ententes [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CA | 03(01) | Échange d'information | Échange d'information : Connexions à des systèmes de sécurité nationaux non classifiés<br>Annulé : Transféré sous le contrôle SC-07(25). | s.o. | s.o. | s.o. | s.o. |
| CA | 03(02) | Échange d'information | Échange d'information : Connexions à des systèmes de sécurité nationaux classifiés<br>Annulé : Transféré sous le contrôle SC-07(26). | s.o. | s.o. | s.o. | s.o. |
| CA | 03(03) | Échange d'information | Échange d'information : Connexions à des systèmes de sécurité non nationaux non classifiés<br>Annulé : Transféré sous le contrôle SC-07(27). | s.o. | s.o. | s.o. | s.o. |
| CA | 03(04) | Échange d'information | Échange d'information : Connexions aux réseaux publics<br>Annulé : Transféré sous le contrôle SC-07(28). | s.o. | s.o. | s.o. | s.o. |
| CA | 03(05) | Échange d'information | Échange d'information : Connexions restreintes à des systèmes externes<br>Annulé : Transféré sous le contrôle SC-07(05). | s.o. | s.o. | s.o. | s.o. |
| CA | 03(06) | Échange d'information | Échange d'information : Autorisations de transfert<br>Vérifier que les personnes ou les systèmes qui transfèrent des données entre des systèmes interconnectés ont les autorisations nécessaires (c'est-à-dire des autorisations écrites ou privilégiées) avant d'accepter de telles données. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 03(07) | Échange d'information | Échange d'information : Échanges d'information éphémère<br>a. Identifier les échanges d'information éphémères (en aval) avec d'autres systèmes par le biais des systèmes identifiés au contrôle CA-03A<br>b. Prendre les mesures nécessaires pour assurer que les échanges d'information éphémères (en aval) cessent lorsqu'il devient impossible de vérifier ou de valider les contrôles sur des systèmes (en aval) éphémères | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 04 | Certification de sécurité | Annulé : Intégré au contrôle CA-02. | s.o. | s.o. | s.o. | s.o. |
| CA | 05 | Plans d'action et des jalons | A. Développer un plan d'action et des jalons pour le système afin de consigner les mesures correctives de l'organisation pour corriger les faiblesses ou les lacunes relevées durant l'évaluation des contrôles et pour réduire et éliminer les vulnérabilités connues du système<br>B. Mettre à jour le plan d'action et les jalons existants [Affectation : fréquence définie par l'organisation] en tenant compte des constatations des évaluations de contrôles, des vérifications ou des examens indépendants et des activités de surveillance continue | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CA | 05(01) | Plans d'action et des jalons | Plans d'action et des jalons : Automatisation du soutien aux fins d'exactitude et d'actualité<br>Assurer l'exactitude, l'actualité et la disponibilité du plan d'action et des jalons pour le système se servant de [Affectation : mécanismes automatisés définis par l'organisation]. | Activité | Non sélectionné | s.o. | s.o. |
| CA | 06 | Autorisation | A. Attribuer à une cadre supérieure ou un cadre supérieur le rôle d'autorité responsable ou de gardienne ou gardien du système<br>B. Attribuer à une cadre supérieure ou un cadre supérieur le rôle d'autorité responsable ou de gardienne ou gardien des contrôles courants pouvant être hérités par les systèmes organisationnels<br>C. S'assurer que l'autorité responsable ou la gardienne ou le gardien du système, avant de débuter les opérations<br>1. accepte l'utilisation de contrôles communs hérités par le système<br>2. autorise l'exploitation du système<br>D. S'assurer que l'autorité responsable ou la gardienne ou le gardien des contrôles communs autorise l'utilisation de ces contrôles pour que les systèmes organisationnels en héritent<br>E. Mettre à jour les autorisations [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CA | 06(01) | Autorisation | Autorisation : Autorisation conjointe (au sein de l'organisation)<br>Faire appel à un processus d'autorisation conjointe pour le système qui comprend plusieurs autorités responsables de la même organisation menant le processus d'autorisation. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 06(02) | Autorisation | Autorisation : Autorisation conjointe (interorganisation)<br>Faire appel à un processus d'autorisation conjointe pour le système qui comprend plusieurs autorités responsables avec au moins une ou un responsable de l'autorisation provenant d'une organisation à l'extérieur de l'organisation menant le processus d'autorisation. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 07 | Surveillance continue | Élaborer et mettre en œuvre une stratégie de surveillance continue des systèmes conformément à la stratégie de surveillance continue de l'organisation qui comprend<br>A. Établir les mesures au niveau du système à surveiller pour : [Affectation : mesures au niveau du système définies par l'organisation]<br>B. la mise en place d'activités de surveillance [Affectation : fréquences définies par l'organisation] et [Affectation : fréquences définies par l'organisation] pour l'évaluation de l'efficacité des contrôles<br>C. les évaluations de contrôle de sécurité permanentes conformément aux stratégies de surveillance continue<br>D. la surveillance en permanence des mesures, conformément à la stratégie de surveillance continue définie par l'organisation<br>E. la corrélation et l'analyse de l'information générée par les évaluations de contrôle et la surveillance<br>F. les mesures d'intervention concernant les résultats qui découlent de l'analyse de l'information<br>G. le signalement de l'état de la sécurité et de la protection de la vie privée du système à la ou au [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CA | 07(01) | Surveillance continue | Surveillance continue : Évaluation indépendante<br>Faire appel à des évaluatrices et évaluateurs indépendants ou à des équipes d'évaluation pour surveiller en permanence les contrôles du système. | Contrôle | Sélectionné | s.o. | s.o. |
| CA | 07(02) | Surveillance continue | Surveillance continue : Types d'évaluations<br>Annulé : Intégré au contrôle CA-02. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CA | 07(03) | Surveillance continue | Surveillance continue : Analyses des tendances<br>Utiliser des analyses de tendances pour déterminer s'il faut modifier les mises en œuvre de contrôles, la fréquence des activités de surveillance continue ou tout autre type d'activités utilisées dans le cadre du processus de surveillance continue, en se basant sur des données empiriques. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 07(04) | Surveillance continue | Surveillance continue : Surveillance des risques<br>S'assurer que la surveillance des risques fait partie intégrante de la stratégie de surveillance continue qui comprend ce qui suit<br>a. la surveillance de l'efficacité<br>b. la surveillance de la conformité<br>c. la surveillance des changements | Contrôle | Sélectionné | s.o. | s.o. |
| CA | 07(05) | Surveillance continue | Surveillance continue : Analyse de la cohérence<br>Utiliser les mesures suivantes pour valider que les stratégies sont établies et que les contrôles mis en œuvre sont fonctionnels de façon uniforme : [Affectation : actions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 07(06) | Surveillance continue | Surveillance continue : Soutien automatisé pour la surveillance<br>Assurer l'exactitude, l'actualité et la disponibilité des résultats de surveillance pour le système en se servant de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 08 | Tests d'intrusion | Effectuer des tests d'intrusion [Affectation : fréquence définie par l'organisation] sur [Affectation : systèmes ou composants de systèmes définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 08(01) | Tests d'intrusion | Tests d'intrusion : Équipe, agente ou agent indépendant chargé des tests d'intrusion<br>Faire appel à une équipe, agente ou agent indépendant chargé des tests d'intrusion pour effectuer des tests d'intrusion sur le système ou les composants du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 08(02) | Tests d'intrusion | Tests d'intrusion : Exercices effectués par l'équipe de testeuses et testeurs<br>Avoir recours à des exercices effectués par l'équipe de testeuses et testeurs pour simuler des tentatives de compromission des systèmes organisationnels lancées par des adversaires conformément aux règles d'engagement : [Affectation : exercices effectués par l'équipe de testeuses et testeurs définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 08(03) | Tests d'intrusion | Tests d'intrusion : Tests d'intrusion des installations<br>Utiliser un processus de tests d'intrusion qui comprend [Affectation : fréquence définie par l'organisation] tentatives [Sélection (un choix ou plus) : prévues; inopinées] de contournement des contrôles associés aux points d'accès physique de l'installation. | Contrôle | Non sélectionné | s.o. | s.o. |
| CA | 09 | Connexions des systèmes internes | A. Autoriser les connexions internes de [Affectation : composants de système ou types de composants définis par l'organisation] au système<br>B. Consigner, pour chaque connexion interne, les caractéristiques d'interface, les exigences de sécurité et de protection de la vie privée, et la nature de l'information communiquée<br>C. Interrompre les connexions des systèmes internes après [Affectation : modalités définies par l'organisation]<br>D. Examiner [Affectation : fréquence définie par l'organisation] la nécessité de chaque connexion interne | Contrôle | Sélectionné | s.o. | s.o. |
| CA | 09(01) | Connexions des systèmes internes | Connexions des systèmes internes : Vérifications de la conformité<br>Vérifier la conformité des composants aux exigences de sécurité avant d'établir une connexion interne. | Contrôle | Sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| CM | 01 | Politique et procédures de gestion des configurations | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de gestion des configurations [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre des politiques de gestion des configurations et des contrôles de gestion des configurations connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la gestion des configurations<br>C. Passer en revue et mettre à jour, par rapport à la gestion des configurations,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| CM | 02 | Configuration de référence | A. Élaborer, consigner et tenir à jour, dans le cadre du contrôle des configurations, une configuration de référence du système<br>B. Passer en revue et mettre à jour la configuration de référence du système<br>1. [Affectation : fréquence définie par l'organisation]<br>2. le cas échéant, selon [Affectation : circonstances définies par l'organisation]<br>3. lorsque des composants du système sont installés ou modifiés | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 02(01) | Configuration de référence | Configuration de référence : Examens et mises à jour<br>Annulé : Intégré au contrôle CM-02. | s.o. | s.o. | s.o. | s.o. |
| CM | 02(02) | Configuration de référence | Configuration de référence : Automatisation du soutien aux fins d'exactitude et d'actualité<br>Assurer l'actualité, le caractère exhaustif, l'exactitude et la disponibilité de la configuration de références pour le système en se servant de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 02(03) | Configuration de référence | Configuration de référence : Conservation des configurations antérieures<br>Conserver [Affectation : nombre défini par l'organisation] versions de configurations de référence antérieures du système pour permettre le retour à la version précédente. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 02(04) | Configuration de référence | Configuration de référence : Logiciels non autorisés<br>Annulé : Intégré au contrôle CM-07(04). | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CM | 02(05) | Configuration de référence | Configuration de référence : Logiciels autorisés<br>Annulé : Intégré au contrôle CM-07(05). | s.o. | s.o. | s.o. | s.o. |
| CM | 02(06) | Configuration de référence | Configuration de référence : Environnements de test et de développement<br>Conserver pour les environnements de développement et de tests des systèmes une configuration de référence gérée séparément de la configuration de référence opérationnelle. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 02(07) | Configuration de référence | Configuration de référence : Configuration des systèmes et des composants pour des zones à risque élevé<br>a. Remettre [Affectation : systèmes, composants de système désignés par l'organisation] dotés de [Affectation : configurations définies par l'organisation] aux personnes qui se rendent dans des endroits que l'organisation juge très risqués<br>b. Appliquer les contrôles suivants aux systèmes ou aux composants de systèmes lorsque les personnes reviennent de voyage : [Affectation : contrôles définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 03 | Contrôle des changements de configuration | A. Déterminer et consigner les types de changements apportés au système qui sont contrôlés par la configuration<br>B. Examiner les changements proposés au système qui sont contrôlés par la configuration et les approuver ou les refuser en tenant compte explicitement des répercussions sur la sécurité et la protection de la vie privée<br>C. Consigner les décisions liées aux changements de configuration du système<br>D. Mettre en œuvre les changements approuvés au système qui sont contrôlés par la configuration<br>E. Conserver les dossiers sur les changements contrôlés par la configuration du système pendant [Affectation : délais définis par l'organisation]<br>F. Surveiller et examiner les activités associées aux changements contrôlés par la configuration visant le système<br>G. Coordonner et surveiller les activités de contrôle des changements de configuration effectuées par [Affectation : élément de contrôle des changements de configuration défini par l'organisation] qui se réunit [Sélection : (un choix ou plus) : [Affectation : fréquence définie par l'organisation]; lorsque [Affectation : conditions de changement de configuration définies par l'organisation]] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 03(01) | Contrôle des changements de configuration | Contrôle des changements de configuration : Automatisation concernant la documentation, les avis et les interdictions de changements<br>Utiliser des [Affectation : mécanismes automatisés définis par l'organisation] pour<br>a. consigner les changements proposés au système<br>b. aviser [Affectation : autorités d'approbation définies par l'organisation] des changements proposés au système et des demandes de changement approuvées<br>c. souligner les changements proposés au système qui n'ont pas été approuvés ou qui ont été jugés défavorables avant [Affectation : délais définis par l'organisation]<br>d. interdire tout changement au système jusqu'à l'obtention des approbations requises<br>e. documenter tous les changements proposés au système<br>f. aviser [Affectation : liste des employées et employés définie par l'organisation] des changements au système approuvés | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 03(02) | Contrôle des changements de configuration | Contrôle des changements de configuration : Tests, validation et documentation des changements<br>Tester, valider et consigner les changements au système avant de les mettre en œuvre dans le système. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CM | 03(03) | Contrôle des changements de configuration | Contrôle des changements de configuration : Mise en œuvre automatisée des changements<br>Apporter des changements au système de référence actuel et les déployer ensuite dans tout le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 03(04) | Contrôle des changements de configuration | Contrôle des changements de configuration : Représentantes et représentants de la sécurité et de la protection de la vie privée<br>Exiger [Affectation : qu'une représentante ou un représentant de la sécurité et de la protection de la vie privée défini par l'organisation] soit membre de [Affectation : élément de contrôle des changements de configuration défini par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 03(05) | Contrôle des changements de configuration | Contrôle des changements de configuration : Mesures de sécurité automatisées<br>Mettre automatiquement en place les mesures de sécurité suivantes lorsque des configurations de référence sont modifiées sans autorisation : [Affectation : mesures de sécurité définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 03(06) | Contrôle des changements de configuration | Contrôle des changements de configuration : Gestion de la cryptographie<br>S'assurer que les mécanismes cryptographiques utilisés pour fournir les contrôles suivants soient intégrés à la gestion des configurations : [Affectation : contrôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 03(07) | Contrôle des changements de configuration | Contrôle des changements de configuration : Examen des changements apportés au système<br>Passer en revue les changements apportés au système [Affectation : fréquence définie par l'organisation] et [Affectation : circonstances définies par l'organisation] pour déterminer si des changements non autorisés ont été apportés. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 03(08) | Contrôle des changements de configuration | Contrôle des changements de configuration : Empêcher ou limiter les changements de configuration<br>Empêcher ou limiter les changements à la configuration du système dans les situations suivantes : [Affectation : circonstances définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 04 | Analyses des répercussions | Analyser les changements visant le système pour déterminer les répercussions possibles sur la sécurité et la protection de la vie privée avant leur mise en œuvre. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 04(01) | Analyses des répercussions | Analyses des répercussions : Environnements de test distincts<br>Analyser les changements apportés au système dans un environnement de test distinct avant de les appliquer dans un environnement opérationnel afin de déceler toute lacune, faiblesse, incompatibilité ou intention malveillante susceptible d'influer sur la sécurité et la protection de la vie privée. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 04(02) | Analyses des répercussions | Analyses des répercussions : Vérification des contrôles<br>Après les changements apportés au système, s'assurer que les contrôles ont été mis en œuvre correctement, qu'ils fonctionnent comme prévu et qu'ils produisent les résultats escomptés tout en respectant les exigences relatives à la sécurité et à la protection de la vie privée du système. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 05 | Restrictions d'accès associées aux changements | Définir, documenter, approuver et appliquer les restrictions d'accès physiques et logiques associées aux changements apportés au système. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CM | 05(01) | Restrictions d'accès associées aux changements | Restrictions d'accès associées aux changements : Enregistrements de vérification et d'application des restrictions d'accès automatisées<br>a. Appliquer des [Affectation : mécanismes automatisés définis par l'organisation]<br>B. Générer automatiquement des enregistrements de vérification des mesures appliquées | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 05(02) | Restrictions d'accès associées aux changements | Restrictions d'accès associées aux changements : Examen des changements apportés au système<br>Annulé : Intégré au contrôle CM-03(07). | Contrôle | s.o. | s.o. | s.o. |
| CM | 05(03) | Restrictions d'accès associées aux changements | Restrictions d'accès associées aux changements : Composants signés<br>Annulé : Transféré sous le contrôle CM-14. | s.o. | s.o. | s.o. | s.o. |
| CM | 05(04) | Restrictions d'accès associées aux changements | Restrictions d'accès associées aux changements : Double autorisation<br>Appliquer le principe d'autorisation double avant d'apporter des changements à [Affectation : information système et composants du système définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 05(05) | Restrictions d'accès associées aux changements | Restrictions d'accès associés aux changements : Limite des privilèges pour la production et l'opération<br>a. Limiter les privilèges relatifs à la modification des composants du système ainsi que de l'information relative au système dans un environnement opérationnel ou de production<br>b. Examiner et réévaluer les privilèges [Affectation : fréquence définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 05(06) | Restrictions d'accès associées aux changements | Restrictions d'accès associés aux changements : Privilèges de bibliothèque limités<br>Limiter les privilèges permettant de changer les logiciels résidants de la bibliothèque de logiciels. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 05(07) | Restrictions d'accès associées aux changements | Restrictions d'accès associés aux changements : Automatisation de la mise en œuvre de mécanismes de sécurité<br>Annulé : Intégré au contrôle SI-07. | s.o. | s.o. | s.o. | s.o. |
| CM | 06 | Paramètres de configuration | A. Établir et documenter les paramètres de configuration des composants employés dans le système qui cadrent avec le mode le plus rigoureux sur le plan des exigences opérationnelles à l'aide de [Affectation : configurations sécurisées communes définies par l'organisation]<br>B. Mettre en œuvre les paramètres de configuration<br>C. Déterminer, documenter et approuver tout écart en ce qui a trait aux paramètres de configuration établis pour [Affectation : composants de système définis par l'organisation] en tenant compte de [Affectation : exigences opérationnelles définies par l'organisation]<br>D. Surveiller et contrôler les changements apportés aux paramètres de configuration conformément à ses stratégies et procédures | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CM | 06(01) | Paramètres de configuration | Paramètres de configuration : Gestion, application et vérification automatisées<br>Gérer, appliquer et vérifier les paramètres de configuration pour [Affectation : composants de systèmes définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 06(02) | Paramètres de configuration | Paramètres de configuration : Intervention lorsque des changements non autorisés sont apportés<br>Prendre les mesures suivantes pour intervenir lorsque des changements non autorisés sont apportés aux [Affectation : paramètres de configuration définis par l'organisation] : [Affectation : actions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 06(03) | Paramètres de configuration | Paramètres de configuration : Détection de changement non autorisé<br>Annulé : Intégré au contrôle SI-07. | s.o. | s.o. | s.o. | s.o. |
| CM | 06(04) | Paramètres de configuration | Paramètres de configuration : Démonstration de conformité<br>Annulé : Intégré au contrôle CM-04. | s.o. | s.o. | s.o. | s.o. |
| CM | 07 | Fonctionnalité minimale | A. Configurer le système pour fournir uniquement des [Affectations : capacités essentielles à la mission définies par l'organisation]<br>B. Interdire ou restreindre l'utilisation des fonctions, des ports, des protocoles, des logiciels et des services suivants : [Affectation : fonctions, ports, protocoles, logiciels ou services du système interdits ou restreints définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 07(01) | Fonctionnalité minimale | Fonctionnalité minimale : Examen périodique<br>a. Examiner le système tous les [Affectation : fréquence définie par l'organisation] afin d'établir les fonctions, les ports, les protocoles, les logiciels et les services non nécessaires<br>b. Désactiver ou retirer [Affectation : fonctions, ports, protocoles et services du système jugés inutiles ou non sécurisés définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 07(02) | Fonctionnalité minimale | Fonctionnalité minimale : Prévention de l'exécution des programmes<br>Empêcher l'exécution des programmes conformément à [Sélection (un choix ou plus) : [Affectation : stratégies, règles de conduite et ententes d'accès sur l'utilisation de programmes informatiques et restrictions connexes définies par l'organisation]; règles d'autorisation des modalités d'utilisation d'un programme informatique]. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 07(03) | Fonctionnalité minimale | Fonctionnalité minimale : Conformité aux exigences d'enregistrement<br>Assurer la conformité avec [Affectation : exigences d'enregistrement définies par l'organisation pour des fonctions, des ports, des protocoles et des services]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 07(04) | Fonctionnalité minimale | Fonctionnalité minimale : Logiciel non autorisé – Interdire par exception<br>a. Identifier les [Affectation : programmes informatiques ne pouvant pas être exécutés sur le système définis par l'organisation]<br>b. Recourir à une stratégie tout permettre, interdire par exception pour empêcher l'exécution des programmes informatiques non autorisés sur le système<br>c. Passer en revue et mettre à jour la liste des programmes informatiques autorisés tous les [Affectation : fréquence définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 07(05) | Fonctionnalité minimale | Fonctionnalité minimale : Logiciels autorisés – Autorisation par exception<br>a. Identifier les [Affectation : programmes informatiques pouvant être exécutés sur le système définis par l'organisation]<br>b. Recourir à une stratégie tout interdire, autoriser par exception pour permettre l'exécution des programmes | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | informatiques autorisés sur le système<br>c. Passer en revue et mettre à jour la liste des programmes informatiques autorisés tous les [Affectation : fréquence définie par l'organisation] | | | | |
| CM | 07(06) | Fonctionnalité minimale | Fonctionnalité minimale : Environnements clos aux privilèges restreints<br>Exiger que les logiciels installés par l'utilisatrice ou utilisateur désignés soient exécutés dans un environnement physique clos ou un environnement clos de machine virtuelle dont les privilèges sont restreints : [Affectation : logiciels installés par les utilisatrices ou utilisateurs désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 07(07) | Fonctionnalité minimale | Fonctionnalité minimale : Exécution de code dans des environnements protégés<br>Permettre l'exécution de code binaire ou exécutable sur machine uniquement dans un environnement physique clos ou dans un environnement clos de machine virtuelle avec l'approbation explicite de [Affectation : personnel ou rôles définis par l'organisation] lorsqu'un tel code<br>a. provient de sources qui n'offrent pas de garantie ou qui offrent une garantie limitée<br>b. dans les cas où ils n'offrent pas le code source | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 07(08) | Fonctionnalité minimale | Fonctionnalité minimale : Code binaire ou exécutable sur machine<br>a. Interdire l'utilisation de code binaire ou exécutable sur machine provenant de sources qui n'offrent pas de garantie ou qui offrent une garantie limitée dans les cas où il n'y a pas de code source<br>b. Permettre des exceptions uniquement dans situations urgentes liées à la mission ou aux besoins opérationnels et avec le consentement écrit exprès de l'autorité responsable | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 07(09) | Fonctionnalité minimale | Fonctionnalité minimale : Empêcher l'utilisation de composants matériels non autorisés<br>a. Identifier [Affectation : composants matériels autorisés définis par l'organisation pour l'utilisation du système]<br>b. Empêcher l'utilisation ou la connexion de composants matériels non autorisés<br>c. Passer en revue et mettre à jour la liste des composants matériels autorisés tous les [Affectation : fréquence définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 08 | Inventaire des composants du système | A. Élaborer et documenter un inventaire des composants des systèmes qui<br>1. illustre exactement le système<br>2. comprend tous les composants dans le système<br>3. ne comprend aucune comptabilisation en double des composants ou des composants attribués à un autre système<br>4. est au niveau de granularité jugé nécessaire aux fins de suivi et de production de rapports<br>5. comprend l'information suivante pour assurer la comptabilisation des composants de systèmes : [Affectation : information définie par l'organisation et jugée nécessaire à la comptabilisation efficace des composants de système]<br>B. Passer en revue et mettre à jour l'inventaire des composants du système tous les [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 08(01) | Inventaire des composants du système | Inventaire des composants de système : Mises à jour durant l'installation et le retrait<br>Faire de la mise à jour de l'inventaire des composantes du système une étape de l'installation ou du retrait de composantes ainsi que de la mise à jour du système. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 08(02) | Inventaire des composants du système | Inventaire des composants de système : Automatisation de la maintenance<br>Assurer l'actualité, le caractère exhaustif, l'exactitude et la disponibilité de l'inventaire des composants du système au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CM | 08(03) | Inventaire des composants du système | Inventaire des composants de système : Détection automatisée de composants non autorisés<br>a. Détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation] [Affectation : fréquence définie par l'organisation]<br>b. Prendre les mesures suivantes lorsque des composants non autorisés sont détectés : [Sélection (un choix ou plus) : désactiver l'accès réseau de ces composants; isoler les composants; aviser [Affectation : personnel ou rôles définis par l'organisation]] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 08(04) | Inventaire des composants du système | Inventaire des composants de système : Information sur la responsabilisation<br>Inclure dans l'information liée à l'inventaire de composants de système d'information une façon d'identifier par [Sélection (un choix ou plus) : nom; poste; rôle] les personnes responsables de l'administration de ces composants. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 08(05) | Inventaire des composants du système | Inventaire des composants de système : Aucune comptabilisation en double des composants<br>Annulé : Intégré au contrôle CM-08. | s.o. | s.o. | s.o. | s.o. |
| CM | 08(06) | Inventaire des composants du système | Inventaire des composants de système : Configurations évaluées et écarts approuvés<br>Inclure dans l'inventaire des composants du système les configurations de composants évaluées et les écarts approuvés en ce qui a trait aux configurations déjà déployées. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 08(07) | Inventaire des composants du système | Inventaire des composants de système : Référentiel centralisé<br>Fournir un référentiel centralisé contenant l'inventaire des composants de système. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 08(08) | Inventaire des composants du système | Inventaire des composants de système : Localisation automatisée<br>Appuyer le suivi des composants de système par géolocalisation des composants de système au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 08(09) | Inventaire des composants du système | Inventaire des composants de système : Attribution de composants à des systèmes :<br>a. Attribuer des composants de systèmes à un système<br>b. Recevoir un avis de cette affectation de la part de [Affectation : personnel ou rôles définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 09 | Plan de gestion des configurations | Élaborer, documenter et mettre en œuvre un plan de gestion des configurations pour le système qui<br>A. traite les rôles, les responsabilités ainsi que les processus et procédures de gestion des configurations<br>B. établit un processus pour déterminer les éléments de configuration tout au long du cycle de développement des systèmes et pour gérer la configuration des éléments de configuration<br>C. définit les éléments de configuration pour le système et intègre les éléments de configuration à la gestion des configurations<br>D. est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation]<br>E. protège le plan de gestion des configurations contre toute divulgation ou modification non autorisée | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 09(01) | Plan de gestion des configurations | Plan de gestion des configurations : Attribution des responsabilités<br>Confier la responsabilité du développement du processus de gestion des configurations à des employées et employés de l'organisation qui ne participent pas directement au développement du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 10 | Restrictions relatives à | A. Utiliser les logiciels et la documentation connexe conformément aux ententes contractuelles et aux lois sur le droit d'auteur | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | l'utilisation des logiciels | B. Faire le suivi de l'utilisation des logiciels et de la documentation connexe qui sont protégés par des licences limitant la copie et la diffusion du produit<br>C. Contrôler et documenter l'utilisation de la technologie de partage de fichiers pair à pair pour s'assurer qu'elle n'est pas utilisée à des fins non autorisées de distribution, d'affichage, d'exécution ou de reproduction d'œuvres protégées par le droit d'auteur | | | | |
| CM | 10(01) | Restrictions relatives à l'utilisation des logiciels | Restrictions relatives à l'utilisation des logiciels : Logiciels ouverts<br>Établir les restrictions suivantes sur l'utilisation de logiciel à source ouverte : [Affectation : restrictions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 11 | Logiciels installés par les utilisatrices et utilisateurs | A. Établir [Affectation : stratégies définies par l'organisation] qui régissent l'installation de logiciels par des utilisatrices et utilisateurs<br>B. Appliquer des stratégies d'installation de logiciels au moyen des méthodes suivantes : [Affectation : méthodes définies par l'organisation]<br>C. Surveiller le respect des stratégies [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 11(01) | Logiciels installés par les utilisatrices et utilisateurs | Logiciels installés par les utilisatrices et utilisateurs : Alertes pour les installations non autorisées;<br>Annulé : Intégré au contrôle CM-08(03). | s.o. | s.o. | s.o. | s.o. |
| CM | 11(02) | Logiciels installés par les utilisatrices et utilisateurs | Logiciels installés par les utilisatrices et utilisateurs : Installation de logiciels avec statut privilégié<br>Autoriser l'installation de logiciel par les utilisatrices et utilisateurs qui ont un accès privilégié explicite. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 11(03) | Logiciels installés par les utilisatrices et utilisateurs | Logiciels installés par les utilisatrices et utilisateurs : Application et surveillance automatisées<br>Appliquer et surveiller la conformité aux stratégies d'installation de logiciels au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CM | 12 | Localisation de l'information | A. Établir et consigner la localisation de [Affectation : information désignée par l'organisation] et des composants de systèmes particuliers où l'information est traitée et stockée<br>B. Établir et consigner les utilisatrices et utilisateurs qui ont accès au système et à ses composants où l'information est traitée et stockée<br>C. Consigner les changements de la localisation (par exemple, le système ou les composants du système) où l'information est traitée et stockée | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 12(01) | Localisation de l'information | Localisation de l'information : Outils automatisés associés à la localisation de l'information<br>Utiliser des outils automatisés pour identifier [Affectation : information définie par l'organisation selon le type d'information] sur des [Affectation : composants de système définis par l'organisation] pour assurer que des contrôles sont mis en place pour protéger l'information de l'organisation et la vie privée des personnes. | Contrôle | Sélectionné | s.o. | s.o. |
| CM | 13 | Mappage des actions de données | Élaboration et documentation d'un plan des actions de données du système. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CM | 14 | Composants signés | Empêcher l'installation de [Affectation : éléments logiciels et micrologiciels définis par l'organisation] sans vérification de leur signature électronique par l'intermédiaire d'un certificat reconnu ou approuvé par l'organisation. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| CP | 01 | Politique et procédures de planification d'urgence | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de planification d'urgence [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre des politiques de gestion de planification d'urgence et des contrôles de planification d'urgence connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la planification d'urgence.<br>C. Passer en revue et mettre à jour, par rapport à la planification d'urgence,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| CP | 02 | Plan d'urgence | A. Élaborer un plan d'urgence pour le système qui<br>1. identifie les fonctions opérationnelles et de mission essentielles et les exigences connexes en matière d'urgence<br>2. définit les objectifs de reprise, les priorités de restauration et les paramètres<br>3. identifie les rôles et responsabilités liés aux urgences et les personnes assignées à ces fonctions, y compris leurs coordonnées<br>4. souligne le besoin de maintenir les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance du système<br>5. traite de la restauration complète du système sans détérioration des contrôles initialement prévus et mis en œuvre<br>6. traite de l'intégrité des données conservées dans le système, y compris les renseignements personnels<br>7. traite des répercussions, des préjudices ou des conséquences de la compromission d'un système, y compris en ce qui a trait aux renseignements personnels<br>8. décrit les modalités d'échange d'information<br>9. est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation]<br>B. Distribuer des exemplaires du plan d'urgence à [Affectation : liste (par nom ou rôle) définie par l'organisation des principales et principaux responsables des mesures d'urgence et des éléments organisationnels]<br>C. S'assurer que les personnes qui assument des responsabilités examinent le plan d'urgence et comprennent leurs rôles<br>D. Coordonner les activités de planification d'urgence avec les activités de traitement des incidents | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | E. Examiner le plan d'urgence pour le système [Affectation : fréquence définie par l'organisation]<br>F. Mettre à jour le plan d'urgence pour tenir compte des changements apportés à l'organisation, au système ou à l'environnement d'exploitation et des problèmes survenus lors de la mise en œuvre, de l'exécution ou des tests du plan<br>G. Communiquer les changements apportés au plan d'urgence à [Affectation : liste (par nom ou rôle) définie par l'organisation des principales et principaux responsables des mesures d'urgence et des éléments organisationnels]<br>H. Intégrer les leçons apprises tirées des essais du plan d'urgence, de la formation ou des activités d'urgence concrètes aux essais et à la formation sur les mesures d'urgence<br>I. Protéger le plan d'urgence contre les divulgations ou les modifications non autorisées | | | | |
| CP | 02(01) | Plan d'urgence | Plan d'urgence : Coordination avec les plans connexes<br>Coordonner le développement du plan d'urgence avec les éléments organisationnels responsables des plans connexes. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 02(02) | Plan d'urgence | Plan d'urgence : Planification de la capacité<br>Planifier la capacité de manière à disposer des ressources nécessaires pour traiter l'information, utiliser les télécommunications et soutenir l'environnement durant les opérations d'urgence. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 02(03) | Plan d'urgence | Plan d'urgence : Reprise de la mission et des activités<br>Planifier la reprise des [Sélection (un choix) : toutes; essentielles] fonctions liées à la mission et aux activités essentielles dans un délai de [Affectation : délais définis par l'organisation] suivant l'activation du plan d'urgence. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 02(04) | Plan d'urgence | Plan d'urgence : Reprise de toutes les fonctions liées à la mission et aux activités de l'organisation<br>Annulé : Intégré au contrôle CP-02(03). | s.o. | s.o. | s.o. | s.o. |
| CP | 02(05) | Plan d'urgence | Plan d'urgence : Continuer les fonctions liées à la mission et aux activités<br>Planifier la continuité des [Sélection (un choix) : toutes; essentielles] fonctions liées à la mission et aux activités avec peu ou pas de perte sur le plan de la continuité opérationnelle et maintenir cet état jusqu'à la restauration complète du système dans les sites principaux de traitement ou de stockage | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 02(06) | Plan d'urgence | Plan d'urgence : Sites de traitement et de stockage auxiliaires<br>Prévoir le transfert des [Sélection (un choix) : toutes; essentielles] fonctions liées à la mission et aux activités essentielles vers des sites de traitement ou de stockage auxiliaires avec peu ou pas de perte sur le plan de la continuité des activités, et maintenir cet état pendant la restauration complète des sites principaux de traitement ou de stockage. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 02(07) | Plan d'urgence | Plan d'urgence : Coordination avec les fournisseurs de services externes<br>Coordonner son plan d'urgence avec ceux des fournisseurs de services externes pour veiller à répondre aux exigences des plans d'urgence. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 02(08) | Plan d'urgence | Plan d'urgence : Désignation des biens essentiels<br>Désigner les biens essentiels du système qui soutiennent [Sélection (un choix) : toutes; essentielles] les fonctions liées à la mission et aux activités. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 03 | Formation en mesure d'urgence | A. Fournir une formation en mesure d'urgence aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués<br>1. dans [Affectation : délais définis par l'organisation] après avoir été affecté à un rôle ou à des responsabilités<br>2. lorsque des changements apportés au système l'exigent<br>3. tous les [Affectation : fréquence définie par l'organisation] par la suite | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | B. Passer en revue et mettre à jour le contenu de la formation en mesure d'urgence tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation] | | | | |
| CP | 03(01) | Formation en mesure d'urgence | Formation en mesure d'urgence : Événements simulés<br>Intégrer des événements simulés à la formation en mesure d'urgence pour faciliter l'intervention efficace du personnel en situation de crise. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 03(02) | Formation en mesure d'urgence | Formation en mesure d'urgence : Mécanismes utilisés dans des environnements de formation<br>Employer des mécanismes utilisés dans des opérations pour offrir un environnement de formation en mesure d'urgence plus approfondi et réaliste. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 04 | Tests relatifs au plan d'urgence | A. Mettre à l'essai le plan d'urgence pour les systèmes [Affectation : fréquence définie par l'organisation] en utilisant les tests suivants pour en déterminer l'efficacité et établir la mesure dans laquelle il est prêt à être exécuté : [Affectation : tests définis par l'organisation].<br>B. Étudier les résultats des tests du plan d'urgence<br>C. Prendre les mesures correctives nécessaires | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 04(01) | Tests relatifs au plan d'urgence | Tests relatifs au plan d'urgence : Coordination avec les plans connexes<br>Coordonner la mise à l'essai du plan d'urgence avec les éléments organisationnels responsables des plans connexes. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 04(02) | Tests relatifs au plan d'urgence | Tests relatifs au plan d'urgence : Site de traitement auxiliaires<br>Tester le plan d'urgence au site de traitement auxiliaire pour<br>a. familiariser le personnel participant au plan d'urgence pour qu'il connaisse mieux l'installation et les ressources qui y sont accessibles<br>b. évaluer si celui-ci peut prendre en charge les opérations d'urgence | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 04(03) | Tests relatifs au plan d'urgence | Tests relatifs au plan d'urgence : Tests automatisés<br>Tester le plan d'urgence au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 04(04) | Tests relatifs au plan d'urgence | Tests relatifs au plan d'urgence : Reprise et reconstitution complètes<br>Inclure dans les tests du plan d'urgence une reprise et une reconstitution complètes du système à un état connu. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 04(05) | Tests relatifs au plan d'urgence | Tests relatifs au plan d'urgence : Se mettre au défi<br>Employer [Affectation : mécanismes définis par l'organisation] pour [Affectation : système ou composant de système désigné par l'organisation] pour perturber et nuire au système ou au composant du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 05 | Mise à jour du plan d'urgence | Annulé : Intégré au contrôle CP-02. | s.o. | s.o. | s.o. | s.o. |
| CP | 06 | Site de stockage auxiliaire | A. Établir un site de stockage auxiliaire, y compris les ententes nécessaires pour permettre le stockage et la récupération de l'information de sauvegarde des systèmes<br>B. S'assurer que le site de stockage auxiliaire offre des contrôles équivalents à ceux du site principal | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 06(01) | Site de stockage auxiliaire | Site de stockage auxiliaire : Séparation du site principal<br>Identifier un site de stockage auxiliaire suffisamment distinct du site principal afin de réduire sensiblement l'exposition aux mêmes menaces. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CP | 06(02) | Site de stockage auxiliaire | Site de stockage auxiliaire : Objectifs de délai de rétablissement et de point de rétablissement<br>Configurer le site auxiliaire de manière à faciliter les opérations de reprise conformément aux objectifs de délai et de point de rétablissement. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 06(03) | Site de stockage auxiliaire | Site de stockage auxiliaire : Accessibilité<br>Identifier les problèmes d'accessibilité potentiels du site stockage auxiliaire dans l'éventualité d'une perturbation ou d'un désastre majeurs et énoncer des mesures d'atténuation explicites. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 07 | Site de traitement auxiliaire | A. Établir un site de traitement auxiliaire, y compris les ententes nécessaires pour permettre le transfert et la reprise [Affectation : opérations des systèmes définies par l'organisation] pour les fonctions opérationnelles et de mission essentielles dans un délai de [Affectation : durée conforme aux objectifs de délai et de point de reprise définis par l'organisation], lorsque les capacités de traitement principales ne sont pas accessibles<br>B. Rendre accessibles au site de traitement auxiliaire l'équipement et les fournitures nécessaires pour transférer et permettre une reprise des activités ou mettre des contrats pour assurer leur livraison au site, et ce, dans les délais définis par l'organisation pour le transfert ou la reprise des activités<br>C. Fournir des contrôles au site de traitement auxiliaire qui sont équivalents à ceux du site principal | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 07(01) | Site de traitement auxiliaire | Site de traitement auxiliaire : Séparation du site principal<br>Identifier un site de traitement auxiliaire suffisamment distinct du site principal afin de réduire sensiblement l'exposition aux mêmes menaces. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 07(02) | Site de traitement auxiliaire | Site de traitement auxiliaire : Accessibilité<br>Identifier les problèmes d'accessibilité potentiels des sites traitement auxiliaires dans l'éventualité d'une perturbation ou d'un désastre majeurs et énoncer des mesures d'atténuation explicites. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 07(03) | Site de traitement auxiliaire | Site de traitement auxiliaire : Priorité de service<br>Élaborer, pour le site de traitement auxiliaire, des conventions qui prévoient des dispositions de priorité de service conformément aux exigences d'accessibilité (y compris les objectifs de délai de récupération). | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 07(04) | Site de traitement auxiliaire | Site de traitement auxiliaire : Préparation en vue de l'utilisation<br>Préparer le site de traitement auxiliaire de manière à ce qu'il serve comme site opérationnel pour le traitement des fonctions opérationnelles et de mission essentielles. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 07(05) | Site de traitement auxiliaire | Site de traitement auxiliaire : Protections équivalentes de sécurité de l'information<br>Annulé : Intégré au contrôle CP-07. | s.o. | s.o. | s.o. | s.o. |
| CP | 07(06) | Site de traitement auxiliaire | Site de traitement auxiliaire : Impossibilité de retourner au site principal<br>Planifier et se préparer pour des circonstances qui empêchent de retourner au site de traitement principal. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 08 | Services de télécommunications | Établir des services de télécommunications de secours, y compris les conventions nécessaires pour permettre la reprise de [Affectation : opérations des systèmes désignés par l'organisation] pour les fonctions opérationnelles et de mission essentielles dans [Affectation : délais définis par l'organisation] lorsque les capacités de télécommunications de première ligne ne sont pas accessibles aux sites de stockage ou de traitement principaux ou auxiliaires. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CP | 08(01) | Services de télécommunications | Services de télécommunications : Dispositions de priorité de service<br>a. Élaborer des conventions de services de télécommunications de première ligne et de secours qui prévoient des dispositions de priorité de service conformément aux exigences d'accessibilité (y compris les objectifs de délai de récupération)<br>b. Demander un accès prioritaire à la composition par Innovation, Sciences et Développement économique Canada (ISDE) (voir la publication d'ISDE intitulée Accès prioritaire à la composition : services de télécommunications en périodes de crise) pour tous les services de télécommunications utilisés dans le cadre de préparatifs d'urgence en cas d'événement portant atteinte à la sécurité nationale dans l'éventualité où les services de télécommunications principaux ou de secours sont assurés par une entreprise de télécommunications | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 08(02) | Services de télécommunications | Services de télécommunications : Points de défaillance uniques<br>Obtenir les services de télécommunication de secours pour réduire la probabilité de partage d'un point de défaillance unique avec les services de télécommunication de première ligne. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 08(03) | Services de télécommunications | Services de télécommunications : Séparation des fournisseurs principaux et auxiliaire<br>Obtenir des services de télécommunications de secours auprès de fournisseurs distincts des fournisseurs principaux afin de réduire la vulnérabilité aux mêmes menaces. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 08(04) | Services de télécommunications | Services de télécommunications : Plan d'urgence des fournisseurs<br>a. Exiger des fournisseurs de services de télécommunications de première ligne et de secours qu'ils possèdent des plans d'urgence<br>b. Examiner les plans d'urgence des fournisseurs pour s'assurer que ces plans répondent aux exigences de l'organisation en matière d'urgence<br>c. Obtenir des preuves des tests du plan d'urgence et des formations de la part des fournisseurs [Affectation : fréquence définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 08(05) | Services de télécommunications | Services de télécommunications : Test des services de télécommunications de secours<br>Tester les services de télécommunications de secours [Affectation : fréquence définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 09 | Sauvegarde du système | A. Effectuer des sauvegardes des données utilisateur contenues dans le système [Affectation : composants de système désignés par l'organisation] [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]<br>B. Effectuer des sauvegardes des données système contenues dans le système [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]<br>C. Effectuer des sauvegardes de la documentation liée au système d'information, y compris la documentation sur la sécurité et la protection de la vie privée [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]<br>D. Protéger la confidentialité, l'intégrité et la disponibilité de l'information de sauvegarde<br>AA. L'organisation détermine les périodes de conservation de l'information opérationnelle essentielle et des sauvegardes archivées | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 09(01) | Sauvegarde du système | Sauvegarde du système : Tests de fiabilité et d'intégrité<br>Effectuer des tests de l'information de sauvegarde [Affectation : fréquence définie par l'organisation] pour vérifier la | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | fiabilité des supports et l'intégrité de l'information. | | | | |
| CP | 09(02) | Sauvegarde du système | Sauvegarde du système : Essai de restauration au moyen de l'échantillonnage<br>Utiliser un échantillon de l'information de sauvegarde pour restaurer certaines fonctions du système dans le cadre des tests du plan d'urgence. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 09(03) | Sauvegarde du système | Sauvegarde du système : Stockage distinct pour l'information essentielle<br>Conserver des copies de sauvegarde [Affectation : information liée à la sécurité et aux logiciels des systèmes essentiels définis par l'organisation], dans une installation distincte ou un conteneur résistant au feu situé hors de l'emplacement du système opérationnel. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 09(04) | Sauvegarde du système | Sauvegarde du système : Protection contre une modification non autorisée<br>Annulé : Intégré au contrôle CP-09. | s.o. | s.o. | s.o. | s.o. |
| CP | 09(05) | Sauvegarde du système | Sauvegarde du système : Transfert vers un site de stockage auxiliaire<br>Transférer l'information de sauvegarde du système dans un site de stockage auxiliaire [Affectation : délais et taux de transfert définis par l'organisation et conformes aux objectifs de délai et de point de reprise]. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 09(06) | Sauvegarde du système | Sauvegarde du système : Système secondaire redondant<br>Effectuer la sauvegarde du système au moyen d'un système secondaire redondant n'étant pas situé au même endroit que le système principal et pouvant être activé sans perte d'information ou perturbation des opérations. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 09(07) | Sauvegarde du système | Sauvegarde du système : Double autorisation pour la suppression ou la destruction<br>Appliquer l'exigence de double autorisation pour la suppression ou la destruction [Affectation : information de sauvegarde définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 09(08) | Sauvegarde du système | Sauvegarde du système : Protection cryptographique<br>Appliquer des mécanismes cryptographiques pour empêcher la divulgation et la modification non autorisées de [Affectation : l'information de sauvegarde définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 10 | Reprise et reconstitution du système | S'occuper de rendre à un état connu la reprise et la reconstitution du système dans [Affectation : un délai conforme aux objectifs de délai et de point de reprise définis par l'organisation] après une perturbation, une compromission ou une défaillance du système. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 10(01) | Reprise et reconstitution du système | Reprise et reconstitution du système : Tests relatifs au plan d'urgence<br>Annulé : Intégré au contrôle CP-04. | s.o. | s.o. | s.o. | s.o. |
| CP | 10(02) | Reprise et reconstitution du système | Reprise et reconstitution du système : Reprise des transactions<br>Appliquer un processus de reprise des transactions pour les systèmes de traitement transactionnel. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CP | 10(03) | Reprise et reconstitution du système | Reprise et reconstitution du système : Contrôles de sécurité compensatoires<br>Annulé : Intégré aux procédures d'adaptation. | s.o. | s.o. | s.o. | s.o. |
| CP | 10(04) | Reprise et reconstitution du système | Reprise et reconstitution du système : Restauration dans les délais précisés<br>Assurer la capacité permettant de rétablir les composants du système en dedans de [Affectation : délais de restauration définis par l'organisation] en utilisant l'information dont la configuration est contrôlée et l'intégrité, protégée représentant les composants dans un état sécurisé et opérationnel. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 10(05) | Reprise et reconstitution du système | Reprise et reconstitution du système : Capacité de basculement<br>Annulé : Intégré au contrôle SI-13. | s.o. | s.o. | s.o. | s.o. |
| CP | 10(06) | Reprise et reconstitution du système | Reprise et reconstitution du système : Protection des composants<br>Protéger les composants du système utilisés pour la reprise et la reconstitution. | Contrôle | Sélectionné | s.o. | s.o. |
| CP | 11 | Protocoles des communications de secours | Permettre l'utilisation [Affectation : protocoles de communications de secours définis par l'organisation] afin de maintenir la continuité des opérations. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 12 | Mode sans échec | Le système passe au mode sans échec [Affectation : contraintes du mode d'opération sans échec définies par l'organisation] lorsqu'il détecte [Affectation : conditions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| CP | 13 | Mécanismes de sécurité de secours | Utiliser [Affectation : mécanismes de sécurité de secours ou additionnels définis par l'organisation] en vue d'exécuter [Affectation : fonctions de sécurité définies par l'organisation] lorsque le mode principal d'exécution de la fonction de sécurité est compromis ou n'est pas disponible. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| IA | 01 | Politique et procédures d'identification et d'authentification | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique d'identification et d'authentification [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique d'identification et d'authentification ainsi que des contrôles d'identification et d'authentification<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | la diffusion de la politique et des procédures d'identification et d'authentification<br>C. Passer en revue et mettre à jour, par rapport à l'identification et l'authentification,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | | | | |
| IA | 02 | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identifier de façon unique et authentifier les utilisatrices et utilisateurs organisationnels, puis associer cet identifiant unique aux processus agissant en leur nom. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 02(01) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : AMF robustes pour les comptes privilégiés<br>Appliquer des mécanismes robustes d'authentification multifacteur (AMF) pour l'accès aux comptes privilégiés. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 02(02) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : AMF pour comptes non privilégiés<br>Appliquer des mécanismes robustes d'authentification multifacteur (AMF) pour l'accès aux comptes privilégiés non privilégiés. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 02(03) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès local aux comptes privilégiés<br>Annulé : Intégré au contrôle IA-02(01). | s.o. | s.o. | s.o. | s.o. |
| IA | 02(04) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès local aux comptes non privilégiés<br>Annulé : Intégré au contrôle IA-02(02). | s.o. | s.o. | s.o. | s.o. |
| IA | 02(05) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Authentification individuelle avec authentification de groupe<br>Lorsque des authentifiants ou des comptes partagés sont utilisés, il faut que les utilisatrices et utilisateurs soient authentifiés individuellement avant d'obtenir l'accès aux ressources ou aux comptes partagés. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 02(06) | Identification et authentification (utilisatrices et | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès aux comptes – Dispositif distinct<br>Mettre en œuvre l'AMF pour l'accès [Sélection (un choix ou plus) : local; réseau; à distance] aux [Sélection (un choix ou plus) : comptes privilégiés; comptes non privilégiés] de façon à ce que | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | utilisateurs de l'organisation) | a. l'un des facteurs soit fourni par un dispositif distinct du système qui obtient un accès<br>b. le dispositif satisfasse [Affectation : exigences de la force du mécanisme définies par l'organisation] | | | | |
| IA | 02(07) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès réseau aux comptes non privilégiés – Dispositif distinct<br>Annulé : Intégré au contrôle IA-02(06). | s.o. | s.o. | s.o. | s.o. |
| IA | 02(08) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès aux comptes – Résistant à la réinsertion<br>Mettre en œuvre des mécanismes d'authentification résistant à la réinsertion pour l'accès aux [Sélection (un choix ou plus) : comptes privilégiés; comptes non privilégiés]. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 02(09) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès réseau aux comptes non privilégiés – Résistance à la réinsertion<br>Annulé : Intégré au contrôle IA-02(08). | s.o. | s.o. | s.o. | s.o. |
| IA | 02(10) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Authentification unique<br>Offrir une fonctionnalité d'authentification unique des [Affectation : services et comptes du système définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 02(11) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Accès à distance – Dispositif distinct<br>Annulé : Intégré au contrôle IA-02(06). | s.o. | s.o. | s.o. | s.o. |
| IA | 02(12) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Utilisation de jeton matériel du GC basé sur des justificatifs d'identité d'ICP<br>Accepter et vérifier électroniquement le jeton matériel du GC basé sur des justificatifs d'identité d'ICP. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 02(13) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Authentification hors bande<br>Mettre en œuvre les mécanismes d'authentification hors bande suivants en vertu des [Affectation : conditions définies par l'organisation] : [Affectation : authentification hors bande définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 02(400) | Identification et authentification | Identification et authentification (utilisatrices et utilisateurs de l'organisation) : Mettre en œuvre des mécanismes robustes d'authentification multifacteur (AMF) pour l'accès à distance aux comptes privilégiés | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | (utilisatrices et utilisateurs de l'organisation) | Annulé : Intégré aux contrôles IA-02(01) et IA-02(06). | | | | |
| IA | 03 | Identification et authentification des dispositifs | Identifier et authentifier, de manière unique [Affectation : dispositifs ou types de dispositifs définis par l'organisation] avant d'établir une connexion [Sélection (un choix ou plus) : locale; à distance; réseau]. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 03(01) | Identification et authentification des dispositifs | Identification et authentification des dispositifs : Authentification bidirectionnelle cryptographique<br>Authentifier [Affectation : dispositifs ou types de dispositifs définis par l'organisation] avant d'établir une connexion [Sélection (un choix ou plus) : locale; à distance; réseau] utilisant l'authentification bidirectionnelle reposant sur la cryptographie. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 03(02) | Identification et authentification des dispositifs | Identification et authentification des dispositifs : Authentification réseau bidirectionnelle cryptographique<br>Annulé : Intégré au contrôle IA-03(01). | s.o. | s.o. | s.o. | s.o. |
| IA | 03(03) | Identification et authentification des dispositifs | Identification et authentification des dispositifs : Attribution dynamique des adresses<br>a. Où les adresses sont attribuées de manière dynamique, l'information de location de l'attribution dynamique des adresses ainsi que la durée de la location attribuée aux dispositifs conformément à [Affectation : information sur la location et durée de la location définies par l'organisation]<br>b. Vérifier l'information de location lorsqu'elle est attribuée à un dispositif | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 03(04) | Identification et authentification des dispositifs | Identification et authentification des dispositifs : Attestation de dispositifs<br>Traiter l'identification et l'authentification des dispositifs conformément à une attestation au moyen [Affectation : processus de gestion des configurations défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04 | Gestion des identifiants | Gérer les identifiants de système des façons suivantes<br>A. recevoir une autorisation de [Affectation : personnel ou rôles de l'organisation] pour attribuer un identifiant à une personne, à un groupe, à un rôle, à un service ou à un dispositif<br>B. sélectionner et déterminer un identifiant qui identifie une personne, un groupe, un rôle, un service ou un dispositif<br>C. attribuer l'identifiant à la personne, au groupe, au rôle, au service ou au dispositif prévu<br>D. prévenir la réutilisation d'identifiant pendant [Affectation : délai défini par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 04(01) | Gestion des identifiants | Gestion des identifiants : Interdire l'utilisation d'identifiants de compte en tant qu'identifiants publics<br>Interdire l'utilisation d'identifiants de compte du système qui sont les mêmes que les identifiants publics pour les comptes individuels. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04(02) | Gestion des identifiants | Gestion des identifiants : Autorisation de superviseure ou superviseur<br>Annulé : Intégré au contrôle IA-12(01). | s.o. | s.o. | s.o. | s.o. |
| IA | 04(03) | Gestion des identifiants | Gestion des identifiants : Multiples formes de certification<br>Annulé : Intégré au contrôle IA-12(02). | s.o. | s.o. | s.o. | s.o. |
| IA | 04(04) | Gestion des identifiants | Gestion des identifiants : Établissement du statut d'une utilisatrice ou d'un utilisateur<br>Gérer les identifiants personnels en identifiant de façon unique chaque personne à titre de [Affectation : caractéristique définie par l'organisation identifiant le statut de la personne]. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IA | 04(05) | Gestion des identifiants | Gestion des identifiants : Gestion dynamique<br>Gérer de manière dynamique les identifiants conformément à la [Affectation : stratégie sur les identifiants dynamiques définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04(06) | Gestion des identifiants | Gestion des identifiants : Gestion interorganisationnelle<br>Collaborer avec les organisations externes suivantes pour la gestion interorganisationnelle des identifiants : [Affectation : organisations externes désignées par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04(07) | Gestion des identifiants | Gestion des identifiants : Inscription en personne<br>Annulé : Intégré au contrôle IA-12(04). | s.o. | s.o. | s.o. | s.o. |
| IA | 04(08) | Gestion des identifiants | Gestion des identifiants : Identifiants pseudonymes par paires<br>Générer des identifiants pseudonymes par paires. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04(09) | Gestion des identifiants | Gestion des identifiants : Maintenance et protection d'attributs<br>Maintenir les attributs de chaque personne, dispositif ou service identifié de manière unique dans [Affectation : stockage central protégé défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04(400) | Gestion des identifiants | Gestion des identifiants : Protection de la biométrie<br>Maintenir une protection adéquate pour la biométrie conformément aux règlements sur la protection des renseignements personnels. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 04(401) | Gestion des identifiants | Gestion des identifiants : Intégrité de la biométrie<br>Assurer l'intégrité de la biométrie recueillie. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05 | Gestion des authentifiants | Gérer les authentifiants de système des façons suivantes<br>A. vérifier, au moment de la distribution initiale d'un authentifiant, l'identité de l'utilisatrice ou utilisateur, du groupe, du rôle, du service ou du dispositif recevant l'authentifiant<br>B. établir le contenu de l'authentifiant initial pour les authentifiants émis par l'organisation<br>C. s'assurer que le mécanisme d'authentification est suffisamment robuste pour l'utilisation prévue<br>D. établir et mettre en œuvre des procédures administratives pour la distribution initiale des authentifiants en cas de perte, de compromission, de corruption et de révocation<br>E. changer les authentifiants par défaut lors de la première utilisation<br>F. modifier ou actualiser les authentifiants [Affectation : durée définie par l'organisation selon le type d'authentifiant] ou quand [Affectation : événements définis par l'organisation]] se produisent<br>G. protéger le contenu des authentifiants contre les divulgations ou les modifications non autorisées<br>H. exiger que les personnes et les dispositifs appliquent des contrôles particuliers de manière à protéger les authentifiants<br>I. modifier les authentifiants pour les comptes de groupes ou de rôles lorsque des changements sont apportés à leurs membres | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 05(01) | Gestion des authentifiants | Gestion des authentifiants : Authentification basée sur mot de passe<br>Pour l'authentification basée sur mot de passe<br>a. créer une liste des mots de passe couramment utilisés, attendus ou compromis et la mettre à jour tous les [Affectation : fréquence définie par l'organisation] et lorsque l'on soupçonne que les mots de passe de l'organisation ont été compromis, directement ou indirectement | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | b. lorsque les utilisatrices et utilisateurs créent ou mettent à jour des mots de passe, vérifier que les mots de passe ne figurent pas sur la liste des mots de passe couramment utilisés, attendus ou compromis figurant au contrôle IA-05(01)a<br>c. transmettre les mots de passe uniquement par des canaux protégés par chiffrement<br>d. stocker les mots de passe au moyen de la fonction de dérivation de clé avec sel, de préférence avec hachage de clé<br>e. exiger la sélection immédiate d'un mot de passe dès la récupération du compte<br>f. autoriser les utilisatrices et utilisateurs à choisir de longs mots de passe et phrases de passe, y compris les espaces et les caractères imprimables<br>g. utiliser des outils automatisés pour aider l'utilisatrice ou utilisateur à sélectionner des authentifiants de mots de passe robustes<br>h. appliquer les règles de composition et de complexité suivantes : [Affectation : règles de composition et de complexité définies par l'organisation] | | | | |
| IA | 05(02) | Gestion des authentifiants | Gestion des authentifiants : Authentification basée sur clé publique<br>a. Pour une authentification basée sur clé publique<br>1) appliquer la procédure d'accès autorisé à la clé privée correspondante<br>2) associer l'identité authentifiée au compte d'une personne ou d'un groupe<br>b. Lorsque l'infrastructure à clé publique (ICP) est utilisée<br>1) valider les certificats en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé, y compris la vérification de l'information d'état des certificats<br>2) utiliser une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 05(03) | Gestion des authentifiants | Gestion des authentifiants : Enregistrement par tierce partie externe de confiance<br>Annulé : Intégré au contrôle IA-12(04). | s.o. | s.o. | s.o. | s.o. |
| IA | 05(04) | Gestion des authentifiants | Gestion des authentifiants : Soutien automatisé aux fins de détermination de la robustesse du mot de passe<br>Annulé : Intégré au contrôle IA-05(01). | s.o. | s.o. | s.o. | s.o. |
| IA | 05(05) | Gestion des authentifiants | Gestion des authentifiants : Changement des authentifiants avant la livraison<br>Exiger des développeuses et développeurs ou des installatrices et installateurs des fabricants des composants de système qu'ils fournissent des authentifiants uniques ou qu'ils changent les authentifiants par défaut avant la livraison ou l'installation. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05(06) | Gestion des authentifiants | Gestion des authentifiants : Protection des authentifiants<br>Protéger les authentifiants au niveau de sécurité qui correspond à la catégorie de sécurité de l'information à laquelle l'authentifiant permet l'accès. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 05(07) | Gestion des authentifiants | Gestion des authentifiants : Aucun authentifiant statique intégré non chiffré<br>S'assurer que les authentifiants statiques non chiffrés ne sont pas intégrés dans les applications ou autres formes de stockage statique. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 05(08) | Gestion des authentifiants | Gestion des authentifiants : Comptes multiples des systèmes<br>Mettre en œuvre [Affectation : contrôles de sécurité définis par l'organisation] pour gérer le risque de compromission que posent les utilisatrices et utilisateurs qui possèdent des comptes dans plusieurs systèmes. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IA | 05(09) | Gestion des authentifiants | Gestion des authentifiants : Gestion des justificatifs d'identité fédérés<br>Utiliser les organisations externes suivantes pour fédérer les justificatifs d'identité : [Affectation : organisations externes désignées par l'organisation]. | Contrôle | Sélectionné | [SPC] | s.o. |
| IA | 05(10) | Gestion des authentifiants | Gestion des authentifiants : Liaison dynamique des justificatifs d'identité<br>Lier les identités et les authentifiants de manière dynamique au moyen des règles suivantes : [Affectation : règles de liaison définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05(11) | Gestion des authentifiants | Gestion des authentifiants : Authentification basée sur un jeton matériel<br>Annulé : Intégré aux contrôles IA-02(01) et IA-02(02). | s.o. | s.o. | s.o. | s.o. |
| IA | 05(12) | Gestion des authentifiants | Gestion des authentifiants : Rendement de l'authentification biométrique<br>Pour l'authentification fondée sur la biométrie, utiliser des mécanismes qui répondent [Affectation : exigences en matière de qualité de la biométrie définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05(13) | Gestion des authentifiants | Gestion des authentifiants : Expiration d'authentifiants en mémoire cache<br>Interdire l'utilisation d'authentifiants en mémoire cache après [Affectation : délais définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 05(14) | Gestion des authentifiants | Gestion des authentifiants : Gestion du contenu des magasins de confiance d'ICP<br>Pour l'authentification fondée sur l'ICP, utiliser une méthodologie de gestion du contenu des magasins de confiance d'ICP installés sur toutes les plateformes, y compris les réseaux, les systèmes d'exploitation, les navigateurs et les applications. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 05(15) | Gestion des authentifiants | Gestion des authentifiants : Produits et services conformes aux niveaux d'assurance de l'identité, des justificatifs et de l'authentification<br>Utiliser uniquement des produits et des services pour la gestion de l'identité, des justificatifs et de l'accès qui sont conformes aux niveaux d'assurance requis. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05(16) | Gestion des authentifiants | Gestion des authentifiants : Émission d'un authentifiant en personne ou par tierce partie externe de confiance<br>Exiger que l'émission [Affectation : types d'authentifiant ou authentifiants spécifiques définis par l'organisation] soit effectuée [Sélection (un choix) : en personne; par une partie externe de confiance] auprès [Affectation : autorité d'enregistrement définie par l'organisation] avec l'autorisation de [Affectation : personnel ou rôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05(17) | Gestion des authentifiants | Gestion des authentifiants : Détection des attaques de présentation pour les authentifiants biométriques<br>Utiliser des mécanismes de détection des attaques pour l'authentification fondée sur la biométrie. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 05(18) | Gestion des authentifiants | Gestion des authentifiants : Gestionnaires de mots de passe<br>a. Utiliser [Affectation : gestionnaires de mots de passe définis par l'organisation] pour générer et gérer les mots de passe.<br>b. Protéger les mots de passe au moyen de [Affectation : contrôles définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 06 | Réinjection d'authentification | Obscurcir les réinjections d'information durant le processus d'authentification afin de protéger l'information contre de possibles exploitations ou utilisations par des personnes non autorisées. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IA | 07 | Authentification du module cryptographique | Mettre en place des mécanismes pour l'authentification auprès d'un module cryptographique qui répond aux exigences imposées par les lois, les décrets, les directives, les politiques, la réglementation, les normes et les lignes directrices applicables, pour une telle authentification. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 08 | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identifier de façon unique et authentifier les utilisatrices et utilisateurs non organisationnels ou les processus exécutés en leur nom. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 08(01) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Acceptation des justificatifs d'identité d'ICP d'autres organismes<br>Accepter et vérifier électroniquement les justificatifs d'identité d'ICP d'autres ministères et organismes du GC. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 08(02) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Acceptation des authentifiants externes<br>a. Accepter uniquement des authentifiants externes qui sont conformes à un niveau d'assurance propre à l'ITSP.30.031<br>b. Consigner et maintenir une liste d'authentifiants externes acceptés | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 08(03) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Utilisation de produits approuvés par l'architecture FICAM (Federal Identity, Credential, and Access Management)<br>Annulé : Intégré au contrôle IA-08(02) et propre aux États-Unis. | s.o. | s.o. | s.o. | s.o. |
| IA | 08(04) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Utilisation de profils définis<br>Se conformer aux profils suivants pour la gestion des identités [Affectation : profils de gestion des identités définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IA | 08(05) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Acceptation des justificatifs de vérification de l'identité personnelle interopérables (PIV-I)<br>Accepter et vérifier les justificatifs fédérés ou d'ICP qui satisfont [Affectation : stratégie définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 08(06) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Dissociabilité<br>Mettre en œuvre les mesures suivantes pour dissocier les attributs d'utilisatrice ou utilisateur ou les relations d'assertion d'identificateur parmi les personnes, les fournisseurs de justificatifs d'identité et les parties de confiance : [Affectation : mesures définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 08(400) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) | Identification et authentification (utilisatrices et utilisateurs ne faisant pas partie de l'organisation) : Identité et assurance des justificatifs<br>Annulé : Intégré au contrôle IA-05(15). | s.o. | s.o. | s.o. | s.o. |
| IA | 09 | Identification et authentification des services | Identifier de façon unique et authentifier les [Affectation : services et applications système définis par l'organisation] avant d'établir des communications avec des dispositifs, des utilisatrices, des utilisateurs ou d'autres services ou applications. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 09(01) | Identification et authentification des services | Identification et authentification des services : Échange d'information<br>Annulé : Intégré au contrôle IA-09. | s.o. | s.o. | s.o. | s.o. |
| IA | 09(02) | Identification et authentification des services | Identification et authentification des services : Transmission des décisions<br>Annulé : Intégré au contrôle IA-09. | s.o. | s.o. | s.o. | s.o. |
| IA | 10 | Authentification adaptative | Exiger que les personnes accédant au système utilisent [Affectation : techniques ou mécanismes d'authentification supplémentaires définis par l'organisation] pour certaines situations particulières, dont notamment [Affectation : circonstances ou situations définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 11 | Réauthentification | Exiger la réauthentification des utilisatrices et utilisateurs lors de [Affectation : circonstances ou situations nécessitant une réauthentification définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 12 | Confirmation de l'identité | A. Confirmer l'identité des utilisatrices et utilisateurs qui ont besoin de comptes pour un accès logique aux systèmes en fonction d'exigences adéquates en matière de niveau d'assurance de l'identité comme il est précisé dans les normes et | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | les lignes directrices applicables<br>B. Régler les identités d'utilisatrices et utilisateurs dans un compte individuel unique<br>C. Collecter, valider et vérifier la preuve d'identité | | | | |
| IA | 12(01) | Confirmation de l'identité | Confirmation de l'identité : Autorisation de superviseure ou superviseur<br>Exiger que le processus d'enregistrement permettant de recevoir un compte pour l'accès logique comprenne une autorisation de superviseure ou superviseur ou d'autorité qui parraine. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 12(02) | Confirmation de l'identité | Confirmation de l'identité : Preuve d'identité<br>Exiger qu'une preuve d'identification d'une personne soit présentée à l'autorité d'enregistrement. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 12(03) | Confirmation de l'identité | Confirmation de l'identité : Validation et vérification de preuve d'identité<br>Exiger que la preuve d'identité présentée soit validée et vérifiée au moyen de [Affectation : méthodes de validation et de vérification définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 12(04) | Confirmation de l'identité | Confirmation de l'identité : Validation et vérification en personne<br>Exiger que la validation et la vérification d'une preuve d'identité soient effectuées en personne auprès d'une autorité d'enregistrement désignée. | Contrôle | Sélectionné | s.o. | s.o. |
| IA | 12(05) | Confirmation de l'identité | Confirmation de l'identité : Confirmation d'adresse<br>Exiger que [Sélection (un choix) : code d'enregistrement; avis de confirmation] soit transmis par l'entremise d'une voie d'acheminement hors bande pour vérifier l'adresse de l'utilisatrice ou utilisateur (physique ou numérique) pour le dossier. | Contrôle | Sélectionné | s.o. | Ce contrôle est recommandé pour les utilisatrices et utilisateurs ne faisant pas partie de l'organisation. |
| IA | 12(06) | Confirmation de l'identité | Confirmation de l'identité : Accepter les identités confirmées externes<br>Accepter les identités confirmées externes au [Affectation : niveau d'assurance de l'identité défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 13 | Fournisseurs d'identité et serveurs d'autorisation | Avoir recours à des fournisseurs d'identité et à des serveurs d'autorisation pour gérer les identités, les attributs et les droits d'accès des personnes, des dispositifs et des entités qui ne sont pas des personnes (NPE pour *Non-Person Entity*) de manière à soutenir les décisions en matière d'authentification et d'autorisation conformément à la [Affectation : stratégie d'identification et d'authentification définie par l'organisation] faisant appel aux [Affectation : mécanismes définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 13(01) | Fournisseurs d'identité et serveurs d'autorisation | Fournisseurs d'identité et serveurs d'autorisation : Protection des clés cryptographiques<br>Les clés cryptographiques qui protègent les jetons d'accès sont générées, gérées et protégées contre toute divulgation et utilisation inappropriée. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 13(02) | Fournisseurs d'identité et serveurs d'autorisation | Fournisseurs d'identité et serveurs d'autorisation : Vérification des assertions d'identité et des jetons d'accès<br>La source et l'intégrité des assertions d'identité et des jetons d'accès sont vérifiées avant d'accorder l'accès au système et aux ressources d'information. | Contrôle | Non sélectionné | s.o. | s.o. |
| IA | 13(03) | Fournisseurs d'identité et serveurs d'autorisation | Fournisseurs d'identité et serveurs d'autorisation : Gestion des jetons<br>Conformément à la [Affectation : stratégie d'identification et d'authentification définie par l'organisation], les assertions et les jetons d'accès sont<br>a. générés | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | b. diffusés<br>c. actualisés<br>d. révoqués<br>e. limités dans le temps<br>f. limités selon le public cible | | | | |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| IR | 01 | Politique et procédure d'intervention en cas d'incident | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique d'intervention en cas d'incident [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre des politiques d'intervention en cas d'incident et des contrôles d'intervention en cas d'incident connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à l'intervention en cas d'incident<br>C. Passer en revue et mettre à jour, par rapport à l'intervention en cas d'incident,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| IR | 02 | Formation sur les interventions en cas d'incident | A. Fournir une formation pour intervenir en cas d'incident aux utilisatrices et utilisateurs du système en fonction des rôles et des responsabilités attribués<br>1. dans [Affectation : délais définis par l'organisation] après avoir été affecté à un rôle ou à des responsabilités d'intervention en cas d'incident ou après avoir obtenu l'accès au système<br>2. lorsque des changements apportés au système l'exigent<br>3. tous les [Affectation : fréquence définie par l'organisation] par la suite<br>B. Passer en revue et mettre à jour le contenu de la formation sur les interventions en cas d'incident tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 02(01) | Formation sur les interventions en cas d'incident | Formation sur les interventions en cas d'incident : Événements simulés<br>Intégrer des événements simulés à la formation sur les interventions en cas d'incident pour faciliter l'intervention du personnel en situation de crise. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IR | 02(02) | Formation sur les interventions en cas d'incident | Formation sur les interventions en cas d'incident : Environnements de formation automatisée<br>Fournir un environnement de formation sur les interventions en cas d'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 02(03) | Formation sur les interventions en cas d'incident | Formation sur les interventions en cas d'incident : Atteinte à la vie privée<br>Fournir une formation d'intervention en cas d'incident sur la façon d'identifier et d'intervenir lors d'atteintes à la vie privée, y compris le processus qu'utilise l'organisation pour signaler une atteinte à la vie privée. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 03 | Tests d'intervention en cas d'incident | Tester l'efficacité de la capacité d'intervention en cas d'incident pour les systèmes [Affectation : fréquence définie par l'organisation] en utilisant : [Affectation : tests définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 03(01) | Tests d'intervention en cas d'incident | Tests d'intervention en cas d'incident : Tests automatisés<br>Tester la capacité d'intervention en cas d'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 03(02) | Tests d'intervention en cas d'incident | Tests d'intervention en cas d'incident : Coordination avec les plans connexes<br>Coordonner la mise à l'essai des interventions en cas d'incident avec les éléments organisationnels responsables des plans connexes. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 03(03) | Tests d'intervention en cas d'incident | Tests d'intervention en cas d'incident : Amélioration continue<br>Employer des données qualitatives et quantitatives tirées des essais pour<br>a. déterminer l'efficacité des processus d'intervention en cas d'incident<br>b. améliorer de façon continue les processus d'intervention en cas d'incident<br>c. fournir des mesures et des paramètres d'intervention en cas d'incident qui sont conformes, pertinents et dans un format reproductible<br>d. cerner les tendances pour faciliter l'identification de modèles sous-jacents en ce qui a trait aux pratiques de traitement des renseignements pour ainsi éviter que ne surviennent d'autres atteintes à la vie privée | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04 | Traitement des incidents | A. Mettre en œuvre des capacités de traitement pour les incidents alignées sur le plan d'intervention en cas d'incident et y inclure les activités de préparation, de détection, d'analyse, de confinement, d'éradication et de reprise<br>B. Coordonner les activités de traitement des incidents avec les activités de planification d'urgence<br>C. Intégrer les leçons apprises découlant des activités de traitement aux procédures d'intervention en cas d'incident, à la formation et aux tests, et mettre en œuvre les changements qui en résultent comme il se doit<br>D. S'assurer que la rigueur, l'intensité, la portée et les résultats des activités de traitement des incidents sont comparables et prévisibles dans l'ensemble de l'organisation | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 04(01) | Traitement des incidents | Traitement des incidents : Processus de traitement des incidents automatisés<br>Prendre en charge le processus de traitement des incidents au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IR | 04(02) | Traitement des incidents | Traitement des incidents : Reconfiguration dynamique<br>Comprendre les types suivants de reconfiguration dynamique [Affectation : composants du système définis par l'organisation] à sa capacité d'intervention en cas d'incident : [Affectation : types de reconfiguration dynamique définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(03) | Traitement des incidents | Traitement des incidents : Continuité des opérations<br>Identifier les [Affectation : classes d'incident définies par l'organisation] et prendre les mesures d'intervention suivantes pour veiller à la continuité de ses missions et fonctions opérationnelles : [Affectation : mesures d'intervention appropriées aux classes d'incident définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 04(04) | Traitement des incidents | Traitement des incidents : Corrélation de l'information<br>Établir une corrélation entre l'information sur les incidents et les interventions individuelles pour obtenir une perspective organisationnelle de la sensibilisation et des interventions en matière d'incident. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(05) | Traitement des incidents | Traitement des incidents : Désactivation automatique du système<br>Mettre en œuvre une capacité configurable pour désactiver automatiquement le système dans l'éventualité où [Affectation : atteintes à la sécurité définies par l'organisation] étaient détectées. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(06) | Traitement des incidents | Traitement des incidents : Menace interne<br>Mettre en œuvre une capacité de traitement des incidents pour les incidents impliquant des menaces internes. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(07) | Traitement des incidents | Traitement des incidents : Menace interne – Coordination au sein de l'organisation<br>Coordonner des capacités de traitement des incidents pour des menaces internes qui comprennent les entités organisationnelles suivantes [Affectation : entités définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(08) | Traitement des incidents | Traitement des incidents : Corrélation avec les organisations externes<br>Coordonner avec [Affectation : organisations externes définies par l'organisation] en vue d'échanger [Affectation : information liée à un incident définie par l'organisation] de sorte à obtenir une représentation interorganisationnelle de la sensibilisation à l'incident et d'intervenir plus efficacement après celui-ci. | Contrôle | Sélectionné | [SPC, SCT, Centre pour la cybersécurité] | s.o. |
| IR | 04(09) | Traitement des incidents | Traitement des incidents : Capacités d'intervention dynamique<br>Utiliser [Affectation : capacités d'intervention dynamique définies par l'organisation] de sorte à intervenir en cas d'incident. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 04(10) | Traitement des incidents | Traitement des incidents : Coordination relative à la chaîne d'approvisionnement<br>Coordonner les activités d'intervention en cas d'incident touchant aux événements d'approvisionnement avec d'autres organisations dans la chaîne d'approvisionnement. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(11) | Traitement des incidents | Traitement des incidents : Équipe intégrée d'intervention en cas d'incident<br>Établir et maintenir une équipe intégrée d'intervention en cas d'incident qui peut être déployée à tout endroit identifié par l'organisation dans [Affectation : délais définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(12) | Traitement des incidents | Traitement des incidents : Programme malveillant et analyse criminalistique<br>Analyser un programme malveillant ou d'autres artéfacts qui restent dans le système après l'incident. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(13) | Traitement des incidents | Traitement des incidents : Analyse comportementale<br>Analyser un comportement des adversaires anormal ou suspect en lien à des [Affectation : environnements ou ressources définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IR | 04(14) | Traitement des incidents | Traitement des incidents : Centre des opérations de sécurité<br>Établir et tenir à jour un centre des opérations de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 04(15) | Traitement des incidents | Traitement des incidents : Relations publiques, réparation de réputation et notification<br>a. Gérer les relations publiques associées à un incident<br>b. Employer des mesures visant à réparer la réputation d'une organisation<br>c. Le cas échéant, aviser les personnes dont les renseignements personnels ont été compromis | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 05 | Surveillance des incidents | Faire le suivi et documenter les incidents. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 05(01) | Surveillance des incidents | Surveillance des incidents : Suivi, collecte de données et analyses automatisés<br>Faire le suivi des incidents, recueillir et analyser l'information sur l'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 06 | Signalement des incidents | A. Exiger que les membres du personnel signalent les incidents suspects à l'équipe d'intervention en cas d'incident de l'organisation dans [Affectation : délais définis par l'organisation]<br>B. Donner de l'information sur l'incident à [Affectation : autorités désignées par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 06(01) | Signalement des incidents | Signalement des incidents : Signalement automatisé<br>Signaler les incidents au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 06(02) | Signalement des incidents | Signalement des incidents : Vulnérabilités liées aux incidents<br>Signaler les vulnérabilités du système associées aux incidents signalés à [Affectation : personnel ou rôles définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 06(03) | Signalement des incidents | Signalement des incidents : Coordination avec la chaîne d'approvisionnement<br>Fournir de l'information sur les incidents au fournisseur du produit ou du service et aux autres organisations impliquées dans la chaîne d'approvisionnement ou la gouvernance de celle-ci pour les systèmes ou les composants de systèmes liés à l'incident. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 07 | Assistance en cas d'incident | Fournir une ressource de soutien qui fait partie intégrante de la capacité d'intervention en cas d'incident de l'organisation et qui offre conseils et assistance aux utilisatrices et utilisateurs du système pour ce qui touche le traitement et le signalement des incidents. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 07(01) | Assistance en cas d'incident | Assistance en cas d'incident : Soutien automatisé concernant la disponibilité de l'information et du soutien<br>Accroître la disponibilité du soutien et de l'information sur les interventions en cas d'incident au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| IR | 07(02) | Assistance en cas d'incident | Assistance en cas d'incident : Coordination avec les fournisseurs externes<br>a. Établir une relation de coopération directe entre la capacité d'intervention en cas d'incident de l'organisation et la capacité de protection des systèmes de fournisseurs externes<br>b. Communiquer l'identité des membres de son équipe d'intervention en cas d'incident aux fournisseurs externes | Contrôle | Non sélectionné | s.o. | s.o. |
| IR | 08 | Plan d'intervention | A. Élaborer un plan d'intervention en cas d'incident qui<br>1. fournit à l'organisation une feuille de route pour la mise en œuvre de ses capacités d'intervention en cas d'incident<br>2. décrit la structure et l'organisation des capacités d'intervention en cas d'incident | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | en cas d'incident | 3. fournit une approche de haut niveau indiquant comment les capacités d'intervention en cas d'incident s'intègrent à l'organisation en général<br>4. répond à ses exigences spécifiques concernant sa mission, sa taille, sa structure et ses fonctions<br>5. définit les incidents devant être signalés<br>6. définit les paramètres de mesure de sa capacité d'intervention en cas d'incident<br>7. définit les ressources et le soutien de la direction nécessaires au maintien et à l'évolution de la capacité d'intervention en cas d'incident<br>8. décrit les modalités d'échange d'information en cas d'incident<br>9. est examiné et approuvé par [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation]<br>10. élabore explicitement la responsabilité de l'intervention en cas d'incident à l'intention de [Affectation : entités, personnel ou rôles définis par l'organisation]<br>B. Distribuer des copies du plan d'intervention en cas d'incident [Affectation : employées et employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation]<br>C. Mettre à jour le plan d'intervention en cas d'incident afin de tenir compte des changements apportés aux systèmes et des changements organisationnels, ou encore des problèmes rencontrés durant la mise en œuvre, l'exécution ou la mise à l'essai du plan d'intervention<br>D. Communiquer les changements apportés au plan d'intervention en cas d'incident [Affectation : employées et employés (par nom ou rôle) et éléments organisationnels responsables de l'intervention en cas d'incident définis par l'organisation]<br>E. Protéger le plan d'intervention en cas d'incident des divulgations et des modifications non autorisées | | | | |
| IR | 08(01) | Plan d'intervention en cas d'incident | Plan d'intervention en cas d'incident : Atteintes à la vie privée<br>Pour les atteintes à la vie privée touchant des renseignements personnels, il faut inclure ce qui suit dans le plan d'intervention en cas d'incident<br>a. un processus permettant de déterminer s'il est nécessaire de faire un signalement à des personnes ou à d'autres organisations, y compris des organisations de surveillance<br>b. un processus d'évaluation pour déterminer l'étendue des dommages, de l'embarras, de l'injustice ou des désagréments aux personnes touchées et tout mécanisme pour atténuer des tels dommages<br>c. l'identification des exigences en matière de protection de la vie privée applicables | Activité | Non sélectionné | s.o. | s.o. |
| IR | 09 | Intervention en cas de fuite d'information | Réagir aux fuites d'information en<br>A. désignant [Affectation : personnel ou rôles définis par l'organisation] à titre de personnes responsables de l'intervention cas de fuite d'information<br>B. déterminant, de manière précise, quelle information a fait l'objet de la contamination du système<br>C. avertissant [Affectation : personnel ou rôles définis par l'organisation] de la fuite d'information au moyen d'un mode de communication n'étant pas lié à la fuite<br>D. isolant le système ou le composant du système contaminé<br>E. supprimant l'information du système ou le composant du système contaminé<br>F. déterminant si d'autres systèmes ou composants de systèmes avaient pu être contaminés subséquemment<br>G. effectuant les mesures supplémentaires suivantes : [Affectation : actions définies par l'organisation] | Contrôle | Non sélectionné | s.o. | Ce contrôle devrait être sélectionné par les ministères et organismes du GC dont les systèmes sont catégorisés à un niveau supérieur à PROTÉGÉ B. |
| IR | 09(01) | Intervention en cas de fuite d'information | Intervention en cas de fuite d'information : Personnel responsable<br>Annulé : Intégré au contrôle IR-09. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| IR | 09(02) | Intervention en cas de fuite d'information | Intervention en cas de fuite d'information : Formation<br>Offrir une formation sur l'intervention en cas de fuite d'information [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | Ce contrôle devrait être sélectionné par les ministères et organismes du GC dont les systèmes sont catégorisés à un niveau supérieur à PROTÉGÉ B. |
| IR | 09(03) | Intervention en cas de fuite d'information | Intervention en cas de fuite d'information : Opérations à la suite d'une fuite<br>Mettre en œuvre les procédures suivantes afin de veiller à ce que les membres du personnel de l'organisation touchés par les fuites d'information puissent continuer d'exécuter leurs fonctions même si les systèmes contaminés sont en cours d'assainissement : [Affectation : procédures définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | Ce contrôle devrait être sélectionné par les ministères et organismes du GC dont les systèmes sont catégorisés à un niveau supérieur à PROTÉGÉ B. |
| IR | 09(04) | Intervention en cas de fuite d'information | Intervention en cas de fuite d'information : Exposition au personnel non autorisé<br>Employer les contrôles suivants pour les membres du personnel exposés à de l'information ne faisant pas partie des autorisations d'accès accordées : [Affectation : contrôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | Ce contrôle devrait être sélectionné par les ministères et organismes du GC dont les systèmes sont catégorisés à un niveau supérieur à PROTÉGÉ B. |
| IR | 10 | Équipe d'analyse de la sécurité de l'information intégrée | Annulé : Transféré sous le contrôle IR-04(11). | Contrôle | s.o. | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| MA | 01 | Politique et procédures de maintenance des systèmes | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de maintenance [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de maintenance et des contrôles d'accès connexes | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la maintenance<br>C. Passer en revue et mettre à jour, par rapport à la maintenance,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | | | | |
| MA | 02 | Maintenance contrôlée | A. Planifier, exécuter, documenter et examiner les dossiers de maintenance, de réparation et de remplacement des composants de système conformément aux spécifications du fabricant ou du fournisseur ou à ses propres exigences<br>B. Approuver et surveiller toutes les activités de maintenance, qu'elles soient effectuées sur place ou à distance et que le système ou les composants des systèmes soient réparés sur les lieux ou dans un autre emplacement<br>C. Exiger que [Affectation : personnel ou rôles définis par l'organisation] approuve explicitement le retrait du système ou de ses composants, de ses installations aux fins de maintenance, de réparation ou de remplacement à l'extérieur de ses locaux<br>D. Nettoyer l'équipement afin de supprimer les données suivantes des supports connexes avant de l'expédier à l'extérieur aux fins de maintenance, de réparation ou de remplacement : [Affectation : information définie par l'organisation]<br>E. Vérifier tous les contrôles potentiellement concernés pour s'assurer qu'ils continuent de fonctionner adéquatement après les activités de maintenance, de réparation ou de remplacement<br>F. Inclure l'information suivante dans les enregistrements de maintenance organisationnels : [Affectation : information définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 02(01) | Maintenance contrôlée | Maintenance contrôlée : Contenu des enregistrements<br>Annulé : Intégré au contrôle MA-02. | s.o. | s.o. | s.o. | s.o. |
| MA | 02(02) | Maintenance contrôlée | Maintenance contrôlée : Activités de maintenance automatisées<br>a. Planifier, effectuer et documenter les interventions de maintenance, de réparation et de remplacement pour le système au moyen de [Affectation : mécanismes automatisés définis par l'organisation]<br>b. Tenir à jour des dossiers précis et complets de toutes les maintenances, réparations et de tous les remplacements exigés, planifiés, en cours et exécutés | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 03 | Outils de maintenance | A. Approuver, contrôler et surveiller l'utilisation des outils de maintenance des systèmes<br>B. Examiner les outils de maintenance précédemment approuvés [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 03(01) | Outils de maintenance | Outils de maintenance : Inspection des outils<br>Inspecter les outils de maintenance utilisés par le personnel de maintenance pour repérer des modifications incorrectes ou non autorisées. | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 03(02) | Outils de maintenance | Outils de maintenance : Inspection des supports<br>Vérifier les supports où sont stockés les programmes de diagnostic et de test afin de détecter la présence de code malveillant, avant d'utiliser les supports dans les systèmes. | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 03(03) | Outils de maintenance | Outils de maintenance : Prévention des retraits non autorisés<br>Prévenir le retrait non autorisé d'équipements de maintenance contenant de l'information sur l'organisation ou des renseignements personnels en<br>a. s'assurant qu'aucune information sur l'organisation ou aucun renseignement personnel ne se trouve dans l'équipement | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | b. nettoyant ou détruisant l'équipement<br>c. conservant l'équipement dans l'installation<br>d. obtenant une exemption de [Affectation : personnel ou rôles définis par l'organisation] autorisant explicitement le retrait de l'équipement de l'installation | | | | |
| MA | 03(04) | Outils de maintenance | Outils de maintenance : Utilisation restreinte des outils<br>Limiter l'utilisation d'outils de maintenance au personnel autorisé uniquement. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 03(05) | Outils de maintenance | Outils de maintenance : Exécution avec privilège<br>Surveiller l'emploi des outils de maintenance qui sont exécutés avec des privilèges accrus. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 03(06) | Outils de maintenance | Outils de maintenance : Mises à jour logicielles et correctifs<br>Inspecter les outils de maintenance pour s'assurer que les plus récentes mises à jour et derniers correctifs ont été installés. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 04 | Maintenance non locale | A. Approuver et surveiller les activités de maintenance et de diagnostic non locales<br>B. Permettre l'utilisation des outils de télémaintenance et de télédiagnostic seulement si elle est conforme à sa politique et documentée dans le plan de sécurité du système<br>C. Utiliser une authentification robuste lors de l'établissement des sessions de maintenance non locale<br>D. Tenir à jour des dossiers des activités de maintenance non locale et de télédiagnostic<br>E. Mettre fin aux sessions et aux connexions réseau lorsque la maintenance non locale est terminée | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 04(01) | Maintenance non locale | Maintenance non locale : Journalisation et examen<br>a. Journalisation [Affectation : événements vérifiables définis par l'organisation] pour des sessions de maintenance non locale et de télédiagnostic<br>b. Passer en revue les enregistrements de vérification des sessions de maintenance non locale et de télédiagnostic pour détecter un comportement anormal | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 04(02) | Maintenance non locale | Maintenance non locale : Documenter la maintenance non locale<br>Annulé : Intégré aux contrôles MA-01 et MA-04. | s.o. | s.o. | s.o. | s.o. |
| MA | 04(03) | Maintenance non locale | Maintenance non locale : Sécurité et nettoyage comparables<br>a. Exiger que les services de maintenance non locale et de télédiagnostic soient effectués à partir d'un système qui applique une capacité comparable à celle mise en œuvre sur le système cible<br>b. Retirer le composant concerné du système avant l'exécution des activités de maintenance non locale et de télédiagnostic, le nettoyer (en supprimer toute information organisationnelle) et, une fois la réparation effectuée, l'inspecter et le nettoyer à nouveau (pour en éliminer tout logiciel malveillant) avant de le reconnecter au système | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 04(04) | Maintenance non locale | Maintenance non locale : Authentification et séparation des sessions de maintenance<br>Protéger les sessions de maintenance non locale en faisant ce qui suit<br>a. employer [Affectation : authentifiants résistant aux attaques par réinsertion définis par l'organisation]<br>b. séparer les sessions de maintenance des autres sessions avec le système en<br>1) séparant physiquement les chemins de communication<br>2) séparant logiquement les chemins de communication | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 04(05) | Maintenance non locale | Maintenance non locale : Approbations et avis<br>a. Obtenir l'approbation de chaque session de maintenance non locale par [Affectation : personnel ou rôles définis par | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | l'organisation]<br>b. Aviser le personnel ou les rôles suivants de la date et l'heure de la maintenance non locale planifiée : [Affectation : personnel ou rôles définis par l'organisation] | | | | |
| MA | 04(06) | Maintenance non locale | Maintenance non locale : Protection cryptographique<br>Mettre en œuvre des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications liées à la maintenance non locale et au télédiagnostic : [Affectation : mécanismes cryptographiques définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 04(07) | Maintenance non locale | Maintenance non locale : Vérification de la déconnexion<br>Vérifier la fin de la connexion de la session et de la connexion réseau après avoir terminé les sessions de maintenance non locale et de diagnostic. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 05 | Personnel de maintenance | A. Établir un processus d'autorisation du personnel de maintenance et tenir à jour une liste des organisations et du personnel autorisé à effectuer les activités de maintenance<br>B. Vérifier que le personnel non accompagné réalisant des activités de maintenance sur le système dispose des autorisations d'accès nécessaires<br>C. Désigner des membres du personnel de l'organisation qui possèdent les autorisations d'accès et les compétences techniques nécessaires pour superviser les activités de maintenance effectuées par le personnel qui ne possède pas les autorisations d'accès appropriées | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 05(01) | Personnel de maintenance | Personnel de maintenance : Personnes ne détenant pas l'accès approprié<br>a. Mettre en œuvre des procédures pour les membres du personnel de maintenance qui ne possèdent pas la cote de sécurité appropriée; ces procédures comprennent les exigences suivantes<br>1) les membres du personnel de maintenance qui ne possèdent pas les autorisations d'accès, les cotes de sécurité ou les approbations formelles d'accès requises sont escortés et surveillés durant l'exécution des activités de maintenance et de diagnostic sur le système par des employés de l'organisation qui sont pleinement habilités, qui possèdent les autorisations d'accès appropriées et qui sont qualifiés sur le plan technique<br>2) avant que des membres du personnel qui ne possèdent pas les autorisations d'accès, les cotes de sécurité ou les approbations formelles d'accès requises puissent entreprendre les activités de maintenance ou de diagnostic, tous les composants de stockage d'information volatile du système sont nettoyés, et les supports d'information non volatile sont enlevés ou physiquement déconnectés du système puis rangés dans un endroit sûr<br>b. Élaborer et mettre en œuvre [Affectation : contrôles de secours définis par l'organisation] dans l'éventualité où un composant de système ne pourrait pas être nettoyé, supprimé ou débranché du système | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 05(02) | Personnel de maintenance | Personnel de maintenance : Habilitations de sécurité pour les systèmes classifiés<br>Veiller à ce que les personnes qui effectuent des activités de maintenance et de diagnostic sur un système qui traite, stocke et transmet de l'information classifiée possèdent l'habilitation de sécurité et les approbations d'accès officiels au moins équivalant au niveau de sécurité le plus élevé de l'information contenue dans le système et équivalant aux compartiments de cette information. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 05(03) | Personnel de maintenance | Personnel de maintenance : Exigences relatives à la citoyenneté pour les systèmes classifiés<br>Veiller à ce que les personnes qui effectuent des activités de maintenance et de diagnostic sur un système qui traite, stocke et transmet de l'information classifiée soient des citoyennes et citoyens canadiens. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| MA | 05(04) | Personnel de maintenance | Personnel de maintenance : Ressortissantes ou ressortissants étrangers<br>S'assurer que<br>a. des ressortissantes ou ressortissants étrangers habilités ont l'habitude d'exécuter les activités de maintenance et de diagnostic sur des systèmes classifiés seulement lorsque ceux-ci sont possédés et exploités à la fois par le gouvernement canadien et des gouvernements étrangers alliés, ou uniquement par des gouvernements étrangers alliés<br>b. les approbations, les consentements et les modalités opérationnelles détaillées concernant l'emploi de ressortissantes et ressortissants étrangers pour mener des activités de maintenance et de diagnostic sur des systèmes classifiés sont bien documentés dans un protocole d'entente | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 05(05) | Personnel de maintenance | Personnel de maintenance : Maintenance non liée aux systèmes<br>S'assurer que les personnes non accompagnées exécutant des activités de maintenance qui ne sont pas directement liées au système, mais qui sont réalisées à proximité du système, détiennent les autorisations d'accès appropriés. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 06 | Maintenance opportune | Obtenir des services de maintenance et/ou des pièces de rechange pour les [Affectation : composants de systèmes définis par l'organisation] dans les [Affectation : délais définis par l'organisation] qui suivent la panne. | Contrôle | Sélectionné | s.o. | s.o. |
| MA | 06(01) | Maintenance opportune | Maintenance opportune : Maintenance préventive<br>L'organisation effectue la maintenance préventive des [Affectation : composants de systèmes définis par l'organisation] tous les [Affectation : intervalles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 06(02) | Maintenance opportune | Maintenance opportune : Maintenance prévisionnelle<br>Effectuer la maintenance prédictive des [Affectation : composants de systèmes définis par l'organisation] tous les [Affectation : intervalles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 06(03) | Maintenance opportune | Maintenance opportune : Soutien automatisé pour la maintenance prévisionnelle<br>Transférer les données de maintenance prédictive à un système de gestion de la maintenance au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| MA | 07 | Maintenance sur site | Limiter ou interdire la maintenance sur site des [Affectation : systèmes ou composants de systèmes définis par l'organisation] dans les [Affectation : installations de maintenance de confiance définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| MP | 01 | Politique et procédures de protection des supports | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de protection des supports [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de protection des supports et des contrôles de protection | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | des supports connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la protection des supports<br>C. Passer en revue et mettre à jour, par rapport à la protection des supports,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | | | | |
| MP | 02 | Accès aux supports | Restreindre l'accès des [Affectation : types de support numérique et non numérique désignés par l'organisation] aux [Affectation : personnel ou rôles définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 02(01) | Accès aux supports | Accès aux supports : Accès limité automatisé<br>Annulé : Intégré au contrôle MP-04(02). | s.o. | s.o. | s.o. | s.o. |
| MP | 02(02) | Accès aux supports | Accès aux supports : Protection cryptographique<br>Annulé : Intégré au contrôle SC-28(01). | s.o. | s.o. | s.o. | s.o. |
| MP | 03 | Marquage des supports | A. Indiquer sur les supports du système d'information les limites de distribution, les mises en garde concernant la manutention et les mentions de sécurité (le cas échéant) de l'information<br>B. Exempter les [Affectation : types de supports du système définis par l'organisation] de tout marquage s'ils demeurent dans [Affectation : zones contrôlées définies par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 04 | Entreposage des supports | A. Contrôler physiquement et entreposer de façon sécurisée les [Affectation : types de support numérique et non numérique définis par l'organisation] dans les [Affectation : zones contrôlées définies par l'organisation]<br>B. Protéger les types de supports du système définis dans MP-04A jusqu'à ce qu'ils soient détruits ou nettoyés avec de l'équipement, des techniques et des procédures approuvés | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 04(01) | Entreposage des supports | Entreposage des supports : Protection cryptographique<br>Annulé : Intégré au contrôle SC-28(01). | s.o. | s.o. | s.o. | s.o. |
| MP | 04(02) | Entreposage des supports | Entreposage des supports : Accès limité automatisé<br>Limiter l'accès aux zones de stockage des supports et journaliser les tentatives d'accès et l'accès octroyé au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 05 | Transport des supports | A. Protéger et contrôler [Affectation : types de supports de système désignés par l'organisation] durant le transport à l'extérieur des zones contrôlées à l'aide de [Affectation : contrôles définis par l'organisation]<br>B. Demeurer responsable des supports du système durant leur transport hors des zones contrôlées<br>C. Documenter les activités associées au transport des supports du système<br>D. Réserver les activités associées au transport des supports au personnel autorisé | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 05(01) | Transport des supports | Transport des supports : Protection à l'extérieur des zones contrôlées<br>Annulé : Intégré au contrôle MP-05. | s.o. | s.o. | s.o. | s.o. |
| MP | 05(02) | Transport des supports | Transport des supports : Documentation des activités<br>Annulé : Intégré au contrôle MP-05. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| MP | 05(03) | Transport des supports | Transport des supports : Gardiennes et gardiens<br>Faire appel à une gardienne ou un gardien désigné durant le transport des supports du système à l'extérieur des zones contrôlées. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 05(04) | Transport des supports | Transport des supports : Protection cryptographique<br>Annulé : Intégré au contrôle SC-28(01). | s.o. | s.o. | s.o. | s.o. |
| MP | 06 | Nettoyage des supports | A. Nettoyer les [Affectation : supports de système définis par l'organisation] avant leur élimination ou leur transfert hors du contrôle de l'organisation ou aux fins de réutilisation au moyen de [Affectation : techniques et procédures de nettoyage définies par l'organisation]<br>B. Utiliser des mécanismes de nettoyage dont la robustesse et l'intégrité correspondent à la catégorie de sécurité ou à la classification de l'information | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 06(01) | Nettoyage des supports | Nettoyage des supports : Examen, approbation, suivi, documentation et vérification<br>Passer en revue, approuver, suivre, documenter et vérifier le nettoyage des supports et les activités d'élimination. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 06(02) | Nettoyage des supports | Nettoyage des supports : Mise à l'essai du matériel<br>Tester les procédures et l'équipement de nettoyage [Affectation : fréquence définie par l'organisation] pour s'assurer que le nettoyage prévu a bien été réalisé. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 06(03) | Nettoyage des supports | Nettoyage des supports : Techniques non destructives<br>Appliquer un nettoyage des dispositifs de stockage portatifs au moyen de techniques de nettoyage non destructives avant de les connecter au système dans les situations suivantes : [Affectation : liste définie par l'organisation des circonstances où les dispositifs de stockage portatifs doivent être nettoyés]. | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 06(04) | Nettoyage des supports | Nettoyage des supports : Information protégée<br>Annulé : Intégré au contrôle MP-06. | s.o. | s.o. | s.o. | s.o. |
| MP | 06(05) | Nettoyage des supports | Nettoyage des supports : Information classifiée<br>Annulé : Intégré au contrôle MP-06. | s.o. | s.o. | s.o. | s.o. |
| MP | 06(06) | Nettoyage des supports | Nettoyage des supports : Destruction de supports<br>Annulé : Intégré au contrôle MP-06. | s.o. | s.o. | s.o. | s.o. |
| MP | 06(07) | Nettoyage des supports | Nettoyage des supports : Double autorisation<br>Appliquer l'exigence de double autorisation pour le nettoyage des [Affectation : supports de système définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 06(08) | Nettoyage des supports | Nettoyage des supports : Purge ou nettoyage à distance de l'information<br>Fournir la capacité de purger ou de nettoyer l'information à partir de [Affectation : systèmes désignés par l'organisation] [Sélection (un choix) : à distance; selon les modalités suivantes : [Affectation : modalités définies par l'organisation]]. | Contrôle | Sélectionné | [perdus, volés, lors d'une cessation d'emploi] | s.o. |
| MP | 07 | Utilisation des supports | A. [Sélection (un choix) : Limiter, interdire] l'utilisation de [Affectation : types de supports de système désignés par l'organisation] sur les [Affectation : systèmes ou composants de systèmes désignés par l'organisation] au moyen de [Affectation : contrôles définis par l'organisation]<br>B. Interdire dans ses systèmes l'utilisation de dispositifs de stockage portatifs dont la ou le propriétaire est inconnu | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| MP | 07(01) | Utilisation des supports | Utilisation des supports : Interdire l'utilisation sans propriétaire<br>Annulé : Intégré au contrôle MP-07. | s.o. | s.o. | s.o. | s.o. |
| MP | 07(02) | Utilisation des supports | Utilisation des supports : Interdire l'utilisation de supports résistant au nettoyage<br>Interdire l'utilisation de supports résistant au nettoyage dans les systèmes organisationnels. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 08 | Déclassement des supports | A. Établir [Affectation : processus de déclassement des supports du système défini par l'organisation] qui comprend le recours à des mécanismes de déclassement dont la robustesse et l'intégrité correspondent à la catégorie de sécurité ou à la classification de l'information<br>B. Veiller à ce que le processus de déclassement des supports du système corresponde à la catégorie de sécurité et/ou au niveau de classification de l'information à supprimer et des autorisations d'accès des potentiels destinataires de l'information déclassée<br>C. Identifier les [Affectation : supports du système à déclasser définis par l'organisation]<br>D. Employer le processus établi pour déclasser les supports de système | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 08(01) | Déclassement des supports | Déclassement des supports : Documentation du processus<br>Documenter les mesures de déclassement des supports du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 08(02) | Déclassement des supports | Déclassement des supports : Mise à l'essai du matériel<br>Tester les procédures et l'équipement de déclassement [Affectation : fréquence définie par l'organisation] pour s'assurer que les mesures de déclassement ont ben été réalisées. | Contrôle | Non sélectionné | s.o. | s.o. |
| MP | 08(03) | Déclassement des supports | Déclassement des supports : Information protégée<br>Déclasser les supports du système comportant de l'information protégée avant toute diffusion publique. | Contrôle | Sélectionné | s.o. | s.o. |
| MP | 08(04) | Déclassement des supports | Déclassement des supports : Information classifiée<br>Déclasser les supports de système comportant de l'information classifiée avant de les rendre publics sans autorisation d'accès obligatoire. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| PE | 01 | Politique et procédures de protection physique et environnementale | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de protection physique et environnementale [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de protection physique et environnementale ainsi que des contrôles de protection physique et environnementale connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | la diffusion de la politique et des procédures de protection physique et environnementale<br>C. Passer en revue et mettre à jour, par rapport à la protection physique et environnementale,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | | | | |
| PE | 02 | Autorisations d'accès physique | A. Développer, approuver et tenir une liste des personnes disposant d'un accès autorisé à l'installation où se trouvent les systèmes<br>B. Émettre des justificatifs d'identité pour autoriser l'accès à l'installation<br>C. Passer en revue la liste d'accès qui fournit les détails quant aux personnes autorisées à accéder aux installations [Affectation : fréquence définie par l'organisation]<br>D. Retirer les personnes de la liste d'accès aux installations lorsqu'un tel accès n'est plus nécessaire | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 02(01) | Autorisations d'accès physique | Autorisations d'accès physique : Accès par poste ou rôle<br>Autoriser l'accès physique à l'installation qui héberge le système selon le poste ou le rôle de l'employée ou employé. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 02(02) | Autorisations d'accès physique | Autorisations d'accès physique : Deux formes d'identification<br>Exiger deux formes d'identification à partir des documents d'identification suivants pour l'accès aux visiteuses et visiteurs dans l'édifice où se trouvent les systèmes : [Affectation : liste des formes acceptables d'identification définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 02(03) | Autorisations d'accès physique | Autorisations d'accès physique : Accès restreint sans escorte<br>Restreindre les accès sans escorte à l'installation qui héberge le système au personnel qui [Sélection (un choix ou plus) : possède les habilitations de sécurité pour toute l'information contenue dans le système; est formellement autorisé à accéder à toute l'information contenue dans le système; nécessite un accès à toute l'information contenue dans le système; [Affectation : autorisations d'accès physique définies par l'organisation]]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 02(400) | Autorisations d'accès physique | Autorisations d'accès physique : Exigences des cartes d'identité<br>S'assurer que les cartes d'identité respectent les exigences avant leur remise. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 03 | Contrôle d'accès physique | A. Appliquer les autorisations d'accès physique aux [Affectation : points d'entrée et de sortie définis par l'organisation de l'installation où se trouvent les systèmes] des façons suivantes<br>1. vérification des autorisations d'accès avant d'accorder l'accès aux installations<br>2. en contrôlant l'entrée et la sortie de l'installation au moyen de [Sélection (un choix ou plus) : [Affectation : systèmes/dispositifs de contrôle d'accès physique désignés par l'organisation]; mécanismes de protection]<br>B. Tenir des journaux de vérification d'accès physique pour [Affectation : points d'entrée et de sortie définis par l'organisation]<br>C. Contrôler l'accès aux zones au sein de l'installation désignée comme étant accessible au public en mettant en œuvre les contrôles suivants : [Affectation : contrôles d'accès physique définis par l'organisation]<br>D. Accompagner les visiteuses et visiteurs et contrôler leurs activités [Affectation : circonstances définies par l'organisation exigeant que les visiteuses et visiteurs soient accompagnés et qu'il y ait un contrôle de leurs activités]<br>E. Fournir des clés sécurisées, des cartes d'accès, des cadenas, des coffres-forts ou d'autres dispositifs d'accès physique<br>F. Inventaire [Affectation : dispositifs d'accès physique définis par l'organisation] tous les [Affectation : fréquence définie | Contrôle | Sélectionné | s.o. | Selon la *Politique sur la sécurité du gouvernement* du SCT et le *Guide de gestion de l'accès* (GSMGC-006) de la GRC, il convient de restreindre l'accès à l'information et aux zones sensibles. Il faut au moins une zone de travail physique pour traiter ou conserver l'information sensible du GC. Une EMR doit être |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | par l'organisation]<br>G. Modifier les combinaisons et les clés [Affectation : fréquence définie par l'organisation] lorsque des clés sont perdues, lorsque des combinaisons sont compromises ou lorsque des employées et employés en possession de clés ou de cadenas sont transférés ou quittent leur poste<br>H. Retirer l'identifiant de la carte d'accès de la liste ou la base de données des accès [Affectation : fréquence définie par l'organisation] lorsque la carte d'accès est perdue, égarée ou volée, ou lorsque la personne en possession de la carte est transférée ou quitte son poste | | | | effectuée pour assurer un niveau de sécurité physique approprié afin de protéger l'information cotée PROTÉGÉ B et les systèmes d'information qui traitent et conservent ce type de données. Cette zone est un secteur dont l'accès est limité au personnel qui y travaille et aux visiteuses et visiteurs accompagnés comme il se doit par une ou un employé titulaire d'une cote de fiabilité valide; elle doit être indiquée par un périmètre reconnaissable et surveillée périodiquement. |
| PE | 03(01) | Contrôle d'accès physique | Contrôle d'accès physique : Accès au système<br>Appliquer les autorisations d'accès physique au système en plus des contrôles d'accès physique à l'installation qui se trouve dans [Affectation : espaces physiques définis par l'organisation qui contiennent un ou plusieurs composants du système]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 03(02) | Contrôle d'accès physique | Contrôle d'accès physique : Installation et systèmes<br>Effectuer des vérifications de sécurité [Affectation : fréquence définie par l'organisation] au périmètre physique de l'installation ou du système pour détecter toute exfiltration d'information ou retrait de composants de systèmes. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 03(03) | Contrôle d'accès physique | Contrôle d'accès physique : Garde continue<br>Mettre en place des gardiennes et gardiens de sécurité pour contrôler en permanence [Affectation : points d'accès physique définis par l'organisation] de l'installation qui héberge le système. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 03(04) | Contrôle d'accès physique | Contrôle d'accès physique : Contenants verrouillables<br>Utiliser des contenants verrouillables pour protéger [Affectation : composants de système définis par l'organisation] contre les accès physiques non autorisés. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 03(05) | Contrôle d'accès physique | Contrôle d'accès physique : Protection antitrafiquage<br>Employer des [Affectation : technologies antitrafiquage définies par l'organisation] pour [Sélection (un choix ou plus) : détecter; empêcher] le trafiquage physique ou la modification des [Affectation : composants matériels définis par l'organisation] du système. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PE | 03(06) | Contrôle d'accès physique | Contrôle d'accès physique : Tests d'intrusion des installations<br>Annulé : Intégré au contrôle CA-08. | s.o. | s.o. | s.o. | s.o. |
| PE | 03(07) | Contrôle d'accès physique | Contrôle d'accès physique : Barrières physiques<br>Restreindre l'accès au moyen de barrières physiques | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 03(08) | Contrôle d'accès physique | Contrôle d'accès physique : Vestibules de contrôle d'accès<br>Employer des vestibules de contrôle d'accès dans [Affectation : emplacements dans l'installation définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 03(400) | Contrôle d'accès physique | Contrôle d'accès physique : Inspections de sécurité<br>Effectuer des inspections de sécurité dans les installations où de l' 'information ou des biens de nature délicate sont traités ou stockés, ou qui appuient des activités ou des services essentiels. | Contrôle | Sélectionné | s.o. | Propre au GC. |
| PE | 04 | Contrôle d'accès pour la transmission | Contrôler l'accès physique aux [Affectation : lignes de distribution et de transmission du système définies par l'organisation] dans ses installations utilisant les [Affectation : contrôles de sécurité définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 05 | Contrôle d'accès aux dispositifs de sortie | Contrôler l'accès physique aux données transmises par les [Affectation : dispositifs de sortie définis par la ou le propriétaire du système] pour empêcher les personnes non autorisées d'obtenir les données de sortie. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 05(01) | Contrôle d'accès aux dispositifs de sortie | Contrôle d'accès aux dispositifs de sortie : Accès à la sortie par personnes autorisées<br>Annulé : Intégré au contrôle PE-05. | s.o. | s.o. | s.o. | s.o. |
| PE | 05(02) | Contrôle d'accès aux dispositifs de sortie | Contrôle d'accès aux dispositifs de sortie : Associer l'identité des individus<br>Associer l'identité des individus aux données transmises par le dispositif. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 05(03) | Contrôle d'accès aux dispositifs de sortie | Contrôle d'accès aux dispositifs de sortie : Marquage des dispositifs de sortie<br>Annulé : Intégré au contrôle PE-22. | s.o. | s.o. | s.o. | s.o. |
| PE | 06 | Surveillance de l'accès physique | A. Surveiller l'accès physique aux installations où se trouvent les systèmes afin de détecter et d'intervenir en cas d'incident de sécurité physique<br>B. Examiner les journaux d'accès physique tous les [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements ou indications potentielles d'événement définis par l'organisation]<br>C. Coordonner les résultats des examens et des enquêtes avec sa capacité d'intervention en cas d'incident | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PE | 06(01) | Surveillance de l'accès physique | Surveillance de l'accès physique : Alarmes de détection d'intrusion et équipement de surveillance<br>Surveiller l'accès physique aux installations où se trouvent les systèmes au moyen d'alarmes de détection d'intrusion physique et d'équipement de surveillance. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 06(02) | Surveillance de l'accès physique | Surveillance de l'accès physique : Automatisation de la reconnaissance des intrusions et des interventions<br>Reconnaître [Affectation : classes ou types d'intrusions définis par l'organisation] et appliquer [Affectation : mesures d'intervention définies par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 06(03) | Surveillance de l'accès physique | Surveillance de l'accès physique : Surveillance vidéo<br>a. Employer la vidéo surveillance des [Affectation : secteurs opérationnels définis par l'organisation]<br>b. Examiner les enregistrements vidéo [Affectation : fréquence définie par l'organisation]<br>c. Conserver les enregistrements vidéo pendant [Affectation : délais définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 06(04) | Surveillance de l'accès physique | Surveillance de l'accès physique : Surveillance de l'accès physique aux systèmes<br>Surveiller l'accès physique au système en plus de l'accès physique à l'installation qui se trouve dans [Affectation : espaces physiques définis par l'organisation qui contiennent un ou plusieurs composants du système]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 07 | Contrôle des visiteuses et visiteurs | Annulé : Intégré aux contrôles PE-02 et PE-03. | s.o. | s.o. | s.o. | s.o. |
| PE | 08 | Registre des accès des visiteuses et visiteurs | A. Tenir un registre des accès des visiteuses et visiteurs à l'installation où se trouve le système pendant [Affectation : délais définis par l'organisation]<br>B. Examiner le registre des accès des visiteuses et visiteurs [Affectation : fréquence définie par l'organisation]<br>C. Signaler les anomalies dans le registre des accès des visiteuses et visiteurs à [personnel défini par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 08(01) | Registre des accès des visiteuses et visiteurs | Registre des accès des visiteuses et visiteurs : Tenue et examen automatisés du registre<br>Tenir un registre des accès des visiteuses et visiteurs au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 08(02) | Registre des accès des visiteuses et visiteurs | Registre des accès des visiteuses et visiteurs : Registre des accès physiques<br>Annulé : Intégré au contrôle PE-02. | s.o. | s.o. | s.o. | s.o. |
| PE | 08(03) | Registre des accès des visiteuses et visiteurs | Registre des accès des visiteuses et visiteurs : Limitation des éléments liés aux renseignements personnels<br>Limiter les renseignements personnels contenus dans les registres d'accès des visiteuses et visiteurs aux éléments suivants identifiés dans l'évaluation des risques d'atteinte à la vie privée : [Affectation : éléments définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 09 | Équipement et câblage d'alimentation | Protéger l'équipement et le câblage d'alimentation du système contre les dommages et la destruction. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PE | 09(01) | Équipement et câblage d'alimentation | Équipement et câblage d'alimentation : Câblage redondant<br>Employer des chemins de câblage d'alimentation redondant qui sont installés à une distance de [Affectation : distance définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 09(02) | Équipement et câblage d'alimentation | Équipement et câblage d'alimentation : Contrôles de tension automatisés<br>Utiliser des contrôles de tension automatisés pour [Affectation : composants essentiels du système définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 10 | Arrêt d'urgence | A. Pouvoir, en situation d'urgence, couper l'alimentation [Affectation : du système ou des composants individuels connexes désignés par l'organisation]<br>B. Placer des interrupteurs ou des dispositifs d'arrêt d'urgence dans [Affectation : liste définie par l'organisation des emplacements par système ou composant] pour faciliter l'accès au personnel<br>C. Protéger la capacité d'interruption d'urgence de l'alimentation contre toute activation non autorisée | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 10(01) | Arrêt d'urgence | Arrêt d'urgence : Activation accidentelle et non autorisée<br>Annulé : Intégré au contrôle PE-10. | s.o. | s.o. | s.o. | s.o. |
| PE | 11 | Alimentation d'urgence | Prévoir un système d'alimentation sans coupure pour faciliter [Sélection (un choix ou plus) : l'arrêt ordonné du système; le réacheminement du système vers une source d'alimentation de secours à long terme] dans l'éventualité d'une perte de la source d'alimentation principale. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 11(01) | Alimentation d'urgence | Alimentation d'urgence : Source d'alimentation de secours – Capacité opérationnelle minimale<br>Fournir une source d'alimentation de secours au système qui est activé [Sélection (un choix) : manuellement; automatiquement] et qui est capable de maintenir la capacité opérationnelle minimale requise dans l'éventualité d'une perte prolongée de la source d'alimentation principale. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 11(02) | Alimentation d'urgence | Alimentation d'urgence : Source d'alimentation de secours – Autonome<br>Fournir une source d'alimentation de secours au système qui est activé [Sélection (un choix) : manuellement; automatiquement] et qui est<br>a. autonome<br>b. indépendante de toute source d'alimentation externe<br>c. capable de maintenir [Sélection (un choix) : la capacité opérationnelle minimale requise; une capacité opérationnelle totale] dans l'éventualité d'une perte prolongée de la source d'alimentation principale | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 12 | Éclairage de sécurité | Utiliser et entretenir, pour le système, un système automatique d'éclairage de sécurité qui entre en fonction lorsqu'il y a coupure ou interruption de courant et qui éclaire les sorties d'urgence et les chemins d'évacuation dans l'installation. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 12(01) | Éclairage de sécurité | Éclairage de sécurité : Fonctions opérationnelles et de mission essentielles<br>Prévoir l'éclairage de sécurité de toutes les zones de l'installation prenant en charge les fonctions opérationnelles et de mission essentielles. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 13 | Protection contre les incendies | Utiliser et maintenir des dispositifs et systèmes de détection et d'extinction d'incendie alimentés par une source d'énergie indépendante. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PE | 13(01) | Protection contre les incendies | Protection contre les incendies : Systèmes de détection – Activation et avis automatiques<br>Utiliser, pour le système, des dispositifs ou systèmes de détection d'incendie qui s'activent automatiquement et informent [Affectation : personnel ou rôles définis par l'organisation] et [Affectation : intervenantes et intervenants d'urgence désignés par l'organisation] dans l'éventualité d'un incendie. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 13(02) | Protection contre les incendies | Protection contre les incendies : Systèmes d'extinction – Activation et avis automatiques<br>a. Utiliser, pour le système, des dispositifs ou systèmes d'extinction d'incendie qui s'activent automatiquement et informent [Affectation : personnel ou rôles définis par l'organisation] et [Affectation : intervenantes et intervenants d'urgence désignés par l'organisation]<br>b. Utiliser, pour le système, une capacité d'extinction automatique d'incendie lorsque l'installation n'a pas de personnel affecté de façon continue | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 13(03) | Protection contre les incendies | Protection contre les incendies : Extinction automatique d'incendie<br>Annulé : Intégré au contrôle PE-13(02). | s.o. | s.o. | s.o. | s.o. |
| PE | 13(04) | Protection contre les incendies | Protection contre les incendies : Inspections<br>S'assurer que l'installation est [Affectation : fréquence définie par l'organisation] inspectée par des inspectrices et inspecteurs autorisés et qualifiés, et que les problèmes relevés sont corrigés dans les [Affectation : délais définis par l'organisation] suivants. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 13(400) | Protection contre les incendies | Protection contre les incendies : Services d'urgence<br>S'assurer de tenir compte de la capacité en eau nécessaire pour l'extinction d'incendie et d'avoir des délais de réponse efficaces pour les services d'urgence dans le cadre de l'élaboration des stratégies de protection. | Contrôle | Sélectionné | s.o. | Propre au GC |
| PE | 14 | Contrôles environnementaux | A. Maintenir les niveaux [Sélection (un choix ou plus) : de température; d'humidité; de pression; de rayonnement; [Affectation : contrôle environnemental défini par l'organisation]] dans l'installation où se trouve le système à [Affectation : niveaux acceptables définis par l'organisation]<br>B. Surveiller les niveaux des contrôles environnementaux [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 14(01) | Contrôles environnementaux | Contrôles environnementaux : Contrôles automatisés<br>Employer les contrôles environnementaux automatisés dans l'installation pour empêcher des fluctuations du système pouvant être potentiellement préjudiciables : [Affectation : contrôles environnementaux automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 14(02) | Contrôles environnementaux | Contrôles environnementaux : Surveillance avec des alarmes et des notifications<br>Utiliser une surveillance des contrôles environnementaux qui fournit une alarme ou une notification des changements potentiellement préjudiciables pour le personnel ou l'équipement à [Affectation : personnel ou rôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 15 | Protection contre les dégâts d'eau | Protéger le système contre tout dommage causé par une fuite d'eau en recourant à des robinets d'arrêt ou d'isolement accessibles qui fonctionnent adéquatement et dont le personnel concerné connaît l'emplacement. | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 15(01) | Protection contre les dégâts d'eau | Protection contre les dégâts d'eau : Soutien automatisé<br>Détecter la présence d'eau près du système et alerter [Affectation : personnel ou rôles définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PE | 16 | Livraison et retrait | A. Autoriser et contrôler [Affectation : types de composants du système définis par l'organisation] entrant et sortant de l'installation<br>B. Tenir des registres des composants du système | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 17 | Autres lieux de travail | A. Déterminer et documenter les [Affectation : autres lieux de travail définis par l'organisation] que peuvent utiliser les employées et employés<br>B. Employer les contrôles suivants dans d'autres lieux de travail : [Affectation : contrôles définis par l'organisation]<br>C. Évaluer l'efficacité des contrôles dans d'autres lieux de travail<br>D. Fournir aux employées et employés un moyen de communiquer avec le personnel responsable de la sécurité de l'information et de la protiection de la vie privée en cas d'incidents | Contrôle | Sélectionné | s.o. | s.o. |
| PE | 18 | Emplacement des composants du système | Installer les composants du système de manière à réduire au minimum les dommages que pourraient causer [Affectation : risques physiques et environnementaux définis par l'organisation], de même que les possibilités d'accès non autorisé. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 18(01) | Emplacement des composants du système | Emplacement des composants du système : Site de l'installation<br>Annulé : Transféré sous le contrôle PE-23. | s.o. | s.o. | s.o. | s.o. |
| PE | 19 | Fuite d'information | Protéger le système contre les fuites d'information dues à l'émission de signaux électromagnétiques. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 19(01) | Fuite d'information | Fuite d'information : Stratégies et procédures nationales en matière d'émission<br>Protéger les composants du système, les communications de données connexes ainsi que les réseaux conformément aux stratégies et procédures nationales en ce qui a trait aux émissions et à la norme TEMPEST. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 20 | Surveillance et suivi des biens | Utiliser [Affectation : technologies associées à l'emplacement des biens définies par l'organisation] pour procéder au suivi et à la surveillance de l'emplacement et des déplacements des [Affectation : biens définis par l'organisation] dans [Affectation : zones contrôles définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 21 | Protection contre les impulsions électromagnétiques | Employer des [Affectation : mesures de protection définies par l'organisation] contre les dommages causés par des impulsions électromagnétiques pour les [Affectation : systèmes et composants des systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 22 | Marquage des composants | Marquer les [Affectation : composants matériels des systèmes définis par l'organisation] indiquant le niveau d'incidence ou de classification de l'information pouvant être traitée, stockée ou transmise par le composant matériel. | Contrôle | Non sélectionné | s.o. | s.o. |
| PE | 23 | Emplacement de l'installation | A. Prévoir l'emplacement ou le site de l'installation où le système réside en tenant compte des risques physiques et environnementaux<br>B. Dans le cas d'installations existantes, tenir compte des risques physiques et environnementaux dans la stratégie de gestion des risques de l'organisation | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PE | 400 | Environnements à distance et de télétravail | A. Évaluer la sécurité physique des environnements à distance et de télétravail<br>B. Appliquer des exigences appropriées en matière de protection et de stockage pour l'information et les biens<br>C. Utiliser un équipement de sécurité et des dispositifs électroniques approuvés conformément à la catégorisation du matériel | Contrôle | Sélectionné | s.o. | Propre au GC. |
| PE | 400(01) | Environnements à distance et de télétravail | Environnements à distance et de télétravail : Rangement physique d'information et de biens<br>Conserver l'information physique et les biens conformément aux conseils de la GRC et des pratiques de sécurité établies par le ministère. | Contrôle | Sélectionné | s.o. | Propre au GC. |
| PE | 400(02) | Environnements à distance et de télétravail | Environnements à distance et de télétravail : Travail à distance et télétravail à l'étranger<br>Autoriser les demandes de travail à distance ou de télétravail à partir d'emplacements à l'étranger que dans des circonstances exceptionnelles. | Contrôle | Sélectionné | s.o. | Propre au GC. |
| PE | 401 | Centre des opérations de sécurité | Établir et tenir à jour un centre des opérations de sécurité (COS) pour protéger le personnel, la propriété, les biens et l'information de l'organisation par une surveillance et un suivi physiques et techniques. | Contrôle | Sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| PL | 01 | Politique et procédures de planification de la sécurité | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de planification [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, à la jurisprudence, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de planification et des contrôles connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la planification<br>C. Passer en revue et mettre à jour, par rapport à la planification,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| PL | 02 | Plans de sécurité et de protection de la vie privée du système | A. Élaborer des plans de sécurité et de protection de la vie privée pour le système qui<br>1. sont conformes à l'architecture d'entreprise de l'organisation<br>2. définissent explicitement les composants constitutifs du système<br>3. décrivent le contexte opérationnel du système sur le plan des processus liés à la mission et aux activités<br>4. identifient les personnes qui assument des responsabilités et des rôles liés au système | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 5. identifient les types d'informations traitées, stockées et transmises par le système<br>6. définissent la catégorisation de sécurité du système, y compris la justification à l'appui<br>7. décrivent les menaces particulières pour le système qui sont préoccupantes pour l'organisation<br>8. fournissent les résultats de l'évaluation des risques d'atteinte à la vie privée pour les systèmes qui traitent les renseignements personnels<br>9. décrivent l'environnement opérationnel du système ainsi que les dépendances ou les connexions à d'autres systèmes ou à d'autres composants du système<br>10. donnent un aperçu des exigences en matière de contrôle de la sécurité et de la protection de la vie privée du système<br>11. déterminent les bases de référence ou les profils des contrôles pertinents, le cas échéant<br>12. décrivent les contrôles en place ou prévus pour satisfaire aux exigences de sécurité et de protection de la vie privée, y compris la justification des décisions concernant l'adaptation des contrôles<br>13. incluent les déterminations des risques découlant des décisions liées à la conception et à l'architecture de sécurité et de protection de la vie privée<br>14. comprennent des activités liées à la sécurité et à la protection de la vie privée visant le système dont la planification et la coordination doivent être assurées avec [Affectation : personnes ou groupes désignés par l'organisation]<br>15. sont examinés et approuvés par l'autorité responsable ou une représentante ou un représentant désigné avant leur mise en œuvre<br>400. documentent les objectifs organisationnels pour le traitement des renseignements personnels<br>401. définissent les normes de conservation et d'élimination des documents pour les renseignements personnels stockés dans le système<br>B. Distribuer des copies des plans et communiquer les changements qui y sont apportés par la suite aux [Affectation : personnel ou rôles définis par l'organisation]<br>C. Examiner les plans [Affectation : fréquence définie par l'organisation]<br>D. Mettre à jour les plans pour tenir compte des changements apportés au système et à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en œuvre des plans ou des évaluations des contrôles<br>E. Protéger les plans contre les divulgations ou les modifications non autorisées | | | | |
| PL | 02(01) | Plans de sécurité et de protection de la vie privée du système | Plans de sécurité et de protection de la vie privée des systèmes : Concept d'opérations<br>Annulé : Intégré au contrôle PL-07. | s.o. | s.o. | s.o. | s.o. |
| PL | 02(02) | Plans de sécurité et de protection de la vie privée du système | Plans de sécurité et de protection de la vie privée des systèmes : Architecture fonctionnelle<br>Annulé : Intégré au contrôle PL-08. | s.o. | s.o. | s.o. | s.o. |
| PL | 02(03) | Plans de sécurité et de protection de la vie privée du système | Plans de sécurité et de protection de la vie privée des systèmes : Planifier et coordonner avec d'autres entités organisationnelles<br>Annulé : Intégré au contrôle PL-02. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PL | 03 | Mise à jour du plan de sécurité des systèmes | Annulé : Intégré au contrôle PL-02. | s.o. | s.o. | s.o. | s.o. |
| PL | 04 | Règles de conduite | A. Établir et communiquer les règles qui décrivent les responsabilités et le comportement attendu des personnes qui doivent accéder au système en ce qui concerne l'utilisation, la sécurité et la protection de la vie privée de l'information et du système<br>B. Obtenir des personnes devant accéder au système une attestation documentée selon laquelle elles ont lu et compris le document et acceptent de respecter les règles de conduite avant d'obtenir l'accès autorisé à l'information et au système<br>C. Passer en revue et mettre à jour les règles de conduite tous les [Affectation : fréquence définie par l'organisation]<br>D. Exiger que les personnes qui ont accepté de se conformer à une version antérieure des règles de conduite les lisent et les acceptent de nouveau [Sélection (un choix ou plus) : [Affectation : fréquence définie par l'organisation]; lorsque les règles sont révisées ou mises à jour] | Activité | Sélectionné | s.o. | s.o. |
| PL | 04(01) | Règles de conduite | Règles de conduite : Restriction d'utilisation des médias sociaux et des sites et applications externes<br>Tenir compte des restrictions que les règles de conduite imposent sur ce qui suit<br>a. l'utilisation des médias sociaux, des réseaux sociaux et de sites et applications externes<br>b. la publication d'information organisationnelle sur des sites Web publics<br>c. l'utilisation d'identifiants fournis par l'organisation (par exemple, des adresses courriel) et de secrets d'authentification (par exemple, des mots de passe) pour la création de comptes sur des sites et applications externes | Activité | Sélectionné | s.o. | s.o. |
| PL | 05 | Évaluation des facteurs relatifs à la vie privée | Annulé : Intégré au contrôle RA-08. | s.o. | s.o. | s.o. | s.o. |
| PL | 06 | Planification des activités relatives à la sécurité | Annulé : Intégré au contrôle PL-02. | s.o. | s.o. | s.o. | s.o. |
| PL | 07 | Concept d'opérations | A. Élaborer un concept d'opérations (CONOPS) pour le système qui définit comment l'organisation prévoit exploiter le système du point de vue de la sécurité de l'information et de la protection de la vie privée<br>B. Passer en revue et mettre à jour le CONOPS [Affectation : fréquence définie par l'organisation] | Activité | Non sélectionné | s.o. | s.o. |
| PL | 08 | Architecture de sécurité et de protection de la vie privée | A. Élaborer des architectures de sécurité et de protection de la vie privée pour le système qui décrit<br>1. les exigences et l'approche à adopter pour protéger la confidentialité, l'intégrité et la disponibilité de l'information de l'organisation<br>2. les exigences et l'approche à adopter pour traiter les renseignements personnels de manière à limiter les risques d'atteinte à la vie privée des personnes<br>3. la façon dont les architectures sont intégrées à l'architecture d'entreprise et prises en charge par cette dernière<br>4. toutes les hypothèses en lien avec les services et systèmes externes et les interdépendances<br>B. Passer en revue et mettre à jour les architectures [Affectation : fréquence définie par l'organisation] de manière à tenir compte des changements apportés à l'architecture d'entreprise<br>C. Refléter les changements prévus à l'architecture dans les plans de sécurité et de protection de la vie privée, le CONOPS, l'analyse de criticité, les procédures organisationnelles, de même que l'approvisionnement et les acquisitions | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PL | 08(01) | Architecture de sécurité et de protection de la vie privée | Architecture de sécurité et de protection de la vie privée : Défense en profondeur<br>Concevoir les architectures de sécurité et de protection de la vie privée pour le système en adoptant une approche de défense en profondeur qui<br>a. affecte [Affectation : contrôles définis par l'organisation] aux [Affectation : emplacements et couches d'architecture désignés par l'organisation]<br>b. s'assure que les contrôles affectés fonctionnent de façon coordonnée et se renforcent mutuellement | Activité | Non sélectionné | s.o. | s.o. |
| PL | 08(02) | Architecture de sécurité et de protection de la vie privée | Architecture de sécurité et de protection de la vie privée : Diversité des fournisseurs<br>Exiger que les [Affectation : mécanismes de sécurité définis par l'organisation] affectés aux [Affectation : emplacements et couches d'architecture désignés par l'organisation] soient obtenus de différents fournisseurs | Activité | Non sélectionné | s.o. | s.o. |
| PL | 09 | Gestion centrale | Centraliser la gestion des [Affectation : contrôles et processus connexes définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PL | 10 | Sélection de la base de référence | Sélectionner la base de référence des contrôles d'un système. | Activité | Sélectionné | s.o. | s.o. |
| PL | 11 | Adaptation de la base de référence | Adapter la base de référence du contrôle sélectionné en appliquant les mesures d'adaptation indiquées. | Activité | Sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| PM | 01 | Plan du programme de sécurité de l'information | A. Élaborer et diffuser le plan d'un programme de sécurité de l'information panorganisationnel qui<br>1. donne une vue d'ensemble des exigences liées au programme de sécurité et une description des contrôles de gestion du programme de sécurité et des contrôles communs qui ont été mis en place ou que l'on envisage de mettre en place en vue de satisfaire ces exigences<br>2. comprend l'identification et la répartition des rôles, les responsabilités, l'engagement de la direction, la coordination au sein des entités organisationnelles et la conformité<br>3. tient compte de la coordination parmi les entités responsables de la sécurité de l'information dans l'organisation<br>4. est approuvé par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur les activités organisationnelles (ce qui comprend la mission, les fonctions, l'image et la réputation), les biens organisationnels, les individus, les autres organisations et le Canada<br>B. Passer en revue et mettre à jour le plan du programme de sécurité de l'information panorganisationnel [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation]<br>C. Protéger le plan du programme de sécurité de l'information contre les divulgations ou les modifications non autorisées | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 02 | Rôle de leadership du programme de | Nommer une ou un haut fonctionnaire de la gouvernance en matière de sécurité du ministère avec la mission et les ressources nécessaires pour coordonner, développer, mettre en œuvre et tenir à jour un programme de sécurité de l'information panorganisationnel. | Contrôle | Déployé dans l'ensemble de l'organisation. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | sécurité de l'information | | | Non associé à la base de référence. | | |
| PM | 03 | Ressources de sécurité de l'information et de protection de la vie privée | A. Inclure les ressources nécessaires pour mettre en œuvre les programmes de sécurité de l'information et de protection de la vie privée dans les demandes de planification des immobilisations et des investissements et documenter toutes les exceptions à cette exigence<br>B. Préparer la documentation nécessaire pour tenir compte des programmes de sécurité de l'information et de protection de la vie privée dans les demandes de planification des immobilisations et des investissements conformément aux lois, aux décrets, aux directives, aux politiques, à la réglementation et aux normes applicables<br>C. Veiller à ce que les ressources liées à la sécurité de l'information et à la protection de la vie privée soient disponibles pour la dépense comme prévu | Contrôle | Déployé dans l'ensemble de l'organisation.<br>Non associé à la base de référence. | s.o. | s.o. |
| PM | 04 | Processus du plan d'action et des jalons | A. Mettre en œuvre un processus visant à s'assurer que les plans d'action et les jalons associés au programme de sécurité de l'information et de protection de la vie privée, au programme de gestion des risques liés à la chaîne d'approvisionnement et aux systèmes organisationnels connexes<br>1. sont élaborés et tenus à jour<br>2. sont approuvés par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur les activités organisationnelles (ce qui comprend la mission, les fonctions, l'image et la réputation), les biens organisationnels, les individus, les autres organisations et le Canada<br>3. sont mentionnés conformément aux exigences liées à la production de rapports qui ont été établies<br>B. Passer en revue les plans d'action et les jalons pour veiller à ce qu'ils soient uniformes avec la stratégie de gestion des risques de l'organisation et les priorités panorganisationnelles en ce qui a trait aux mesures d'intervention liées aux risques | Activité | Déployé dans l'ensemble de l'organisation.<br>Non associé à la base de référence. | s.o. | s.o. |
| PM | 05 | Inventaire des systèmes et des programmes | Élaborer et tenir à jour [Affectation : fréquence définie par l'organisation] un inventaire des systèmes et des programmes organisationnels. | Contrôle | Déployé dans l'ensemble de l'organisation.<br>Non associé à la base de référence. | s.o. | s.o. |
| PM | 05(01) | Inventaire des systèmes et des programmes | Inventaire des systèmes et des programmes : Inventaire des renseignements personnels<br>Réaliser, tenir et mettre à jour [Affectation : fréquence définie par l'organisation] un inventaire de tous les systèmes, programmes, applications et projets qui traitent des renseignements personnels | Contrôle | Déployé dans l'ensemble de l'organisation.<br>Non associé à la base de référence. | s.o. | s.o. |
| PM | 06 | Mesures du rendement | Développer et surveiller les résultats des mesures du rendement de la sécurité de l'information et de la protection de la vie privée et en faire rapport. | Activité | Déployé dans l'ensemble de l'organisation.<br>Non associé à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PM | 07 | Architecture d'entreprise | Développer une architecture d'entreprise en tenant compte de la sécurité de l'information, de la protection de la vie privée et du risque qui en résulte sur les activités et les biens organisationnels, les individus, les autres organisations et le Canada. | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 07(01) | Architecture d'entreprise | Architecture d'entreprise : Déchargement<br>Décharger les [Affectation : fonctions ou services définis par l'organisation] sur d'autres systèmes, des composants de systèmes ou un fournisseur externe. | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 08 | Plan des infrastructures essentielles | Aborder les problèmes liés à la sécurité de l'information et à la protection de la vie privée qui touchent le développement, la documentation et la mise à jour d'un plan de protection visant les infrastructures essentielles et des ressources clés. | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 09 | Stratégie de gestion des risques | A. Élaborer une stratégie complète de gestion<br>1. des risques pour les activités et les biens organisationnels, les individus, les autres organisations et le Canada associés à l'exploitation et à l'utilisation des systèmes de l'organisation<br>2. des risques d'atteinte à la vie privée qui pèsent sur les personnes dans le cadre du traitement autorisé des renseignements personnels<br>B. Mettre en place la stratégie de gestion des risques uniformément dans l'ensemble de l'organisation<br>C. Passer en revue et mettre à jour la stratégie de gestion des risques [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 10 | Processus d'autorisation | A. Gérer l'état de sécurité et de protection de la vie privée des systèmes organisationnels et des environnements dans lequel ces systèmes s'exécutent dans le cadre des processus d'autorisation<br>B. Désigner les personnes qui assumeront des rôles et des responsabilités, en particulier dans le processus de gestion des risques de l'organisation<br>C. Intégrer les processus d'autorisation au programme panorganisationnel de gestion des risques | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 11 | Définition des processus liés à la mission et aux activités | A. Développer des processus liés à la mission et aux activités de l'organisation en tenant compte de la sécurité de l'information et de la protection de la vie privée et du risque qui en résulte sur les activités et les biens organisationnels, les individus, les autres organisations et le Canada<br>B. Déterminer les besoins en matière de protection de l'information et de traitement des renseignements personnels qui découlent des processus liés à la mission et aux activités qui ont été définis<br>C. Examiner et revoir les processus liés à la mission et aux activités [Affectation : fréquence définie par l'organisation] | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PM | 12 | Programme de protection contre la menace interne | Mettre en place un programme de protection contre la menace interne qui comprend une équipe multidisciplinaire de traitement des incidents liés à la menace interne. | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 13 | Personnel affecté à la sécurité et à la protection de la vie privée | Élaborer un programme de développement et de perfectionnement du personnel affecté à la sécurité et à la protection de la vie privée. | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 14 | Tests, formation et surveillance | A. Mettre en place un processus visant à s'assurer que les plans organisationnels liés à la conduite des activités de mise à l'essai, de formation et de surveillance en matière de sécurité qui sont associées aux systèmes organisationnels<br>1. sont élaborés et tenus à jour<br>2. continuent d'être exécutés<br>B. Passer en revue les plans de mise à l'essai, de formation et de surveillance pour veiller à ce qu'ils soient uniformes avec la stratégie organisationnelle de gestion des risques en matière de sécurité et de protection de la vie privée, et les priorités panorganisationnelles en ce qui a trait aux mesures d'intervention liées aux risques | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 15 | Groupes et associations de sécurité et de protection de la vie privée | Déterminer et institutionnaliser les contacts avec certains groupes et certaines associations de la collectivité de la sécurité pour<br>A. faciliter la formation continue de son personnel en matière de sécurité et de protection de la vie privée<br>B. se tenir au fait des pratiques, des techniques et des technologies recommandées en matière de sécurité et de protection de la vie privée<br>C. échanger de l'information à jour sur la sécurité et la protection de la vie privée, notamment sur les menaces, les vulnérabilités et les incidents | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 16 | Programme de sensibilisation aux menaces | Mettre en œuvre un programme de sensibilisation aux menaces qui comprend une capacité d'échange d'information interorganisationnelle pour le renseignement sur les menaces. | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 16(01) | Programme de sensibilisation aux menaces | Programme de sensibilisation aux menaces : Moyens automatisés pour l'échange de renseignement sur les menaces<br>Avoir recours à des mécanismes automatisés pour maximiser l'efficacité de l'échange de renseignement sur les menaces. | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PM | 17 | Protection de l'information contrôlée sur les systèmes externalisés | A. Établir la stratégie et les procédures nécessaires pour veiller à ce que les exigences relatives à la protection de l'information contrôlée qui est traitée, stockée ou transmise sur des systèmes externes, soient mises en œuvre conformément aux lois, aux décrets, aux directives, aux politiques, à la réglementation et aux normes applicables<br>B. Passer en revue et mettre à jour la stratégie et les procédures tous les [Affectation : fréquence définie par l'organisation] | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 18 | Plan du programme de protection de la vie privée | A. Élaborer et diffuser le plan du programme de protection de la vie privée panorganisationnel, qui offre une vue d'ensemble du programme de protection de la vie privée de l'organisation et<br>1. comprend une description de la structure du programme de prestation des services en matière de protection de la vie privée et des ressources consacrées au programme de protection de la vie privée<br>2. donne une vue d'ensemble des exigences liées au programme de protection de la vie privée et une description des contrôles de gestion du programme de protection de la vie privée et des contrôles communs qui ont été mis en place ou que l'on envisage de mettre en place en vue de satisfaire ces exigences<br>3. comprend le rôle de la ou du haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée approprié, décrit la délégation officielle des pouvoirs de l'administratrice générale ou de l'administrateur général, et établit et affecte les rôles et responsabilités des autres cadres supérieures et supérieurs en matière de protection de la vie privée et de leur personnel<br>4. décrit l'engagement de la direction, les exigences relatives à la conformité, ainsi que les buts et les objectifs du programme de protection de la vie privée<br>5. tient compte de la coordination parmi les entités organisationnelles responsables des différents aspects de la protection de la vie privée<br>6. est approuvé par une ou un cadre supérieur ayant les responsabilités et la reddition de comptes nécessaires pour le risque qui pèse sur la protection de la vie privée des opérations organisationnelles (ce qui comprend la mission, les fonctions, l'image et la réputation), les biens organisationnels, les individus, les autres organisations et le Canada<br>B. Mettre à jour le plan [Affectation : fréquence définie par l'organisation] et tenir compte des changements apportés à l'application des lois fédérales en matière de respect de la vie privée en fonction de la jurisprudence, des changements stratégiques et organisationnels et des problèmes relevés au cours de la mise en œuvre du plan ou des évaluations de contrôle de la protection de la vie privée<br>AA. S'assurer que le plan du programme de protection de la vie privée est communiqué et transmis au personnel responsable de sa mise en œuvre | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 19 | Rôle de leadership du programme de protection de la vie privée | Désigner une ou un haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée et lui conférer les pouvoirs, la mission, les responsabilités et les ressources nécessaires pour coordonner, élaborer et mettre en place les exigences de protection de la vie privée applicables et pour gérer les risques d'atteinte à la vie privée dans le cadre du programme de protection de la vie privée panorganisationnel. | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 20 | Communication des principaux services de protection de la vie privée | Tenir à jour une page Web centrale des ressources sur le site Web principal public de l'organisation, qui sert de source centralisée d'information sur les services de protection de la vie privée de l'organisation et<br>A. permet de s'assurer que le public a accès à une liste des programmes et des services qui collectent et utilisent des renseignements personnels par l'entremise d'Info Source<br>B. veille à ce que les stratégies, les pratiques et les ressources organisationnelles en matière de protection de la vie privée | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | soient publiées dans le Rapport annuel au Parlement sur l'administration de la LPRP<br>C. rend public des adresses courriel et des numéros de téléphone afin que le public puisse fournir une rétroaction et poser des questions aux bureaux de la protection des renseignements personnels concernant les pratiques en matière de respect de la vie privée<br>AA. comprend les résumés des évaluations des facteurs relatifs à la vie privée qui ont été réalisées<br>BB. fournit de l'orientation pour aider les personnes à soumettre une demande d'accès à leurs renseignements personnels, à soumettre une demande de correction officielle de leur dossier ou à déposer une plainte officielle si elles décident de le faire | | base de référence. | | |
| PM | 20(01) | Communication des principaux services de protection de la vie privée | Communication des principaux services de protection de la vie privée : Politiques de protection de la vie privée pour les sites Web, les applications et les services numériques<br>Élaborer et diffuser les politiques de protection de la vie privée sur tous les sites Web externes, les applications mobiles et les autres services numériques si la vie privée des personnes qui visitent les sites Web est à risque S'assurer que les politiques<br>a. sont rédigées dans un langage clair et organisées de manière à faciliter leur compréhension et leur consultation<br>b. fournissent l'information dont le public a besoin pour prendre une décision éclairée sur la pertinence et la façon d'interagir avec l'organisation<br>c. sont mises à jour chaque fois que l'organisation apporte des changements importants aux pratiques qu'elles visent à décrire et incluent l'estampille temporelle pour informer le public de la date des plus récents changements | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 21 | Maintien d'un registre des divulgations | A. Mettre en place les procédures relatives à la divulgation des renseignements personnels et au maintien d'un registre des divulgations, notamment<br>1. la date et les détails de la divulgation<br>2. le poste et l'adresse (ou autres coordonnées) de la personne ou de l'organisation à qui l'information a été divulguée<br>B. Conserver un registre des divulgations pour la période durant laquelle les renseignements personnels sont conservés ou conformément aux normes de gestion de l'' information de l'organisation<br>C. Faire en sorte que le registre des divulgations soit accessible sur demande aux personnes à qui se rapportent les renseignements personnels dans la mesure où la divulgation respecte les exceptions citées dans la LPRP<br>AA. Conclure un contrat, un accord d'échange de renseignements ou une entente d'échange de renseignements pour documenter les mesures de protection appropriées avant toute divulgation de renseignements personnels à un autre programme fédéral ou à une autre entité du secteur public ou privé | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 22 | Gestion de la qualité des renseignements personnels | Élaborer et documenter les stratégies et les procédures panorganisationnelles pour<br>A. assurer l'exactitude, la pertinence, la rapidité et l'exhaustivité des renseignements personnels tout au long du cycle de vie de l'information<br>B. mettre en place un processus de correction des registres qui facilite la correction ou la suppression de renseignements personnels inexacts ou obsolètes<br>C. mettre en place un processus de correction des registres qui facilite la diffusion des avis de renseignements personnels corrigés lorsque de l'information erronée a été divulguée précédemment<br>AA. s'assurer que les procédures de collecte respectent les exigences imposées par les lois applicables<br>BB. documenter toute modification ou tout changement apporté aux renseignements, y compris la date et les sources du changement d'information | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PM | 23 | Comité de gouvernance des données | Mettre en place un comité de gouvernance des données composé de [Affectation : rôles définis par l'organisation] avec [Affectation : responsabilités définies par l'organisation]. | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 24 | Comité de l'intégrité des données | Mettre en place un comité de l'intégrité des données pour<br>A. examiner les propositions visant à organiser un programme d'appariement statistique ou à y participer<br>B. procéder à un examen annuel de tous les programmes d'appariement statistique auxquels l'organisation a pris part | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 25 | Réduction des renseignements personnels utilisés aux fins de tests, de formation et de recherche | A. Élaborer, documenter et mettre en place des stratégies et des procédures qui abordent l'utilisation de renseignements personnels aux fins de test, de formation et de recherche<br>B. Limiter ou réduire la quantité de renseignements personnels utilisés aux fins de test, de formation et de recherche<br>C. Autoriser l'utilisation de renseignements personnels aux fins de tests, de formation et de recherche internes lorsque le résultat requis ne peut être obtenu sans le recours aux renseignements personnels<br>D. Passer en revue et mettre à jour les stratégies et les procédures [Affectation : fréquence définie par l'organisation]<br>AA. Limiter la divulgation des jeux de données contenant des renseignements personnels aux entrepreneures et entrepreneurs externes, dans la mesure du possible | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 26 | Gestion des plaintes | Mettre en place un processus pour la réception et le traitement des plaintes, des préoccupations ou des questions des individus concernant les pratiques de l'organisation en matière de sécurité et de protection de la vie privée, ce qui comprend<br>A. des mécanismes simples à utiliser et facilement accessibles au public<br>B. toute l'information nécessaire pour déposer une plainte<br>C. les mécanismes de suivi nécessaires pour veiller à ce que toutes les plaintes reçues soient examinées et traitées dans les [Affectation : délais définis par l'organisation]<br>D. accuser réception des plaintes, des préoccupations ou des questions des individus dans les [Affectation : délais définis par l'organisation]<br>E. répondre avec discrétion aux plaintes, aux préoccupations ou aux questions des individus dans les [Affectation : délais définis par l'organisation] | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 27 | Génération de rapports concernant la protection de la vie privée | A. Élaborer [Affectation : rapports concernant la protection de la vie privée désignés par l'organisation] et les diffuser<br>1. aux [Affectation : organes d'examen désignés par l'organisation] pour démontrer la responsabilité quant aux mandats de réglementation, ainsi que les mandats conférés par la loi et relatifs aux politiques de protection de la vie privée<br>2. aux [Affectation : responsables désignées ou désignés par l'organisation] et aux autres membres du personnel responsables de surveiller la conformité au programme de protection de la vie privée<br>B. Passer en revue et mettre à jour les rapports [Affectation : fréquence définie par l'organisation]<br>AA. Les ministères et organismes fédéraux doivent faire rapport des détails liés à l'administration de la LPRP au Parlement et au SCT conformément à l'article 72 de la LPRP | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PM | 28 | Cadrage des risques | A. Établir et documenter<br>1. les hypothèses relatives à l'évaluation des risques, aux mesures d'atténuation des risques et à la surveillance des risques<br>2. les contraintes relatives à l'évaluation des risques, aux mesures d'atténuation des risques et à la surveillance des risques<br>3. les priorités et les compromis envisagés par l'organisation pour gérer le risque<br>4. la tolérance au risque de l'organisation<br>B. Distribuer les résultats des activités de cadrage des risques à [Affectation : personnel désigné par l'organisation]<br>C. Passer en revue et mettre à jour les facteurs à considérer sur le plan du cadrage des risques [Affectation : fréquence définie par l'organisation] | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 29 | Rôles de leadership pour le programme de gestion des risques | A. Nommer une ou un cadre supérieur responsable de la gestion des risques pour veiller à ce que les processus organisationnels de gestion de la sécurité de l'information et de la protection de la vie privée soient conformes aux processus de planification stratégique, opérationnelle et budgétaire<br>B. Mettre en place une fonction de gestion des risques pour considérer et analyser le risque d'un point de vue panorganisationnel et s'assurer que la gestion des risques est uniforme à travers l'organisation | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 30 | Stratégie de gestion des risques liés à la chaîne d'approvisionnement | A. Élaborer une stratégie panorganisationnelle pour gérer les risques liés à la chaîne d'approvisionnement associés au développement, à l'acquisition, à la maintenance et à la disposition des systèmes, des composants de systèmes et des services qui s'y rapportent<br>B. Mettre en place la stratégie de gestion des risques liés à la chaîne d'approvisionnement uniformément dans l'ensemble de l'organisation<br>C. Passer en revue et mettre à jour la stratégie de gestion des risques liés à la chaîne d'approvisionnement [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 30(01) | Stratégie de gestion des risques liés à la chaîne d'approvisionnement | Stratégie de gestion des risques liés à la chaîne d'approvisionnement : Fournisseurs d'articles critiques ou essentiels à la mission<br>Identifier, prioriser et évaluer les fournisseurs de technologies, de produits et de services critiques ou essentiels à la mission. | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |
| PM | 31 | Stratégie de surveillance continue | Élaborer une stratégie de surveillance continue panorganisationnelle et mettre en place des programmes de surveillance continue qui tiennent compte de<br>A. l'établissement des mesures panorganisationnelles suivantes qu'il convient de surveiller : [Affectation : mesures définies par l'organisation]<br>B. la mise en place de [Affectation : fréquences de surveillance définies par l'organisation] et de [Affectation : fréquences d'évaluation définies par l'organisation] pour l'efficacité des contrôles<br>C. la surveillance en permanence des mesures définies par l'organisation, conformément à la stratégie de surveillance continue définie par l'organisation<br>D. la corrélation et l'analyse de l'information générée par les évaluations de contrôle et la surveillance<br>E. les mesures d'intervention concernant les résultats qui découlent de l'analyse de l'information<br>F. le signalement de l'état de la sécurité et de la protection de la vie privée du système à [Affectation : personnel ou rôles définis par l'organisation] [Affectation : fréquence définie par l'organisation] | Activité | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PM | 32 | Établissement des objectifs | Analyser les [Affectation : systèmes ou composants de systèmes désignés par l'organisation] qui prennent en charge les fonctions ou les services essentiels à la mission pour s'assurer que les ressources d'information sont utilisées aux fins prévues. | Contrôle | Déployé dans l'ensemble de l'organisation. Non associé à la base de référence. | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| PS | 01 | Politique et procédures de sécurité du personnel | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de sécurité du personnel [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures facilitant la mise en œuvre des politiques de sécurité du personnel et des contrôles de sécurité du personnel connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la sécurité du personnel<br>C. Passer en revue et mettre à jour, par rapport à la sécurité du personnel,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| PS | 02 | Analyse de sécurité des postes | A. Déterminer les exigences en matière de filtrage de sécurité pour tous les postes de l'organisation<br>B. Établir les critères de sélection des personnes occupant ces postes<br>C. Passer en revue et mettre à jour l'exigence en matière de filtrage de sécurité [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| PS | 03 | Filtrage de sécurité du personnel | A. Procéder au filtrage de sécurité des personnes avant de leur accorder l'accès au système<br>B. Effectuer une nouvelle enquête de sécurité lorsque [Affectation : liste définie par l'organisation des conditions qui exigent un nouveau filtrage de sécurité et de la fréquence de ce filtrage, le cas échéant] | Contrôle | Sélectionné | s.o. | s.o. |
| PS | 03(01) | Filtrage de sécurité du personnel | Filtrage de sécurité du personnel : Information classifiée<br>S'assurer que chaque utilisatrice ou utilisateur d'un système qui traite, stocke ou transmet de l'information classifiée a une habilitation et un endoctrinement au plus haut niveau de classification de l'information à laquelle il a accès dans le système. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PS | 03(02) | Filtrage de sécurité du personnel | Filtrage de sécurité du personnel : Endoctrinement officiel<br>S'assurer que chaque utilisatrice ou utilisateur d'un système qui traite, stocke ou transmet des types d'information classifiée pour lesquels il faut suivre une séance d'endoctrinement officielle est officiellement endoctriné pour tous les types d'information pertinents auxquels il a accès sur le système. | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 03(03) | Filtrage de sécurité du personnel | Filtrage de sécurité du personnel : Information exigeant des mesures de protection spéciales<br>Vérifier si les personnes qui accèdent à un système qui traite, stocke ou transmet de l'information exigeant une protection spéciale<br>a. possèdent une autorisation d'accès valide attestée par les fonctions gouvernementales officielles qui leur ont été assignées<br>b. satisfont aux [Affectation : critères additionnels de filtrage de sécurité du personnel définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 03(04) | Filtrage de sécurité du personnel | Filtrage de sécurité du personnel : Exigences relatives à la citoyenneté<br>Vérifier si les personnes qui accèdent à un système qui traite, stocke ou transmet [Affectation : types d'information définis par l'organisation] satisfont aux [Affectation : exigences relatives à la citoyenneté définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 04 | Cessation d'emploi du personnel | Lors de la cessation d'emploi d'une employée ou un employé<br>A. désactiver l'accès au système dans une période de [Affectation : période définie par l'organisation]<br>B. mettre fin ou révoquer tous les authentifiants et les justificatifs d'identité associés à la personne<br>C. effectuer une entrevue de fin d'emploi et mener une discussion sur [Affectation : sujets liés à la sécurité de l'information définis par l'organisation]<br>D. récupérer toutes les propriétés liées à la sécurité et à un système organisationnel<br>E. conserver l'accès à l'information et aux systèmes précédemment contrôlés par la personne concernée | Contrôle | Sélectionné | s.o. | s.o. |
| PS | 04(01) | Cessation d'emploi du personnel | Cessation d'emploi du personnel : Exigences régissant l'après-mandat<br>a. Informer les personnes ayant quitté leur emploi des exigences applicables régissant l'après-mandat auxquelles elles sont tenues par la loi de se conformer pour protéger l'information de l'organisation<br>b. Exiger que les personnes ayant quitté leur emploi signent un avis de reconnaissance des exigences régissant l'après-mandat dans le cadre du processus organisationnel de cessation d'emploi | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 04(02) | Cessation d'emploi du personnel | Cessation d'emploi du personnel : Opérations automatisées<br>Utiliser des [Affectation : mécanismes automatisés définis par l'organisation] pour [Sélection (un choix ou plus) : informer [Affectation : personnel ou rôles définis par l'organisation] des mesures de cessation d'emploi; désactiver l'accès aux ressources des systèmes]. | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 04(400) | Cessation d'emploi du personnel | Cessation d'emploi du personnel : Astreint au secret à perpétuité<br>Transmettre les données sur le formulaire *Registre d'une personne d'un ministère ou organisme mentionné à l'annexe en application de la Loi sur la protection de l'information (LPI)* au Service canadien du renseignement de sécurité (SCRS). | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 05 | Transfert du personnel | A. Examiner et confirmer les exigences opérationnelles liées aux autorisations d'accès physique et logique existantes aux systèmes et aux installations lorsque des employées et employés sont réaffectés ou transférés à d'autres postes au sein de l'organisation<br>B. Amorcer [Affectation : mesures de transfert ou de réaffectation définies par l'organisation] dans les [Affectation : délais définis par l'organisation suivant la prise de mesures de transfert officielles]<br>C. Modifier au besoin les autorisations d'accès afin de tenir compte de toute modification apportée aux exigences opérationnelles en raison d'une réaffectation ou d'un transfert | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | D. Informer [Affectation : personnel ou rôles définis par l'organisation] dans les [Affectation : délais définis par l'organisation] | | | | |
| PS | 05(400) | Transfert du personnel | Transfert du personnel : Autorisation de sécurité<br>a. Accepter la cote de fiabilité ou l'habilitation de la personne lorsque le niveau de celle qui est exigée est équivalent ou inférieur au niveau précédemment accordé<br>b. Refaire le processus de filtrage de sécurité lorsque<br>1) les résultats remontent à plus de cinq ans<br>2) la preuve indique que le filtrage de sécurité n'a pas été fait précédemment conformément à la Norme sur le filtrage de sécurité du SCT<br>3) une dispense de sécurité est jointe à la cote ou à l'autorisation<br>4) les résultats des enquêtes sur l'exécution de la loi et des évaluations de sécurité ont été retirés du dossier de la personne concernée<br>5) des renseignements défavorables figurant au dossier pourraient poser un risque de sécurité pour le ministère ou l'organisme d'arrivée | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 06 | Ententes d'accès | A. Élaborer et documenter les ententes d'accès aux systèmes organisationnels<br>B. Passer en revue et mettre à jour les ententes d'accès [Affectation : fréquence définie par l'organisation]<br>C. S'assurer que les personnes qui ont besoin d'accéder à l'information et aux systèmes de l'organisation<br>1. signent les ententes d'accès appropriées avant qu'on leur accorde l'accès<br>2. signent de nouveau les ententes d'accès pour conserver l'accès aux systèmes de l'organisation lorsque les ententes d'accès sont mises à jour ou [Affectation : fréquence définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| PS | 06(01) | Ententes d'accès | Ententes d'accès : Information exigeant une protection spéciale<br>Annulé : intégré au contrôle PS-03. | s.o. | s.o. | s.o. | s.o. |
| PS | 06(02) | Ententes d'accès | Ententes d'accès : Information classifiée exigeant une protection spéciale<br>S'assurer que l'accès à l'information classifiée exigeant une protection spéciale est accordée uniquement aux personnes qui<br>a. possèdent une autorisation d'accès valide attestée par les responsabilités gouvernementales officielles qui leur ont été conférées<br>b. satisfont aux critères connexes de sécurité du personnel<br>c. ont lu, compris et signé une entente de non-divulgation | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 06(03) | Ententes d'accès | Ententes d'accès : Exigences régissant l'après-mandat<br>a. Informer les employées et employés des exigences applicables régissant l'après-mandat auxquelles elles sont tenues par la loi de se conformer pour protéger l'information de l'organisation<br>b. Exiger que les employées et employés attestent par écrit de ces exigences, le cas échéant, au moment d'accorder l'accès à l'information concernée | Contrôle | Non sélectionné | s.o. | s.o. |
| PS | 07 | Sécurité du personnel externe | A. Définir les exigences liées à la sécurité du personnel, y compris les rôles et responsabilités des fournisseurs externes<br>B. Exiger que les fournisseurs externes se conforment aux stratégies et aux procédures en matière de sécurité du personnel mises en place par l'organisation<br>C. Documenter les exigences en matière de sécurité du personnel<br>D. Exiger que les fournisseurs externes informent [Affectation : personnel ou rôles définis par l'organisation] du transfert ou de la cessation d'emploi de toute employée ou tout employé de tierces parties qui possède des justificatifs d'identité | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | et/ou des laissez-passer de l'organisation, ou dispose de privilèges d'accès au système dans les [Affectation : délais définis par l'organisation]<br>E. Surveiller la conformité des fournisseurs aux exigences en matière de sécurité du personnel<br>AA. S'assurer que les organisations et les personnes du secteur privé qui ont accès à l'information, aux installations et aux biens protégés et classifiés font l'objet d'un filtrage de sécurité, conformément à la Norme sur le filtrage de sécurité du SCT<br>BB. Définir explicitement la surveillance gouvernementale et les rôles et responsabilités d'utilisatrice finale ou utilisateur final relativement aux services fournis par des tiers, conformément à la publication du SCT, *Directive sur la gestion de la sécurité – Annexe F : Procédures obligatoires relatives aux mesures de sécurité lors de l'octroi de contrats et d'autres ententes* | | | | |
| PS | 08 | Sanctions imposées au personnel | A. Utiliser un processus formel de sanctions pour le personnel qui ne se conforme pas aux stratégies et aux procédures de sécurité de l'information et de protection de la vie privée qui ont été établies<br>B. Informer [Affectation : personnel ou rôles définis par l'organisation] dans les [Affectation : délais définis par l'organisation] lorsque le processus formel de sanctions est amorcé et indique qui est l'employée ou employé sanctionné et les motifs de la sanction | Contrôle | Sélectionné | s.o. | s.o. |
| PS | 09 | Descriptions de poste | Intégrer les rôles et les responsabilités en matière de sécurité et de protection de la vie privée aux descriptions de postes de l'organisation. | Activité | Sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| PT | 01 | Politique et procédures de traitement des renseignements personnels et de transparence | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de protection de la vie privée et des procédures de traitement des renseignements personnels [Sélection (un choix ou plus) : au niveau de l'organisation; au niveau des processus de la mission et des activités; au niveau du système] qui<br>a. définissent les objectifs, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et les obligations en matière de conformité<br>b. sont conformes aux lois, à la jurisprudence, aux directives, à la réglementation, aux politiques, aux directives, aux normes et aux lignes directrices applicables<br>2. les procédures visant à faciliter la mise en œuvre de la politique de protection de la vie privée et des procédures de traitement des renseignements personnels, ainsi que les contrôles de traitement des renseignements personnels et de transparence connexes<br>B. Déléguer la responsabilité à [Affectation : responsable désignée ou désigné par l'organisation] pour élaborer, documenter et communiquer la politique et les procédures de traitement de renseignements personnels et de transparence<br>C. Passer en revue et mettre à jour, par rapport au traitement des renseignements personnels et de la transparence,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation] | Activité | Non attribué à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 2. les procédures de traitement des renseignements personnels, dont les exigences en matière de transparence, [Affectation : fréquence définie par l'organisation] et à la suite de [Affectation : événements définis par l'organisation] | | | | |
| PT | 02 | Pouvoir en matière de collecte et d'utilisation de renseignements personnels | A. Déterminer et documenter [Affectation : autorité définie par l'organisation] qui permet [Affectation : collecte et utilisation définies par l'organisation] des renseignements personnels<br>B. Limiter [Affectation : collecte et utilisation définies par l'organisation] des renseignements personnels à ce qui est autorisé seulement | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 02(01) | Pouvoir en matière de collecte et d'utilisation de renseignements personnels | Pouvoir en matière de collecte et d'utilisation de renseignements personnels : Étiquetage des données<br>Joindre les étiquettes des données contenant [Affectation : traitement autorisé défini par l'organisation] aux [Affectation : éléments de renseignements personnels définis par l'organisation]. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 02(02) | Pouvoir en matière de collecte et d'utilisation de renseignements personnels | Pouvoir en matière de collecte et d'utilisation de renseignements personnels : Automatisation<br>Gérer l'application du traitement autorisé des renseignements personnels au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 03 | Traitement, utilisation et divulgation de renseignements personnels | A. Reconnaître et documenter les [Affectation : utilisations et divulgations définies par l'organisation] associées aux collectes de renseignements personnels<br>B. Décrire le ou les buts de la collecte dans les énoncés sur la protection de la vie privée et les stratégies de l'activité du programme ou de l'organisation<br>C. Limiter les [Affectation : utilisations et divulgations définies par l'organisation] des renseignements personnels à ce qui est compatible avec les fins mentionnées ou autorisées dans la LPRP<br>D. Surveiller les changements apportés au traitement des renseignements personnels et mettre en place les [Affectation : mécanismes définis par l'organisation] pour s'assurer que tous les changements sont apportés conformément à [Affectation : exigences prévues par la loi identifiées]<br>AA. Mettre à jour le FRP et informer le Commissariat à la protection de la vie privée du Canada (CPVP) et le SCT de la nouvelle utilisation ou divulgation | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 03(01) | Traitement, utilisation et divulgation de renseignements personnels | Traitement, utilisation et divulgation de renseignements personnels : Étiquetage des données<br>Joindre les étiquettes des données contenant les objectifs des [Affectation : éléments définis par l'organisation] suivants : [Affectation : objectifs en matière de traitement définis par l'organisation]. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 03(02) | Traitement, utilisation et divulgation de | Traitement, utilisation et divulgation de renseignements personnels : Automatisation<br>Assurer le suivi du traitement des renseignements personnels au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | renseignements personnels | | | | | |
| PT | 04 | Consentement | A. S'assurer que le consentement est obtenu par écrit ou est adéquatement documenté, y compris l'information comme la date et l'heure de consentement<br>B. Dans le gouvernement fédéral, mettre en place [Affectation : outils ou mécanismes désignés par l'organisation] afin que les individus puissent fournir un consentement éclairé pour les utilisations secondaires ou la collecte indirecte de leurs renseignements personnels. Le consentement doit comprendre<br>1. l'objectif du consentement<br>2. les éléments de renseignements personnels concernés<br>3. dans le cas d'une collecte indirecte, les sources qui seront exigées pour fournir l'information, ainsi que la raison pour laquelle il s'agit d'une collecte indirecte<br>4. les utilisations ou les divulgations qui ne respectent pas l'objectif initial de la collecte et pour lesquelles le consentement est demandé<br>5. toute conséquence qui pourrait résulter du refus d'accorder le consentement<br>6. toute alternative à l'accord du consentement<br>C. Dans le secteur privé, mettre en place [Affectation : outils ou mécanismes désignés par l'organisation] afin que les individus puissent fournir un consentement valable pour la collecte, l'utilisation et la divulgation de leurs renseignements personnels | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 04(01) | Consentement | Consentement : Consentement adapté au gouvernement du Canada<br>Fournir les [Affectation : mécanismes désignés par l'organisation] pour permettre aux individus d'adapter les autorisations de traitement aux éléments sélectionnés des renseignements personnels. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 04(02) | Consentement | Consentement : Consentement opportun<br>Présenter les [Affectation : mécanismes de consentement désignés par l'organisation] aux individus [Affectation : fréquence définie par l'organisation] et parallèlement à [Affectation : traitement des renseignements personnels défini par l'organisation]. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 04(03) | Consentement | Consentement : Révocation<br>Mettre en place [Affectation : outils ou mécanismes désignés par l'organisation] afin que les individus puissent retirer leur consentement au traitement de leurs renseignements personnels. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 04(400) | Consentement | Consentement : Consentement adapté au secteur privé<br>Fournir les [Affectation : mécanismes désignés par l'organisation] pour permettre aux individus d'adapter les autorisations de traitement aux éléments sélectionnés des renseignements personnels. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 05 | Énoncé de confidentialité | Informer les individus de la collecte de leurs renseignements personnels, ce qui comprend<br>A. l'autorisation légale de collecter les renseignements personnels<br>B. les conséquences juridiques et administratives de tout refus de fournir des renseignements personnels<br>C. le droit de protection des renseignements personnels et le droit d'y accéder et de faire des demandes de correction<br>D. un avertissement indiquant que l'utilisation du système peut être surveillée, enregistrée et sujette à une vérification et qu'elle inclut<br>1. un énoncé expliquant les pratiques de surveillance régulières des réseaux électroniques<br>2. un énoncé expliquant que les réseaux électroniques seront surveillés à des fins professionnelles<br>3. un énoncé indiquant qu'une surveillance spéciale peut être autorisée sans préavis si une utilisation illégale ou | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | inacceptable est soupçonnée<br>E. une explication de la manière dont les renseignements seront utilisés<br>F. le droit de déposer une plainte auprès du Commissariat à la protection de la vie privée du Canada concernant le traitement par les institutions des renseignements personnels des individus<br>G. la référence au FRP pertinent, le cas échéant | | | | |
| PT | 05(01) | Énoncé de confidentialité | Énoncé de confidentialité : Énoncés de confidentialité opportuns<br>Présenter l'énoncé du traitement des renseignements personnels aux individus lorsqu'ils fournissent leurs renseignements personnels [Affectation : fréquence définie par l'organisation]. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 05(02) | Énoncé de confidentialité | Énoncé de confidentialité : Avis et énoncés de confidentialité<br>Inclure les avis et énoncés de confidentialité sur les formulaires servant à collecter l'information qui sera conservée dans un fichier de renseignements personnels (FRP). | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 06 | Fichiers de renseignements personnels | Les activités du programme qui collectent des renseignements personnels doivent consigner et publier un FRP si de tels renseignements ont été utilisés, sont utilisés ou peuvent être utilisés à des fins administratives, ou si leur organisation ou leur récupération est effectuée en fonction du nom d'un individu ou au moyen d'un numéro d'identification, d'un symbole ou de tout autre élément particulier attribué à un individu. Les [Affectation : rôles ou personnel définis par l'organisation] sont responsables de ce qui suit<br>A. enregistrer ou soumettre de nouveaux FRP ou des FRP considérablement modifiés conformément à la *Directive sur les pratiques relatives à la protection de la vie privée* du SCT au moyen du formulaire de soumission des fichiers de renseignements personnels fourni par le SCT<br>B. publier les FRP sur la page Info Source pertinente de l'institution et mettre à jour l'information chaque année<br>C. faire en sorte que les FRP soient précis, à jour et pris en compte conformément à la politique | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 06(01) | Fichiers de renseignements personnels | Fichiers de renseignements personnels : Usages et divulgations compatibles<br>Passer en revue tous les usages compatibles publiés dans le FRP [Affectation : fréquence définie par l'organisation] pour assurer une exactitude continue et veiller à ce que les usages compatibles continuent de correspondre aux fins pour lesquelles l'information a été collectée. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 06(02) | Fichiers de renseignements personnels | Fichiers de renseignements personnels : Fichiers inconsultables<br>Passer en revue tous les FRP qui ont été désignés comme étant des fichiers consultables selon l'article 18 de la LPRP [Affectation : fréquence définie par l'organisation] pour s'assurer qu'ils sont toujours appropriés et nécessaires en vertu de la loi. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 07 | Renseignements personnels particulièrement sensibles | Appliquer [Affectation : conditions de traitement définies par l'organisation] aux renseignements personnels particulièrement sensibles. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 07(01) | Renseignements personnels particulièrement sensibles | Renseignements personnels particulièrement sensibles : Numéros d'assurance sociale<br>Si un programme ou une activité collecte, utilise ou divulgue des numéros d'assurance sociale (NAS)<br>a. s'assurer d'avoir l'autorisation expresse de collecter et d'utiliser le NAS<br>b. fournir un énoncé au point de collecte concernant l'autorisation de collecter ainsi que l'utilisation ou la divulgation anticipée du NAS<br>c. s'assurer que la collecte et l'utilisation du NAS sont comprises dans le FRP connexe, le cas échéant | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| PT | 07(02) | Renseignements personnels particulièrement sensibles | Renseignements personnels particulièrement sensibles : *Charte canadienne des droits et libertés*<br>Limiter le traitement de l'information décrivant la façon dont un individu exerce ses droits garantis par la *Charte des droits et libertés* du Canada à moins qu'il n'existe une autorité légitime ou qu'un traitement soit effectué dans le cadre d'une activité autorisée d'application de la loi. | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 07(400) | Renseignements personnels particulièrement sensibles | Renseignements personnels particulièrement sensibles : Secteur privé<br>Au moment de collecter, d'utiliser ou de divulguer des renseignements personnels particulièrement sensibles, les organisations du secteur privé devraient<br>a. déterminer la forme de consentement à utiliser selon la sensibilité de l'information<br>b. protéger les renseignements personnels avec les [Affectation : outils ou mécanismes désignés par l'organisation] appropriés à la sensibilité de l'information | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |
| PT | 08 | Exigences de couplage de données | Lorsqu'une activité d'un programme vise à collecter, à utiliser ou à divulguer des renseignements personnels afin de mener une activité de couplage de données<br>A. s'assurer que les autorisations nécessaires sont en place pour collecter, utiliser ou divulguer les renseignements personnels aux fins de couplage des données<br>B. élaborer et établir une entente ou un accord d'échange de renseignements aux fins de couplage des données<br>C. vérifier que [Sélection (un choix) : l'avis envoyé à l'individu; le consentement obtenu de l'individu] indique que les renseignements seront utilisés dans le cadre d'activités de couplage des données<br>D. vérifier que le FRP connexe indique que les renseignements seront utilisés dans le cadre d'activités de couplage des données | Contrôle | Non attribué à la base de référence. | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| RA | 01 | Politique et procédures d'évaluation des risques | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique d'évaluation des risques [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique d'évaluation des risques et des contrôles d'évaluation des risques connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à l'évaluation des risques<br>C. Passer en revue et mettre à jour, par rapport à l'évaluation des risques,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | | | | |
| RA | 01(400) | Politique et procédures d'évaluation des risques | Stratégie et procédures d'évaluation des risques : Évaluations des facteurs relatifs à la vie privée<br>Développer un processus d'évaluation des facteurs relatifs à la vie privée (EFVP) avec procédures connexes, qui<br>a. est établi par les responsables des institutions du GC<br>b. tient compte de la responsabilité de l'institution en ce qui a trait à l'établissement des fichiers de renseignements personnels (FRP)<br>c. est proportionnel à la gravité des préjudices potentiels associés au niveau de risque d'entrave à la vie privée lié aux programmes et aux activités de l'institution<br>d. s'assurer que l'EFVP est effectuée par la ou le haut fonctionnaire ou cadre supérieur en matière de protection de la vie privée qui est responsable des programmes ou des activités qui sont ajoutés ou considérablement modifiés au sein de l'institution | Activité | Non sélectionné | s.o. | s.o. |
| RA | 02 | Catégorisation de la sécurité | A. Catégoriser le système et l'information qu'il traite, stocke et transmet<br>B. Documenter les résultats de la catégorisation de la sécurité, y compris les justifications, dans le plan de sécurité du système<br>C. S'assurer que l'autorité responsable ou sa représentante ou son représentant désigné examine et approuve la décision relative à la catégorisation de la sécurité | Contrôle | Sélectionné | s.o. | s.o. |
| RA | 02(01) | Catégorisation de la sécurité | Catégorisation de la sécurité : Hiérarchisation des répercussions<br>Procéder à la hiérarchisation des répercussions liées aux systèmes de l'organisation pour obtenir une plus grande granularité des niveaux d'incidence sur les systèmes. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 03 | Évaluation des risques | A. Mener une évaluation des risques, y compris<br>1. identifier les menaces et les vulnérabilités dans le système<br>2. déterminer la probabilité et l'ampleur estimée des préjudices qui pourraient être associés à l'utilisation, à la divulgation, à l'interruption, à la modification et à l'accès non autorisés ou encore à la destruction du système, de l'information qu'il traite, stocke ou transmet, ou toute information connexe<br>3. déterminer la probabilité et l'incidence de répercussions négatives sur les individus qui peuvent découler du traitement des renseignements personnels<br>B. Intégrer les résultats de l'évaluation des risques et les décisions liées à la gestion des risques du point de vue de l'organisation et du processus lié à la mission et aux activités aux évaluations des risques au niveau du système<br>C. Documenter les résultats de l'évaluation des risques dans [Sélection (un choix) : des plans de sécurité et de protection de la vie privée; un rapport d'évaluation des risques; [Affectation : document défini par l'organisation]]<br>D. Examiner les résultats de l'évaluation des risques [Affectation : fréquence définie par l'organisation]<br>E. Communiquer les résultats de l'évaluation des risques aux [Affectation : personnel ou rôles définis par l'organisation]<br>F. Mettre à jour l'évaluation des risques [Affectation : fréquence définie par l'organisation] ou chaque fois que des changements importants sont apportés au système ou à l'environnement d'exploitation, ou encore lorsque d'autres conditions sont susceptibles d'influer sur l'état de sécurité et de protection de la vie privée du système | Contrôle | Sélectionné | s.o. | s.o. |
| RA | 03(01) | Évaluation des risques | Évaluation des risques : Évaluation des risques liés à la chaîne d'approvisionnement<br>a. Évaluer les risques liés à la chaîne d'approvisionnement associés à [Affectation : systèmes, composants de systèmes et services qui s'y rapportent désignés par l'organisation]<br>b. Mettre à jour l'évaluation des risques liés à la chaîne d'approvisionnement [Affectation : fréquence définie par l'organisation], lorsque des changements importants sont apportés à la chaîne d'approvisionnement pertinente ou lorsque | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | des changements sont apportés au système ou aux environnements d'exploitation ou d'autres conditions nécessitent qu'un changement soit apporté à la chaîne d'approvisionnement | | | | |
| RA | 03(02) | Évaluation des risques | Évaluation des risques : Utilisation du renseignement de toutes sources<br>Utiliser du renseignement de toutes sources pour faciliter l'analyse du risque. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 03(03) | Évaluation des risques | Évaluation des risques : Sensibilisation aux menaces dynamiques<br>Déterminer l'environnement de cybermenaces actuel sur une base régulière au moyen de [Affectation : moyens définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 03(04) | Évaluation des risques | Évaluation des risques : Cybernanalyse prédictive<br>Faire appel aux capacités d'automatisation et d'analyse avancées suivantes pour prédire et identifier les risques qui pèsent sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] : [Affectation : capacités d'automatisation et d'analyse avancées définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 04 | Mise à jour de l'évaluation des risques | Annulé : Intégré au contrôle RA-03. | s.o. | s.o. | s.o. | s.o. |
| RA | 05 | Surveillance et analyse des vulnérabilités | A. Surveiller et analyser les vulnérabilités dans le système et les applications hébergées [Affectation : fréquence définie par l'organisation ou de manière aléatoire conformément au processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système sont identifiées et signalées<br>B. Utiliser des outils et des techniques de surveillance des vulnérabilités qui facilitent l'interopérabilité et automatisent les composantes du processus de gestion des vulnérabilités en appliquant des normes sur<br>1. les relevés des plateformes, des lacunes logicielles et des configurations inappropriées<br>2. le formatage des listes de vérification et des procédures de test<br>3. la mesure de l'incidence des vulnérabilités<br>C. Analyser les rapports d'analyse des vulnérabilités et les résultats de la surveillance des vulnérabilités<br>D. Corriger les vulnérabilités légitimes [Affectation : temps de réponse défini par l'organisation] conformément à l'évaluation des risques de l'organisation<br>E. Communiquer l'information découlant du processus de surveillance des vulnérabilités et des évaluations des contrôles à [Affectation : personnel ou rôles définis par l'organisation] pour faciliter l'élimination de vulnérabilités semblables dans les autres systèmes<br>F. Employer des outils de surveillance des vulnérabilités qui sont dotés de la capacité de mettre à jour rapidement les vulnérabilités à analyser | Contrôle | Sélectionné | s.o. | s.o. |
| RA | 05(01) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Mise à jour de la capacité des outils<br>Annulé : Intégré au contrôle RA-05. | s.o. | s.o. | s.o. | s.o. |
| RA | 05(02) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Mise à jour de la liste de vulnérabilités à analyser<br>Mettre à jour le registre des vulnérabilités des systèmes [Sélection (un choix ou plus) : [Affectation : fréquence définie par l'organisation]; avant une nouvelle analyse; lorsque de nouvelles vulnérabilités sont identifiées et signalées]. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| RA | 05(03) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Étendue et profondeur de la couverture<br>Définir l'étendue et la profondeur de la couverture de l'analyse des vulnérabilités. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 05(04) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Information découvrable<br>Déterminer l'information relative au système qui est découvrable et prendre [Affectation : mesures correctives définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 05(05) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Accès privilégiés<br>Mettre en œuvre l'autorisation des accès privilégiés aux [Affectation : composants de systèmes désignés par l'organisation] pour [Affectation : activités d'analyse des vulnérabilités définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| RA | 05(06) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Automatisation des analyses de tendances<br>Comparer les résultats de multiples analyses des vulnérabilités au moyen de [Affectation : mécanismes automatisés désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 05(07) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Automatisation de la détection et du signalement des composants non autorisés<br>Annulé : Intégré au contrôle CM-08. | s.o. | s.o. | s.o. | s.o. |
| RA | 05(08) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Examiner les journaux de vérification historiques<br>Examiner les journaux de vérification historiques pour déterminer si une vulnérabilité identifiée dans [Affectation : système désigné par l'organisation] a été exploitée précédemment au cours de [Affectation : période définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 05(09) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Tests d'intrusion et analyses<br>Annulé : Intégré au contrôle CA-08. | s.o. | s.o. | s.o. | s.o. |
| RA | 05(10) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Corrélation de l'information tirée des analyses<br>Établir une corrélation entre les résultats produits par les outils d'analyse des vulnérabilités dans le but de déceler la présence de vecteurs d'attaque visant plusieurs vulnérabilités ou se déplaçant sur plusieurs bonds. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 05(11) | Surveillance et analyse des vulnérabilités | Surveillance et analyse des vulnérabilités : Programme de divulgation publique<br>Mettre en place un canal de signalement public pour la soumission de rapports de vulnérabilités touchant les systèmes et les composants de systèmes de l'organisation. | Contrôle | Sélectionné | s.o. | s.o. |
| RA | 06 | Dépistage des contre-mesures de surveillance technique | Avoir recours à un dépistage des contre-mesures de surveillance technique aux [Affectation : lieux définis par l'organisation] [Sélection (un choix ou plus) : [Affectation : fréquence définie par l'organisation]; lorsque les événements suivants se produisent : [Affectation : événements ou indicateurs définis par l'organisation]]. | Contrôle | Non sélectionné | s.o. | s.o. |
| RA | 07 | Réponse aux risques | Répondre aux conclusions tirées des évaluations de la sécurité et de la protection de la vie privée, de la surveillance et des vérifications conformément à la tolérance aux risques de l'organisation. | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| RA | 08 | Évaluations des facteurs relatifs à la vie privée | Effectuer des EFVP pour les systèmes, les programmes et les autres activités au moment de<br>A. concevoir, développer ou livrer des moyens de traiter les renseignements personnels<br>B. procéder à une nouvelle collecte des renseignements personnels<br>AA. apporter des modifications importantes aux systèmes, aux programmes ou aux activités lorsque des renseignements personnels sont traités | Activité | Non sélectionné | s.o. | s.o. |
| RA | 09 | Analyse de criticité | Déterminer les composants et les fonctions des systèmes en procédant à une analyse de criticité de [Affectation : systèmes, composants de systèmes ou services qui s'y rapportent désignés par l'organisation] à [Affectation : points de décision du cycle de développement des systèmes définis par l'organisation]. | Activité | Sélectionné | s.o. | s.o. |
| RA | 10 | Chasse aux cybermenaces | A. Établir et maintenir une capacité de chasse aux cybermenaces de manière à<br>1. relever les indicateurs de compromission dans les systèmes organisationnels<br>2. détecter, suivre et contrer les menaces qui visent les contrôles existants<br>B. Avoir recours à la capacité de chasse aux cybermenaces [Affectation : fréquence définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| SA | 01 | Politique et procédures d'acquisition des systèmes et des services | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique d'acquisition des systèmes et des services [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique d'acquisition des systèmes et des services ainsi que des contrôles connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'acquisition des systèmes et des services<br>C. Passer en revue et mettre à jour, par rapport à l'acquisition des systèmes et des services,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| SA | 02 | Affectation des ressources | A. Déterminer les exigences de haut niveau en matière de sécurité de l'information et de protection de la vie privée pour le système ou les services connexes lors de la planification des processus liés à la mission et aux activités<br>B. Déterminer, documenter et affecter les ressources nécessaires pour protéger le système ou les services connexes dans le cadre du processus de planification des immobilisations et de contrôle des investissements<br>C. Établir un poste distinct pour la sécurité de l'information et la protection de la vie privée dans sa documentation de programmation et de budgétisation | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 03 | Cycle de développement des systèmes | A. Acquérir, développer et gérer le système au moyen de [Affectation : cycle de développement des systèmes défini par l'organisation] qui comprend les facteurs à considérer en matière de sécurité de l'information et de protection de la vie privée<br>B. Définir et documenter les rôles et les responsabilités en matière de sécurité de l'information et de protection de la vie privée tout au long du cycle de développement des systèmes<br>C. Identifier les personnes qui assument des rôles et des responsabilités en matière de sécurité de l'information et de protection de la vie privée<br>D. Intégrer le processus de gestion des risques liés à la sécurité de l'information et à la protection de la vie privée de l'organisation dans les activités du cycle de développement des systèmes | Activité | Sélectionné | s.o. | s.o. |
| SA | 03(01) | Cycle de développement des systèmes | Cycle de développement des systèmes : Gestion de l'environnement de préproduction<br>S'assurer que la protection des environnements de préproduction est proportionnelle au risque tout au long du cycle de développement du système, du composant de système ou du service qui s'y rapporte. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 03(02) | Cycle de développement des systèmes | Cycle de développement des systèmes : Utilisation de données opérationnelles et en temps réel<br>a. Approuver, documenter et contrôler l'utilisation de données en temps réel dans les environnements de préproduction pour le système, le composant de système ou le service qui s'y rapporte<br>b. Protéger les environnements de préproduction pour le système, le composant de système ou le service qui s'y rapporte de manière à avoir le même niveau d'incidence ou le même niveau de classification que toute donnée en cours d'utilisation en temps réel dans les environnements de préproduction | Activité | Non sélectionné | s.o. | s.o. |
| SA | 03(03) | Cycle de développement des systèmes | Cycle de développement des systèmes : Mise à jour technologique<br>Planifier et mettre en œuvre un calendrier de mise à jour technologique pour le système tout au long du cycle de développement du système. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 04 | Processus d'acquisition | Inclure, explicitement ou en référence, les exigences, les descriptions et les critères suivants en utilisant [Sélection (un choix ou plus) : langage contractuel normalisé; [Affectation : langage contractuel défini par l'organisation]] dans le contrat d'acquisition du système, des composants du système ou des services qui s'y rapportent<br>A. exigences fonctionnelles de sécurité et de protection de la vie privée<br>B. exigences en matière de robustesse du mécanisme<br>C. exigences d'assurance de sécurité et de protection de la vie privée<br>D. contrôles nécessaires pour satisfaire les exigences de sécurité et de protection de la vie privée<br>E. exigences liées à la documentation sur la sécurité et la protection de la vie privée<br>F. exigences liées à la protection de la documentation sur la sécurité et la protection de la vie privée<br>G. description de l'environnement de développement du système et de l'environnement dans lequel on prévoit exploiter le système<br>H. affectation de responsabilités ou identification des parties responsables de la sécurité de l'information, de la protection de la vie privée et de la gestion des risques liés à la chaîne d'approvisionnement<br>I. critères d'acceptation | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 04(01) | Processus d'acquisition | Processus d'acquisition : Propriétés fonctionnelles des contrôles<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte donne une description des propriétés fonctionnelles des contrôles à mettre en œuvre. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 04(02) | Processus d'acquisition | Processus d'acquisition : Renseignements relatifs à la conception et à la mise en œuvre des contrôles<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte fournisse des renseignements sur la conception et la mise en œuvre des contrôles, ce qui comprend : [Sélection (un choix ou plus) : interfaces de systèmes externes servant à la sécurité; conception de haut niveau; conception de bas niveau; code source ou schémas des composants matériels; [Affectation : renseignements produits par l'organisme sur la conception et sur la mise en œuvre]] selon [Affectation : degré de détails défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 04(03) | Processus d'acquisition | Processus d'acquisition : Méthodes, techniques et pratiques en matière de développement<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte démontre que le cycle de développement du système comprend<br>a. [Affectation : méthodes d'ingénierie définies par l'organisation]<br>b. [Sélection (un choix ou plus) : [Affectation : méthodes d'ingénierie de la sécurité de système définies par l'organisation]; [Affectation : méthodes d'ingénierie de la protection de la vie privée définies par l'organisation]]<br>c. [Affectation : méthodes de développement logiciel définies par l'organisation; méthodes de test, d'évaluation, de vérification et de validation; et processus de contrôle de la qualité] | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 04(04) | Processus d'acquisition | Processus d'acquisition : Attribution de composants à des systèmes :<br>Annulé : Intégré au contrôle CM-08(09). | Contrôle | s.o. | s.o. | s.o. |
| SA | 04(05) | Processus d'acquisition | Processus d'acquisition : Configurations de systèmes, de composants et de services<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. produire un système, des composants ou des services dont les [Affectation : configurations de sécurité définies par l'organisation] sont mises en œuvre<br>b. utiliser les configurations comme valeurs par défaut pour tout système, composant ou service devant faire ultimement l'objet d'une réinstallation ou d'une mise à niveau | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 04(06) | Processus d'acquisition | Processus d'acquisition : Utilisation de produits de cybersécurité<br>A. Utiliser uniquement les produits gouvernementaux sur étagère (GOTS pour *Government Off-the-Shelf*) ou commerciaux sur étagère (COTS pour *Commercial Off-the-Shelf*) de cybersécurité et les produits informatiques sécurisés qui constituent une solution approuvée par le Centre pour la cybersécurité pour protéger l'information classifiée lorsque les réseaux servant à transmettre cette information ont un niveau de classification inférieur à celui de l'information transmise<br>b. Exiger que ces produits soient évalués ou validés par le Centre pour la cybersécurité ou conformément à des procédures approuvées par le Centre pour la cybersécurité | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 04(07) | Processus d'acquisition | Processus d'acquisition : Profils de protection reconnus par le Programme canadien lié aux Critères communs (PCCC)<br>a. Limiter l'utilisation de produits commerciaux de cybersécurité et de produits informatiques sécurisés à ceux qui ont déjà été évalués selon un profil de protection reconnu par le PCCC pour un type de technologie particulier, si un tel profil existe<br>b. S'il n'y a aucun profil de protection reconnu par le PCCC pour un type de technologie en particulier et qu'un produit de TI commercial a recours à une fonctionnalité cryptographique pour appliquer sa stratégie de sécurité, exiger que le module cryptographique soit validé selon la norme FIPS (Federal Information Processing Standard) ou reconnu par le PCCC | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 04(08) | Processus d'acquisition | Processus d'acquisition : Plan de surveillance continue des contrôles<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | élabore un plan pour assurer une surveillance continue de l'efficacité des contrôles, conformément au programme de surveillance continue de l'organisation. | | | | |
| SA | 04(09) | Processus d'acquisition | Processus d'acquisition : Fonctions, ports, protocoles et services utilisés<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte détermine les fonctions, les ports, les protocoles et les services qui seront utilisés dans l'organisation. | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 04(10) | Processus d'acquisition | Processus d'acquisition : Utilisation de produits de justificatifs d'identité numériques approuvés<br>Utiliser seulement les produits informatiques recommandés par le Centre pour la cybersécurité pour la capacité des justificatifs d'identité numériques mise en œuvre dans les systèmes de l'organisation. | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 04(11) | Processus d'acquisition | Processus d'acquisition : Système d'enregistrement<br>Inclure les [Affectation : exigences en matière de la LPRP définies par l'organisation] dans le contrat d'acquisition relatif à l'exploitation d'un système d'enregistrement au nom d'une organisation afin d'assurer la mission ou les activités de cette dernière. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 04(12) | Processus d'acquisition | Processus d'acquisition : Propriété des données<br>a. Inclure les exigences relatives à la propriété des données organisationnelles dans le contrat d'acquisition<br>b. Exiger que toutes les données soient supprimées du système de l'entrepreneure ou entrepreneur et retournées à l'organisation dans les [Affectation : délais définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 05 | Documentation relative aux systèmes | A. Obtenir ou élaborer la documentation à l'intention des administratrices et administrateurs d'un système, d'un composant du système ou du service qui s'y rapporte, qui décrit<br>1. la configuration, l'installation et l'exploitation sécurisées du système, du composant ou du service<br>2. l'utilisation et la maintenance efficaces des fonctions et mécanismes de sécurité et de protection de la vie privée<br>3. les vulnérabilités connues associées à la configuration et à l'utilisation des fonctions administratives et privilégiées<br>B. Obtenir ou élaborer la documentation des utilisatrices et utilisateurs d'un système, d'un composant du système ou du service qui s'y rapporte, laquelle décrit<br>1. les fonctions et mécanismes de sécurité et de protection de la vie privée accessibles aux utilisatrices et utilisateurs, et la façon d'utiliser efficacement ces fonctions et mécanismes<br>2. les méthodes d'interaction utilisateur qui permettent aux utilisatrices et utilisateurs d'utiliser le système, le composant ou le service de façon plus sécurisée et de protéger leur vie privée<br>3. les responsabilités des utilisatrices ou utilisateurs concernant le maintien de la sécurité du système, de ses composants ou des services qui s'y rapportent, et de la vie privée de ces personnes<br>C. Documenter les tentatives visant à obtenir des documents sur le système, ses composants ou les services qui s'y rapportent, qui n'existent pas ou qui ne sont pas disponibles, et réagir en [Affectation : mesures définies par l'organisation]<br>D. Distribuer la documentation à [Affectation : personnel ou rôles définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| SA | 05(01) | Documentation relative aux systèmes | Documentation relative aux systèmes : Propriétés fonctionnelles des contrôles de sécurité<br>Annulé : Intégré au contrôle SA-04(01). | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 05(02) | Documentation relative aux systèmes | Documentation relative aux systèmes : Interfaces des systèmes externes servant à la sécurité<br>Annulé : Intégré au contrôle SA-04(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 05(03) | Documentation relative aux systèmes | Documentation relative aux systèmes : Conception de haut niveau<br>Annulé : Intégré au contrôle SA-04(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 05(04) | Documentation relative aux systèmes | Documentation relative aux systèmes : Conception de bas niveau<br>Annulé : Intégré au contrôle SA-04(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 05(05) | Documentation relative aux systèmes | Documentation relative aux systèmes : Code source<br>Annulé : Intégré au contrôle SA-04(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 06 | Restrictions relatives à l'utilisation des logiciels | Annulé : Intégré aux contrôles CM-10 et SI-07. | s.o. | s.o. | s.o. | s.o. |
| SA | 07 | Logiciels installés par les utilisatrices et utilisateurs | Annulé : Intégré aux contrôles CM-11 et SI-07. | s.o. | s.o. | s.o. | s.o. |
| SA | 08 | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Appliquer les principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes suivants pour la spécification, la conception, le développement, la mise en œuvre et la modification des systèmes et des composants de systèmes : [Affectation : principes d'ingénierie de la sécurité et de la protection de la vie privée des systèmes définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 08(01) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Abstractions claires<br>Mettre en place le principe de la conception sécurisée des abstractions claires. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(02) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Mécanisme moindre commun<br>Mettre en place le principe du moindre mécanisme commun dans la conception sécurisée des [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(03) | Principes d'ingénierie de la sécurité et de | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Modularité et structuration en couches<br>Mettre en place les principes de conception sécurisée de la modularité et de la structuration en couches dans les | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | la protection de la vie privée | [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | | | | |
| SA | 08(04) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Dépendances partiellement hiérarchisées<br>Mettre en place le principe de conception sécurisée des dépendances partiellement hiérarchisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(05) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Accès avec médiation efficace<br>Mettre en place le principe de conception sécurisée de l'accès avec médiation efficace dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(06) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Échange minimal<br>Mettre en place le principe de conception sécurisée de l'échange minimal dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(07) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Complexité réduite<br>Mettre en place le principe de conception sécurisée de la complexité réduite dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(08) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Évolutivité sécurisée<br>Mettre en place le principe de conception sécurisée de l'évolutivité dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(09) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Composants fiables<br>Mettre en place le principe de conception sécurisée des composants fiables dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(10) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Confiance hiérarchique<br>Mettre en place le principe de conception sécurisée de la confiance hiérarchique dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 08(11) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Seuil de modification inverse<br>Mettre en place le principe de conception sécurisée du seuil de modification inverse dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(12) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Protection hiérarchique<br>Mettre en place le principe de conception sécurisée de la protection hiérarchique dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(13) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Éléments de sécurité minimisés<br>Mettre en place le principe de conception sécurisée des éléments de sécurité minimisés dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(14) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Droit d'accès minimal<br>Mettre en place le principe de conception sécurisée du droit d'accès minimal dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(15) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Autorisation des prédicats<br>Mettre en place le principe de conception sécurisée de l'autorisation des prédicats dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(16) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Fiabilité autonome<br>Mettre en place le principe de conception sécurisée de la fiabilité autonome dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(17) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Composition distribuée sécurisée<br>Mettre en place le principe de conception sécurisée de la composition distribuée sécurisée dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(18) | Principes d'ingénierie de la sécurité et de | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Voies de communication fiables<br>Mettre en place le principe de conception sécurisée des voies de communication fiables dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | la protection de la vie privée | | | | | |
| SA | 08(19) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Protection continue<br>Mettre en place le principe de conception sécurisée de la protection continue dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(20) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Gestion sécurisée des métadonnées<br>Mettre en place le principe de conception sécurisée de la gestion sécurisée des métadonnées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(21) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Auto-analyse<br>Mettre en place le principe de conception sécurisée de l'auto-analyse dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(22) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Responsabilisation et traçabilité<br>Mettre en place le principe de conception sécurisée de la responsabilisation et de la traçabilité dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(23) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Valeurs par défaut sécurisées<br>Mettre en place le principe de conception sécurisée des valeurs par défaut sécurisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(24) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Défaillance et reprise sécurisées<br>Mettre en place le principe de conception sécurisée de la défaillance et de la reprise sécurisées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(25) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Sécurité économique<br>Mettre en place le principe de conception sécurisée de la sécurité économique dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 08(26) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Sécurité des performances<br>Mettre en place le principe de conception sécurisée de la sécurité des performances dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(27) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Sécurité tenant compte du facteur humain<br>Mettre en place le principe de conception sécurisée de la sécurité tenant compte du facteur humain dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(28) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Sécurité acceptable<br>Mettre en place le principe de conception sécurisée de la sécurité acceptable dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(29) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Procédures reproduisibles et documentées<br>Mettre en place le principe de conception sécurisée des procédures reproduisibles et documentées dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(30) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Rigueur procédurale<br>Mettre en place le principe de conception sécurisée de la rigueur procédurale dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(31) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Modification de systèmes sécurisés<br>Mettre en place le principe de conception sécurisée de la modification de systèmes sécurisés dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(32) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Documentation adéquate<br>Mettre en place le principe de conception sécurisée de la documentation adéquate dans les [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 08(33) | Principes d'ingénierie de la sécurité et de | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Minimisation<br>Mettre en place le principe de protection de la vie privée de la minimisation au moyen de [Affectation : processus définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | la protection de la vie privée | | | | | |
| SA | 08(400) | Principes d'ingénierie de la sécurité et de la protection de la vie privée | Principes d'ingénierie de la sécurité et de la protection de la vie privée : Ingénieures et ingénieurs brevetés et agréés<br>Avoir recours à des ingénieures et ingénieurs brevetés et agréés en sécurité qui assument la responsabilité des spécifications, de la conception, du développement et de la mise en œuvre de solutions de sécurité et de protection de la vie privée du système d'information. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 09 | Services de systèmes externes | A. Exiger que les fournisseurs de services de systèmes externes respectent les exigences organisationnelles en matière de sécurité et de protection de la vie privée et aient recours aux contrôles suivants : [Affectation : contrôles définis par l'organisation]<br>B. Définir et documenter la surveillance organisationnelle, de même que les rôles et responsabilités des utilisatrices et utilisateurs en ce qui a trait aux services de systèmes externes<br>C. Mettre en œuvre sur une base continue des processus, des méthodes et des techniques pour surveiller la conformité aux contrôles des fournisseurs de services externes : [Affectation : méthodes, techniques et processus définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 09(01) | Services de systèmes externes | Services de systèmes externes : Évaluations des risques et approbations organisationnelles<br>a. Procéder à une évaluation des risques organisationnels avant d'acquérir ou d'externaliser des services de sécurité de l'information<br>b. S'assurer que l'acquisition ou l'externalisation des services de sécurité de l'information est approuvée par [Affectation : personnel ou rôles définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 09(02) | Services de systèmes externes | Services de systèmes externes : Établissement des fonctions, des ports, des protocoles et des services<br>Exiger que les fournisseurs de services de systèmes externes identifient les fonctions, les ports, les protocoles et les autres services nécessaires à l'utilisation des services en question : [Affectation : services de systèmes externes définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 09(03) | Services de systèmes externes | Services de systèmes externes : Établissement et maintien d'une relation de confiance avec les fournisseurs de services<br>Établir, documenter et maintenir des relations de confiance avec les fournisseurs de services externes en fonction des exigences, des propriétés, des conditions ou des facteurs suivants : [Affectation : exigences de sécurité et de protection de la vie privée, propriétés, conditions ou facteurs définis par l'organisation qui constituent des relations de confiance acceptables]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 09(04) | Services de systèmes externes | Services de systèmes externes : Concordance des intérêts des clients et des fournisseurs<br>Prendre les mesures suivantes pour confirmer que les intérêts de [Affectation : fournisseurs de services externes désignés par l'organisation] répondent aux intérêts de l'organisation : [Affectation : actions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 09(05) | Services de systèmes externes | Services de systèmes externes : Lieux de traitement, de stockage et de service<br>Circonscrire les lieux de [Sélection (un choix ou plus) : traitement de l'information; stockage de l'information ou de données; services de systèmes] à [Affectation : lieux désignés par l'organisation] en se fondant sur [Affectation : exigences ou conditions définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 09(06) | Services de systèmes externes | Services de systèmes externes : Clés cryptographiques contrôlées par l'organisation<br>Maintenir un contrôle exclusif des clés cryptographiques pour le matériel chiffré stocké ou transmis par l'entremise d'un système externe. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 09(07) | Services de systèmes externes | Services de systèmes externes : Vérification de l'intégrité contrôlée par l'organisation<br>Fournir la capacité de vérifier l'intégrité de l'information qui réside sur le système externe. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 09(08) | Services de systèmes externes | Services de systèmes externes : Lieu de stockage et de traitement (au Canada)<br>Restreindre le lieu géographique du traitement de l'information et du stockage des données aux installations situées dans la frontière gouvernementale et juridique du Canada. | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 10 | Gestion des configurations par les développeuses et développeurs | Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>A. procéder à la gestion des configurations au cours [Sélection (un choix ou plus) : de la conception; du développement; de la mise en œuvre; de l'exploitation; de l'élimination] du système, du composant ou du service<br>B. documenter, gérer et contrôler l'intégrité des changements apportés aux [Affectation : éléments de configuration définis par l'organisation dans le cadre de la gestion des configurations]<br>C. mettre en œuvre uniquement les changements approuvés par l'organisation au système, au composant ou au service<br>D. documenter les changements approuvés apportés au système, au composant ou au service et les répercussions potentielles de tels changements sur la sécurité et la protection de la vie privée<br>E. assurer le suivi des failles de sécurité informatique et de leur résolution dans le système, le composant ou le service et faire rapport des conclusions au [Affectation : personnel désigné par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| SA | 10(01) | Gestion des configurations par les développeuses et développeurs | Gestion des configurations par les développeuses et développeurs : Vérification de l'intégrité des logiciels et des micrologiciels<br>Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s'y rapporte vérifie l'intégrité des composants logiciels et micrologiciels. | Activité | Sélectionné | s.o. | s.o. |
| SA | 10(02) | Gestion des configurations par les développeuses et développeurs | Gestion des configurations par les développeuses et développeurs : Processus de gestion des configurations de rechange<br>Prévoir un processus de gestion des configurations de rechange auquel participent des membres du personnel en l'absence d'une équipe de développeuses et développeurs ou d'intégratrices et intégrateurs spécialisés en gestion des configurations. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 10(03) | Gestion des configurations par les développeuses et développeurs | Gestion des configurations par les développeuses et développeurs : Vérification de l'intégrité du matériel<br>Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s'y rapporte vérifie l'intégrité des composants matériels. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 10(04) | Gestion des configurations par les | Gestion des configurations par les développeuses et développeurs : Génération fiable<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte emploie des outils permettant de comparer les versions nouvellement générées aux versions précédentes des descriptions, du code source et du code objet des composants matériels servant à la sécurité. | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | développeuses et développeurs | | | | | |
| SA | 10(05) | Gestion des configurations par les développeuses et développeurs | Gestion des configurations par les développeuses et développeurs : Intégrité du mappage pour le contrôle des versions<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte maintienne l'intégrité du mappage entre les données de la version maîtresse qui décrivent, d'une part, la version actuelle du matériel, des logiciels et des micrologiciels servant à la sécurité et, d'autre part, la copie maîtresse des données de la version qui se trouve actuellement sur le site. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 10(06) | Gestion des configurations par les développeuses et développeurs | Gestion des configurations par les développeuses et développeurs : Distribution fiable<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte exécute les procédures visant à garantir que les mises à jour des composants matériels, logiciels et micrologiciels servant à la sécurité, qui sont distribuées à l'organisation sont en tout point conformes aux spécifications des copies maîtresses. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 10(07) | Gestion des configurations par les développeuses et développeurs | Gestion des configurations par les développeuses et développeurs : Représentantes et représentants de la sécurité et de la protection de la vie privée<br>Exiger que [Affectation : représentante ou représentant de la sécurité et de la protection de la vie privée désigné par l'organisation] soit membre de [Affectation : processus de gestion et de contrôle des configurations défini par l'organisation]. | Activité | Sélectionné | 1 [SPC, SCT et Centre pour la cybersécurité]<br>2 [Projets et services de SPC utilisés par plusieurs ministères] | s.o. |
| SA | 11 | Évaluations et tests effectués par les développeuses et développeurs | Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte fasse ce qui suit à toutes les phases de postconception du cycle de développement du système de manière à<br>A. élaborer et mettre en œuvre un plan pour les évaluations des contrôles de sécurité et de protection de la vie privée en cours<br>B. procéder au test ou à l'évaluation [Sélection (un choix ou plus) : unité; intégration; système; régression] tous les [Affectation : fréquence définie par l'organisation] selon [Affectation : profondeur et couverture définies par l'organisation]<br>C. fournir une preuve de l'élaboration d'un plan d'évaluation et des résultats des tests ou de l'évaluation<br>D. mettre en œuvre un processus vérifiable de correction des défauts<br>E. corriger les défauts relevés au cours des tests et de l'évaluation | Activité | Sélectionné | s.o. | s.o. |
| SA | 11(01) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Analyse statique du code<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils d'analyse statique du code pour identifier les défauts courants et documenter les résultats de l'analyse. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(02) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Modélisation des menaces et analyses des vulnérabilités<br>Exiger que la développeuse ou le développeur du système, du composant ou du service qui s'y rapporte effectue une modélisation des menaces et des analyses des vulnérabilités au cours du développement, ainsi que des tests et une évaluation du système, du composant ou du service qui<br>a. utilise l'information contextuelle suivante : [Affectation : information relative aux répercussions définie par l'organisation, environnement opérationnel, menaces connues ou présumées, et niveaux acceptables de risque]<br>b. utilise les méthodes et les outils suivants : [Affectation : méthodes et outils définis par l'organisation]<br>c. procède à la modélisation et à l'analyse du niveau de rigueur suivant : [Affectation : profondeur et étendue de | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | modélisation et d'analyse définies par l'organisation]<br>d. démontre que les critères d'acceptation suivants ont été respectés : [Affectation : critères d'acceptation définis par l'organisation] | | | | |
| SA | 11(03) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Vérification indépendante des plans d'évaluation et des preuves<br>a. Exiger que [Affectation : critères d'indépendance définis par l'organisation] soit en mesure d'attester de l'adéquation de la mise en œuvre du plan d'évaluation de sécurité et de vérifier les preuves produites pendant les tests et les évaluations<br>b. Veiller à ce que l'agente ou agent indépendant ait reçu suffisamment d'information pour mener à bien le processus de vérification ou qu'il dispose de l'autorité nécessaire pour obtenir l'information en question | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(04) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Revues manuelles du code<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte procède à la revue manuelle du code de [Affectation : code particulier désigné par l'organisation] au moyen des procédures, des techniques ou des processus suivants : [Affectation : procédures, techniques et processus définis par l'organisation]. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(05) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Tests d'intrusion<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte procède à des tests d'intrusion<br>a. au niveau de rigueur suivant : [Affectation : profondeur et étendue des tests définies par l'organisation]<br>b. selon les contraintes suivantes : [Affectation : contraintes définies par l'organisation] | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(06) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Examens de la surface d'attaque<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte procède à des examens de la surface d'attaque. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(07) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Vérification de la portée des tests et des évaluations<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure que la portée des tests et des évaluations fournit une couverture complète des contrôles requis au niveau de rigueur suivant : [Affectation : profondeur et étendue des tests et des évaluations définies par l'organisation]. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(08) | Évaluations et tests effectués par les développeuses et développeurs | Évaluations et tests effectués par les développeuses et développeurs : Analyse dynamique du code<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils d'analyse dynamique du code pour relever les défauts courants et documenter les résultats de l'analyse. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 11(09) | Évaluations et tests effectués par les | Évaluations et tests effectués par les développeuses et développeurs : Tests de sécurité des applications interactives<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou du service qui s'y rapporte utilise des outils de tests de la sécurité des applications interactives pour relever les défauts et documenter les résultats. | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | développeuses et développeurs | | | | | |
| SA | 12 | Protection de la chaîne d'approvision-nement | Annulé : Transféré sous la famille de contrôles SR. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(01) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Stratégies, outils et méthodes d'acquisition<br>Annulé : Transféré sous le contrôle SR-05. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(02) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Examen des fournisseurs<br>Annulé : Transféré sous le contrôle SR-06. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(03) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Expédition et entreposage sécurisés<br>Annulé : Intégré au contrôle SR-03. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(04) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Diversité des fournisseurs<br>Annulé : Intégré au contrôle SR-03(01). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(05) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Limitation des dommages<br>Annulé : Intégré au contrôle SR-03(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(06) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Réduction du temps d'approvisionnement<br>Annulé : Intégré au contrôle SR-05(01). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(07) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Évaluation préalable à la sélection, à l'acceptation et à la mise à jour<br>Annulé : Transféré sous le contrôle SR-05(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(08) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Utilisation du renseignement de toutes sources<br>Annulé : Intégré au contrôle RA-03(02). | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 12(09) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Sécurité opérationnelle<br>Annulé : Transféré sous le contrôle SR-07. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(10) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Attestation de l'authenticité et de la non-altérité<br>Annulé : Transféré sous le contrôle SR-04(03). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(11) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Tests d'intrusion et analyse d'éléments, de processus et des parties prenantes<br>Annulé : Transféré sous le contrôle SR-06(01). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(12) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Accords interorganisationnels<br>Annulé : Transféré sous le contrôle SR-08. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(13) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Composants de systèmes d'information essentiels<br>Annulé : Intégré aux contrôles MA-06 et RA-09. | s.o. | s.o. | s.o. | s.o. |
| SA | 12(14) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Identité et traçabilité<br>Annulé : Transféré sous les contrôles SR-04(01) et SR-04(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 12(15) | Protection de la chaîne d'approvision-nement | Protection de la chaîne d'approvisionnement : Processus visant à réagir aux faiblesses et aux lacunes<br>Annulé : Intégré au contrôle SR-03. | s.o. | s.o. | s.o. | s.o. |
| SA | 13 | Fiabilité | Annulé : Intégré au contrôle SA-08. | s.o. | s.o. | s.o. | s.o. |
| SA | 14 | Analyse de criticité | Annulé : Intégré au contrôle RA-09. | s.o. | s.o. | s.o. | s.o. |
| SA | 14(01) | Analyse de criticité | Analyse de criticité : Composants essentiels sans autre source d'approvisionnement viable<br>Annulé : Intégré au contrôle SA-20. | s.o. | s.o. | s.o. | s.o. |
| SA | 15 | Processus, normes et outils de développement | A. Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte suive un processus de développement documenté qui permet<br>1. de répondre explicitement aux exigences de sécurité et de protection de la vie privée<br>2. d'identifier les normes et les outils devant servir au processus de développement | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 3. de documenter les options et les configurations particulières aux outils utilisés dans le processus de développement<br>4. de documenter, de gérer et de garantir l'intégrité des changements apportés aux processus et aux outils servant au développement<br>B. Examiner les processus, les normes, les outils, les options d'outils et les configurations d'outils liés au développement [Affectation : fréquence définie par l'organisation] pour établir si les processus, les normes, les outils, les options des outils et les configurations des outils peuvent répondre aux exigences de sécurité et de protection de la vie privée suivantes : [Affectation : exigences de sécurité et de protection de la vie privée définies par l'organisation] | | | | |
| SA | 15(01) | Processus, normes et outils de développement | Processus, normes et outils de développement : Mesure de la qualité<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. définir les mesures de la qualité au début du processus de développement<br>b. fournir des preuves que les critères de qualité sont respectés à [Sélection (un choix ou plus) : [Affectation : fréquence définie par l'organisation]; [Affectation : échéancier d'examen de programmes défini par l'organisation]; au moment de la mise en service] | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(02) | Processus, normes et outils de développement | Processus, normes et outils de développement : Outils de traçabilité des contrôles de sécurité et de protection de la vie privée<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte utilise des outils de traçabilité des contrôles de sécurité et de protection de la vie privée au cours du processus de développement. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(03) | Processus, normes et outils de développement | Processus, normes et outils de développement : Analyse de criticité<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte procède à une analyse de criticité<br>a. aux points de décision suivants dans le cycle de développement du système : [Affectation : points de décision dans le cycle de développement du système définis par l'organisation]<br>b. au niveau de rigueur suivant : [Affectation : profondeur et étendue de l'analyse de criticité définies par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| SA | 15(04) | Processus, normes et outils de développement | Processus, normes et outils de développement : Modélisation des menaces et analyse des vulnérabilités<br>Annulé : Intégré au contrôle SA-11(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 15(05) | Processus, normes et outils de développement | Processus, normes et outils de développement : Réduction de la surface d'attaque<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte réduise les surfaces d'attaque à [Affectation : limites définies par l'organisation]. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(06) | Processus, normes et outils de développement | Processus, normes et outils de développement : Amélioration continue<br>Exiger que la développeuse ou le développeur d'un système d'information, d'un composant du système ou du service qui s'y rapporte mette en œuvre un processus détaillé visant expressément à améliorer continuellement le processus de développement. | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 15(07) | Processus, normes et outils de développement | Processus, normes et outils de développement : Analyse automatisée des vulnérabilités<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte, [Affectation : fréquence définie par l'organisation]<br>a. réalise une analyse automatisée des vulnérabilités au moyen de [Affectation : outils définis par l'organisation]<br>b. définisse les possibilités d'exploitation des vulnérabilités relevées<br>c. définisse les mesures d'atténuation des risques liés aux vulnérabilités décelées<br>d. fournisse les données produites par les outils et les résultats des analyses à [Affectation : personnel ou rôles définis par l'organisation] | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(08) | Processus, normes et outils de développement | Processus, normes et outils de développement : Réutilisation de l'information sur les menaces et les vulnérabilités<br>Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte utilise une modélisation des menaces et des analyses des vulnérabilités exécutées sur des systèmes, des composants ou des services semblables de façon à éclairer le processus de développement en cours. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(09) | Processus, normes et outils de développement | Processus, normes et outils de développement : Utilisation de données en temps réel<br>Annulé : Intégré au contrôle SA-03(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 15(10) | Processus, normes et outils de développement | Processus, normes et outils de développement : Plan d'intervention en cas d'incident<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure d'élaborer, de mettre en œuvre et de mettre à l'essai un plan d'intervention en cas d'incident. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(11) | Processus, normes et outils de développement | Processus, normes et outils de développement : Système ou composant d'archivage<br>Exiger que la développeuse ou le développeur d'un système ou d'un composant du système archive le système ou le composant à mettre en service avec les preuves connexes qui appuient l'examen de sécurité et de protection de la vie privée final. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 15(12) | Processus, normes et outils de développement | Processus, normes et outils de développement : Réduction des renseignements personnels<br>Exiger que la développeuse ou le développeur du système ou du composant du système limite l'utilisation de renseignements personnels dans les environnements de développement et de test. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 16 | Formation offerte par la développeuse ou le développeur | Exiger que la développeuse ou le développeur d'un système, d'un composant du système ou d'un service qui s'y rapporte fournisse la formation portant sur l'utilisation et l'exploitation adéquates des fonctions, des contrôles et des mécanismes de sécurité et de protection de la vie privée mis en œuvre : [Affectation : formation définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 17 | Architecture et conception de la sécurité et de la protection de la vie privée de la | Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte produise des spécifications de conception et une architecture de sécurité et de protection de la vie privée qui<br>A. est conforme à l'architecture de sécurité et de protection de la vie privée de l'organisation qui fait partie intégrante de l'architecture d'entreprise de l'organisation<br>B. décrit intégralement et précisément les fonctions de sécurité et de protection de la vie privée requises ainsi que | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | développeuse ou du développeur | l'attribution des contrôles de sécurité parmi les composants physiques et logiques<br>C. expose comment les fonctions de sécurité et de protection de la vie privée, les mécanismes et les services fonctionnent ensemble pour fournir les capacités de sécurité requises et favoriser une approche coordonnée en matière de protection | | | | |
| SA | 17(01) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur :<br>Modèle formel de stratégie<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. produire, en parfaite intégration avec le processus de développement, un modèle formel de stratégie décrivant [Affectation : éléments de stratégie organisationnelle de sécurité désignés par l'organisme] à mettre en œuvre<br>b. démontrer que le modèle formel de stratégie est cohérent et suffisant pour appliquer les dispositions de la stratégie organisationnelle de sécurité dès lors que celle-ci est en vigueur | Activité | Non sélectionné | s.o. | s.o. |
| SA | 17(02) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur :<br>Composants servant à la sécurité<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. définir le matériel, les logiciels et les micrologiciels servant à la sécurité<br>b. fournir un argumentaire démontrant l'exhaustivité de la définition du matériel, des logiciels et des micrologiciels de sécurité | Activité | Non sélectionné | s.o. | s.o. |
| SA | 17(03) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur :<br>Correspondance formelle<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. produire, en parfaite intégration avec le processus de développement, des spécifications formelles de haut niveau qui décrivent les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets<br>b. montrer – par des preuves accessibles et, s'il y a lieu, par des démonstrations informelles – que les spécifications de haut niveau sont conformes au modèle formel de stratégie<br>c. montrer, par des démonstrations informelles, que les spécifications formelles de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité<br>d. montrer que les spécifications formelles de haut niveau décrivent précisément le matériel, les logiciels et les micrologiciels utilisés à des fins de sécurité<br>e. décrire les mécanismes liés au matériel, aux logiciels et aux micrologiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications formelles de haut niveau, mais qui sont inhérents à ce matériel, à ces logiciels et à ces micrologiciels servant à la sécurité | Activité | Non sélectionné | s.o. | s.o. |
| SA | 17(04) | Architecture et conception de la sécurité et de la protection de la vie privée de la | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur :<br>Correspondance informelle<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. produire, en parfaite intégration avec le processus de développement, des spécifications descriptives informelles de | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | développeuse ou du développeur | haut niveau qui décrivent les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets<br>b. montrer par [Sélection (un choix) : démonstration informelle; arguments convaincants fournis, si possible, par des méthodes formelles] que les spécifications descriptives de haut niveau sont conformes au modèle formel de stratégie<br>c. montrer, par des démonstrations informelles, que les spécifications descriptives de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité<br>d. montrer que les spécifications descriptives de haut niveau décrivent précisément les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité<br>e. décrire les mécanismes liés au matériel, aux logiciels et aux micrologiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications descriptives de haut niveau, mais qui sont strictement inhérents à ce matériel, à ces logiciels et à ces micrologiciels servant à la sécurité | | | | |
| SA | 17(05) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur : Conception simple<br>Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de<br>a. concevoir et structurer le matériel, les logiciels et les micrologiciels servant à la sécurité de façon à créer un mécanisme de protection complet, de conception simple et doté d'une sémantique précisément définie<br>b. structurer en interne le matériel, les logiciels et les micrologiciels servant à la sécurité, en portant une attention particulière au mécanisme en question | Activité | Non sélectionné | s.o. | s.o. |
| SA | 17(06) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur : Structure de mise à l'essai<br>Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s'y rapporte structure le matériel, les logiciels et les micrologiciels servant à la sécurité de manière à faciliter la mise à l'essai. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 17(07) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur : Structure relative au droit d'accès minimal<br>Exiger que la développeuse ou le développeur du système, du composant de système ou du service qui s'y rapporte structure le matériel, les logiciels et les micrologiciels servant à la sécurité de manière à faciliter le contrôle de l'accès avec le droit d'accès minimal. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 17(08) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur : Orchestration<br>Concevoir [Affectation : systèmes ou composants de systèmes critiques désignés par l'organisation] avec un comportement coordonné pour mettre en œuvre les capacités suivantes : [Affectation : capacités définies par l'organisation, par système ou composant]. | Activité | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | ou du développeur | | | | | |
| SA | 17(09) | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur | Architecture et conception de la sécurité et de la protection de la vie privée de la développeuse ou du développeur :<br>Diversité de la conception<br>Utiliser les différentes conceptions de [Affectation : systèmes ou composants de systèmes critiques désignés par l'organisation] pour satisfaire à un ensemble commun d'exigences ou fournir une fonctionnalité équivalente. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 18 | Résistance au trafiquage et détection | Annulé : Transféré sous le contrôle SR-09. | s.o. | s.o. | s.o. | s.o. |
| SA | 18(01) | Résistance au trafiquage et détection | Résistance au trafiquage et détection : Multiples phases du cycle de développement de systèmes<br>Annulé : Transféré sous le contrôle SR-09(01). | s.o. | s.o. | s.o. | s.o. |
| SA | 18(02) | Résistance au trafiquage et détection | Résistance au trafiquage et détection : Inspection des systèmes ou des composants<br>Annulé : Transféré sous le contrôle SR-10. | s.o. | s.o. | s.o. | s.o. |
| SA | 19 | Authenticité des composants | Annulé : Transféré sous le contrôle SR-11. | s.o. | s.o. | s.o. | s.o. |
| SA | 19(01) | Authenticité des composants | Authenticité des composants : Formation anticontrefaçon<br>Annulé : Transféré sous le contrôle SR-11(01). | s.o. | s.o. | s.o. | s.o. |
| SA | 19(02) | Authenticité des composants | Authenticité des composants : Contrôle des configurations pour l'entretien et la réparation des composants<br>Annulé : Transféré sous le contrôle SR-11(02). | s.o. | s.o. | s.o. | s.o. |
| SA | 19(03) | Authenticité des composants | Authenticité des composants : Mise hors service des composants<br>Annulé : Transféré sous le contrôle SR-12. | s.o. | s.o. | s.o. | s.o. |
| SA | 19(04) | Authenticité des composants | Authenticité des composants : Analyse anticontrefaçon<br>Annulé : Transféré sous le contrôle SR-11(03). | s.o. | s.o. | s.o. | s.o. |
| SA | 20 | Développement sur mesure des composants essentiels | Procéder à une nouvelle mise en œuvre ou au développement sur mesure des composants de systèmes essentiels suivants : [Affectation : composants essentiels désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 21 | Filtrage de sécurité des développeuses et développeurs | Exiger que la développeuse ou le développeur de [Affectation : système, composant de système ou service qui s'y rapporte désigné par l'organisation]<br>A. dispose des autorisations d'accès requises en fonction des [Affectation : responsabilités gouvernementales officielles définies par l'organisation] qui ont été attribuées | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | B. satisfasse aux critères additionnels de filtrage de sécurité du personnel définis par l'organisation : [Affectation : critères additionnels de sélection du personnel définis par l'organisation] | | | | |
| SA | 21(01) | Filtrage de sécurité des développeuses et développeurs | Filtrage de sécurité des développeuses et développeurs : Validation du filtrage de sécurité<br>Annulé : Intégré au contrôle SA-21. | s.o. | s.o. | s.o. | s.o. |
| SA | 22 | Composants de systèmes non pris en charge | A. Remplacer les composants des systèmes lorsqu'ils ne sont plus pris en charge par les développeuses, les développeurs, les fournisseurs ou les fabricants<br>B. Offrir les options suivantes pour les solutions de rechange visant à assurer la continuité du soutien des composants non pris en charge faisant l'objet d'un [Sélection (un choix ou plus) : soutien interne; [Affectation : soutien offert par des fournisseurs externes défini par l'organisation]] | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 22(01) | Composants de systèmes non pris en charge | Composants de systèmes non pris en charge : Solution de rechange visant à assurer la continuité du soutien<br>Annulé : Intégré au contrôle SA-22. | s.o. | s.o. | s.o. | s.o. |
| SA | 23 | Spécialisation | Avoir recours [Sélection (un choix ou plus) : à la conception; à la modification; au renforcement; à la reconfiguration] des [Affectation : systèmes ou composants de systèmes désignés par l'organisation] prenant en charge des services ou des fonctions essentiels à la mission pour renforcer la robustesse de ces systèmes ou composants. | Activité | Non sélectionné | s.o. | s.o. |
| SA | 400 | Souveraineté et juridiction | Exiger que les fonctions opérationnelles de l'organisation respectent un processus d'évaluation des menaces et des risques en matière de souveraineté et de juridiction au [Sélection (un choix ou plus) : niveau de l'organisation; niveau de la mission et des activités; niveau du système] qui consiste à<br>A. procéder à l'évaluation des préjudices pour déterminer les préjudices potentiels maximaux qui pourraient être causés par une contrainte légale externe imposée aux fonctions organisationnelles ou aux ressources informationnelles en<br>1. considérant les besoins opérationnels en matière de sécurité, y compris les lois ou la réglementation qui exigent que les données ne soient pas divulguées ou compromises<br>2. mettant à jour la catégorisation de la sécurité des fonctions organisationnelles ou des ressources informationnelles<br>3. documentant les conséquences négatives de la contrainte légale<br>B. procéder à l'évaluation des menaces propres à la juridiction pour établir la probabilité d'être pris pour cible<br>C. effectuer une évaluation des vulnérabilités pour déterminer les moyens potentiels que la juridiction externe pourrait utiliser pour exploiter les fonctions organisationnelles ou les ressources informationnelles<br>D. procéder à l'évaluation des risques propres à la juridiction | Contrôle | Sélectionné | s.o. | s.o. |
| SA | 400(01) | Souveraineté et juridiction | Souveraineté et juridiction : Évaluation des menaces et des risques<br>Exiger que l'organisation effectue des évaluations des menaces et des risques qui pèsent sur la souveraineté des données en tenant compte de sa juridiction et des aspects pour lesquels des contraintes légales pourraient être efficaces. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(02) | Souveraineté et juridiction | Souveraineté et juridiction : Évaluation d'ordre juridique et contractuel<br>Exiger que l'organisation effectue des évaluations des menaces et des risques qui pèsent sur la souveraineté des données en tenant compte de sa juridiction et des aspects pour lesquels des contraintes légales pourraient être efficaces. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(03) | Souveraineté et juridiction | Souveraineté et juridiction : Marquage des attributs liés aux processus opérationnels<br>S'assurer que les processus opérationnels fassent l'objet du traitement prévu selon la compétence juridique. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SA | 400(04) | Souveraineté et juridiction | Souveraineté et juridiction : Protection des données au repos<br>Éviter que les données résident dans des territoires qui relèvent d'autres compétences juridiques. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(05) | Souveraineté et juridiction | Souveraineté et juridiction : Protection des données en transit<br>Éviter que les données transitent par des territoires qui relèvent d'autres compétences juridiques. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(06) | Souveraineté et juridiction | Souveraineté et juridiction : Protection des données en cours d'utilisation<br>Éviter que les données soient utilisées dans des territoires qui relèvent d'autres compétences juridiques. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(07) | Souveraineté et juridiction | Souveraineté et juridiction : Protection contre les contraintes extraterritoriales<br>Prévenir la compromission des fonctions opérationnelles par des personnes ou des sociétés assujetties à une autre compétence juridique. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(08) | Souveraineté et juridiction | Souveraineté et juridiction : Protection du cycle de vie des activités<br>Prévenir la compromission des fonctions opérationnelles dans le cadre d'attaques du cycle de vie découlant d'une contrainte légale ou menées depuis une autre compétence juridique. | Contrôle | Non sélectionné | s.o. | s.o. |
| SA | 400(09) | Souveraineté et juridiction | Souveraineté et juridiction : Propriété publique<br>Prévenir la compromission des fonctions opérationnelles lors d'un transfert de propriété des fonctions du cycle de vie à une autre compétence juridique. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| SC | 01 | Politique et procédures de protection des systèmes et des communications | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de protection des systèmes et des communications [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de protection des systèmes et des communications ainsi que des contrôles connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures de protection des systèmes et des communications.<br>C. Passer en revue et mettre à jour, par rapport à la protection des systèmes et des communications,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 02 | Séparation des fonctionnalités d'utilisateur et du système | Séparer la fonctionnalité d'utilisateur, dont les services d'interface utilisateur, de la fonctionnalité de gestion du système. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 02(01) | Séparation des fonctionnalités d'utilisateur et du système | Séparation des fonctionnalités d'utilisateur et du système : Interfaces pour les utilisatrices et utilisateurs non privilégiés :<br>Éviter de présenter la fonctionnalité de gestion des systèmes sur les interfaces destinées aux utilisatrices et utilisateurs non privilégiés. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 02(02) | Séparation des fonctionnalités d'utilisateur et du système | Séparation des fonctionnalités d'utilisateur et du système : Dissociabilité<br>Stocker l'information d'état séparément des applications et des logiciels. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 03 | Isolation des fonctions de sécurité | Isoler les fonctions de sécurité des autres fonctions. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 03(01) | Isolation des fonctions de sécurité | Isolation des fonctions de sécurité : Séparation du matériel<br>Avoir recours à des mécanismes de séparation du matériel pour mettre en œuvre l'isolation des fonctions de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 03(02) | Isolation des fonctions de sécurité | Isolation des fonctions de sécurité : Accès et fonctions de contrôle des flux<br>Isoler les fonctions de sécurité appliquant le contrôle de l'accès et du flux d'information des autres fonctions de sécurité et des fonctions non liées à la sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 03(03) | Isolation des fonctions de sécurité | Isolation des fonctions de sécurité : Réduction des fonctionnalités n'ayant pas trait à la sécurité<br>Réduire à son minimum le nombre des fonctions non liées à la sécurité appelées à intégrer le périmètre isolé qui comprend les fonctions de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 03(04) | Isolation des fonctions de sécurité | Isolation des fonctions de sécurité : Jumelage et cohésion des modules<br>Appliquer les fonctions de sécurité sous forme de modules essentiellement indépendants qui maximisent la cohésion interne des modules et réduisent les jumelages entre modules. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 03(05) | Isolation des fonctions de sécurité | Isolation des fonctions de sécurité : Structures en couches<br>Appliquer les fonctions de sécurité dans une structure en couches qui permet de réduire les interactions entre les couches de la conception et d'éviter que les couches inférieures soient assujetties au bon fonctionnement des couches supérieures ou de leurs fonctions. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 04 | Information dans les ressources système partagées | Empêcher les transferts d'information non autorisés ou non prévus au moyen de ressources système partagées. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 04(01) | Information dans les ressources système partagées | Information dans les ressources système partagées : Niveaux de sécurité<br>Annulé : Intégré au contrôle SC-04. | s.o. | s.o. | s.o. | s.o. |
| SC | 04(02) | Information dans les ressources système partagées | Information dans les ressources système partagées : Traitement multiniveau ou des périodes<br>Prévenir le transfert non autorisé d'information par l'intermédiaire de ressources partagées conformément à [Affectation : procédures définies par l'organisation] lorsque le traitement exécuté par le système alterne explicitement entre divers niveaux de classification de l'information ou différentes catégories de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 05 | Protection contre les dénis de service | A. [Sélection (un choix) : Protéger contre; Limiter] les effets des types d'attaques par déni de service suivants : [Affectation : types d'attaque par déni de service définis par l'organisation]<br>B. Employer les contrôles suivants pour atteindre l'objectif de déni de service : [Affectation : contrôles définis par l'organisation par types d'attaque par déni de service] | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 05(01) | Protection contre les dénis de service | Protection contre les dénis de service : Restreindre la capacité de mener des attaques sur d'autres systèmes<br>Restreindre la capacité des individus à lancer les attaques par déni de service suivantes sur d'autres systèmes : [Affectation : attaques par déni de service définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 05(02) | Protection contre les dénis de service | Protection contre les dénis de service : Capacité, bande passante et redondance<br>Gérer l'excédent de capacité et de largeur de bande, ou toute autre redondance, afin de limiter les effets d'attaques par déni de service avec inondation d'information. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 05(03) | Protection contre les dénis de service | Protection contre les dénis de service : Détection et surveillance<br>a. Utiliser les outils de surveillance suivants pour détecter les indicateurs d'attaques par déni de service visant le système ou lancées à partir de celui-ci : [Affectation : outils de surveillance définis par l'organisation]<br>b. Surveiller les ressources système suivantes pour déterminer si elles sont suffisantes pour prévenir les attaques par déni de service fructueuses : [Affectation : ressources du système définies par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 06 | Disponibilité des ressources | Garantir la disponibilité des ressources en attribuant [Affectation : ressources définies par l'organisation] en fonction de [Sélection (un choix ou plus) : priorité; quota; [Affectation : contrôles définis par l'organisation]]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07 | Protection des frontières | A. Surveiller et contrôler les communications des interfaces externes gérées vers le système et celles des principales interfaces internes gérées au sein du système<br>B. Mettre en œuvre des sous-réseaux pour les composants de systèmes à accès public qui sont séparés [Sélection (un choix) : physiquement ou logiquement] des réseaux internes de l'organisation<br>C. Se connecter aux réseaux ou aux systèmes externes uniquement par des interfaces gérées qui sont dotées de mécanismes de protection des frontières répartis conformément à l'architecture de sécurité et de protection de la vie privée de l'organisation | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(01) | Protection des frontières | Protection des frontières : Sous-réseaux séparés physiquement<br>Annulé : Intégré au contrôle SC-07. | s.o. | s.o. | s.o. | s.o. |
| SC | 07(02) | Protection des frontières | Protection des frontières : Accès public<br>Annulé : Intégré au contrôle SC-07. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 07(03) | Protection des frontières | Protection des frontières : Points d'accès<br>Limiter le nombre de connexions réseau externes au système. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(04) | Protection des frontières | Protection des frontières : Services de télécommunications externes<br>a. Appliquer une interface gérée à chaque service de télécommunications externe<br>b. Établir une stratégie de flux de trafic pour chaque interface gérée<br>c. Protéger la confidentialité et l'intégrité de l'information transmise par l'intermédiaire des interfaces<br>d. Documenter chaque exception à la stratégie de flux de trafic en précisant le besoin de la mission ou de l'activité donnant lieu à l'exception et la durée de ce besoin<br>e. Examiner les exceptions à la stratégie relative aux flux de trafic [Affectation : fréquence définie par l'organisation] et retrancher les exceptions qui ne sont plus justifiées par un besoin lié à la mission ou aux activités<br>f. Prévenir l'échange non autorisé du trafic du plan de contrôle avec des réseaux externes<br>g. Publier de l'information pour permettre aux réseaux distants de détecter le trafic du plan de contrôle non autorisé depuis les réseaux internes<br>h. Filtrer le trafic du plan de contrôle en provenance des réseaux externes | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(05) | Protection des frontières | Protection des frontières : Refus par défaut – Autorisation par exception<br>Refuser par défaut le trafic de communications réseau et permettre le trafic de communications réseau au moyen d'exceptions [Sélection (un choix ou plus) : à proximité des interfaces gérées; pour [Affectation : systèmes définis par l'organisation]]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(06) | Protection des frontières | Protection des frontières : Réponse aux échecs reconnus<br>Annulé : Intégré au contrôle SC-07(18). | s.o. | s.o. | s.o. | s.o. |
| SC | 07(07) | Protection des frontières | Protection des frontières : Tunnellisation partagée pour les appareils distants<br>Prévenir la tunnellisation partagée pour les dispositifs distants qui se connectent à des systèmes organisationnels à moins que le tunnel partagé soit fourni de façon sécurisée au moyen de [Affectation : mesures de protection définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(08) | Protection des frontières | Protection des frontières : Acheminement du trafic vers des serveurs mandataires authentifiés<br>Acheminer [Affectation : trafic de communications internes défini par l'organisation] vers [Affectation : réseaux externes désignés par l'organisation] par l'intermédiaire de serveurs mandataires authentifiés à proximité des interfaces gérées. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(09) | Protection des frontières | Protection des frontières : Restriction du trafic de communications malveillant sortant<br>a. Détecter et bloquer le trafic de communications sortant susceptible de constituer une menace pour les systèmes externes<br>b. Vérifier l'identité des utilisatrices et utilisateurs internes associés aux communications bloquées | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(10) | Protection des frontières | Protection des frontières : Prévention de l'exfiltration<br>a. Prévenir l'exfiltration de l'information<br>b. Procéder à des tests d'exfiltration [Affectation : fréquence définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(11) | Protection des frontières | Protection des frontières : Restrictions du trafic de communications entrant<br>Faire en sorte que seules les communications entrantes provenant de [Affectation : sources autorisées désignées par l'organisation] puissent être acheminées vers [Affectation : destinations autorisées désignées par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 07(12) | Protection des frontières | Protection des frontières : Protection au niveau de l'hôte<br>Mettre en œuvre [Affectation : mécanismes de protection de la frontière au niveau de l'hôte définis par l'organisation] à [Affectation : composants des systèmes désignés par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(13) | Protection des frontières | Protection des frontières : Isolation des outils de sécurité, des mécanismes et des composants de soutien<br>Isoler les [Affectation : principaux outils, mécanismes et composants de soutien de la sécurité de l'information désignés par l'organisation] des autres composants internes du système au moyen de sous-réseaux physiques distincts dotés d'interfaces gérées tournées vers les autres parties du système. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 07(14) | Protection des frontières | Protection des frontières : Protection contre les connexions physiques non autorisées<br>Assurer une protection contre les connexions physiques non autorisées à [Affectation : interfaces gérées désignées par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(15) | Protection des frontières | Protection des frontières : Accès privilégiés aux réseaux<br>Acheminer tous les accès réseau privilégiés par l'intermédiaire d'une interface gérée spécialisée aux fins de contrôle des accès et de vérification. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(16) | Protection des frontières | Protection des frontières : Prévention de la découverte de composants de systèmes<br>Prévenir la découverte des composants de systèmes particuliers qui représentent une interface gérée. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(17) | Protection des frontières | Protection des frontières : Application automatisée des formats de protocoles<br>Appliquer la stricte adhésion aux formats de protocoles. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(18) | Protection des frontières | Protection des frontières : Fonctionnement à sécurité intégrée<br>Éviter que les systèmes passent en mode non sécurisé dans l'éventualité de la défaillance opérationnelle d'un dispositif de protection des frontières. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(19) | Protection des frontières | Protection des frontières : Blocage des communications provenant d'hôtes non configurés par l'organisme<br>Bloquer le trafic de communications entrant et sortant entre [Affectation : clients en communication désignés par l'organisation] qui est configuré indépendamment par les utilisatrices, les utilisateurs et les fournisseurs de services externes. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(20) | Protection des frontières | Protection des frontières : Isolation dynamique et séparation<br>Fournir la capacité d'isoler dynamiquement [Affectation : composants de systèmes désignés par l'organisation] des autres composants de systèmes. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(21) | Protection des frontières | Protection des frontières : Isolation des composants de systèmes<br>Avoir recours à des mécanismes de protection de la frontière dans le but de séparer [Affectation : composants du système désignés par l'organisation] assurant le soutien aux [Affectation : fonctions liées à la mission et aux activités définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(22) | Protection des frontières | Protection des frontières : Sous-réseaux distincts pour la connexion à des domaines de sécurité différents<br>Appliquer des adresses réseau distinctes pour établir une connexion à des systèmes se trouvant dans des domaines de sécurité différents. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 07(23) | Protection des frontières | Protection des frontières : Désactivation de la rétroaction à l'expéditrice ou expéditeur après l'échec de validation d'un protocole<br>Désactiver la fonction de rétroaction à l'expéditrice ou expéditeur advenant l'échec de la validation d'un format de protocole. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(24) | Protection des frontières | Protection des frontières : Renseignements personnels<br>Pour les systèmes qui traitent des renseignements personnels<br>a. appliquer les règles de traitement suivantes aux éléments de données des renseignements personnels : [Affectation : règles de traitement définies par l'organisation]<br>b. surveiller le traitement autorisé dans les interfaces externes du système et à ses principales frontières internes<br>c. documenter chaque exception à la règle de traitement<br>d. examiner et supprimer les exceptions qui ne sont plus prises en charge | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(25) | Protection des frontières | Protection des frontières : Connexions à des systèmes de sécurité nationaux non classifiés<br>Interdire toute connexion directe de [Affectation : système de sécurité national non classifié désigné par l'organisation] à un réseau externe sans utiliser [Affectation : dispositif de protection des frontières désigné par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(26) | Protection des frontières | Protection des frontières : Connexions à des systèmes de sécurité nationaux classifiés<br>Interdire toute connexion directe de [Affectation : système de sécurité national classifié désigné par l'organisation] à un réseau externe sans utiliser [Affectation : dispositif de protection des frontières désigné par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(27) | Protection des frontières | Protection des frontières : Connexions à des systèmes de sécurité non nationaux non classifiés<br>Interdire toute connexion directe de [Affectation : système de sécurité non national non classifié désigné par l'organisation] à un réseau externe sans utiliser [Affectation : dispositif de protection des frontières désigné par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(28) | Protection des frontières | Protection des frontières : Connexions aux réseaux publics<br>Interdire toute connexion directe de [Affectation : système désigné par l'organisation] à un réseau public. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 07(29) | Protection des frontières | Protection des frontières : Séparation des sous-réseaux pour l'isolation des fonctions<br>Mettre en œuvre [Sélection (un choix) : physiquement; logiquement] des sous-réseaux distincts pour isoler les fonctions et les composants de systèmes critiques suivants : [Affectation : composants et fonctions de systèmes essentiels définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 08 | Confidentialité et intégrité des transmissions | Protéger [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information transmise. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 08(01) | Confidentialité et intégrité des transmissions | Confidentialité et intégrité des transmissions : Protection cryptographique<br>Mettre en œuvre des mécanismes de chiffrement pour [Sélection (un choix ou plus) : prévenir la divulgation non autorisée d'information; détecter les modifications apportées à l'information] durant la transmission. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 08(02) | Confidentialité et intégrité des transmissions | Confidentialité et intégrité des transmissions : Traitement pré-transmission et post-transmission<br>Maintenir [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information au cours de la préparation à la transmission et pendant la réception. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 08(03) | Confidentialité et intégrité des transmissions | Confidentialité et intégrité des transmissions : Protection cryptographique pour les éléments complémentaires des messages<br>Appliquer des mécanismes visant à protéger les éléments complémentaires des messages, sauf si l'information est protégée par [Affectation : autres mesures de protection physique définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 08(04) | Confidentialité et intégrité des transmissions | Confidentialité et intégrité des transmissions : Dissimulation et distribution aléatoire des communications<br>Appliquer des mécanismes cryptographiques visant à protéger ou à distribuer aléatoirement les schémas de communication, sauf si l'information est protégée par [Affectation : autres contrôles physiques définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 08(05) | Confidentialité et intégrité des transmissions | Confidentialité et intégrité des transmissions : Système de distribution protégé<br>Mettre en œuvre [Affectation : système de distribution protégé désigné par l'organisation] pour [Sélection (un choix ou plus) : prévenir la divulgation non autorisée d'information; détecter les modifications apportées à l'information] durant la transmission. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 09 | Confidentialité des transmissions | Annulé : Intégré au contrôle SC-08. | s.o. | s.o. | s.o. | s.o. |
| SC | 10 | Déconnexion du réseau | Mettre fin à la connexion réseau associée à la session de communication à la fin de la session ou après [Affectation : période définie par l'organisation] d'inactivité. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 11 | Chemin de confiance | A. Fournir un chemin de communication de confiance isolé [Sélection (un choix) : physiquement; logiquement] pour établir les communications entre les utilisatrices et utilisateurs et les composants fiables du système<br>B. Permettre aux utilisatrices et utilisateurs d'invoquer le chemin de communication de confiance pour les communications entre l'utilisatrice ou utilisateur et les fonctions de sécurité suivantes du système qui incluent, au minimum, l'authentification et la réauthentification : [Affectation : fonctions de sécurité définies par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 11(01) | Chemin de confiance | Chemin de confiance : Chemin de communication irréfutable<br>a. Fournir un chemin de communication de confiance qui est irréfutablement distinct des autres chemins de communication<br>b. Amorcer le chemin de communication de confiance pour les communications entre les [Affectation : fonctions de sécurité définies par l'organisation] du système et l'utilisatrice ou utilisateur | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 12 | Établissement et gestion des clés cryptographi-ques | Établir et gérer les clés cryptographiques lorsque la cryptographie est utilisée dans le système conformément aux exigences de gestion de clés suivantes : [Affectation : exigences définies par l'organisation liées à la génération, à la distribution, au stockage, à l'accès et à la destruction des clés]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 12(01) | Établissement et gestion des clés cryptographi-ques | Établissement et gestion des clés cryptographiques : Disponibilité<br>Maintenir la disponibilité de l'information dans l'éventualité où les utilisatrices et utilisateurs perdent leurs clés cryptographiques. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 12(02) | Établissement et gestion des clés cryptographi-ques | Établissement et gestion des clés cryptographiques : Clés symétriques<br>Produire, contrôler et distribuer les clés cryptographiques symétriques en faisant appel à une technologie et à des processus de gestion des clés [Sélection (un choix) : validés par le PVMC; approuvés par le Centre pour la cybersécurité; avec matériel de chiffrement préplacé]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 12(03) | Établissement et gestion des clés cryptographi-ques | Établissement et gestion des clés cryptographiques : Clés asymétriques<br>Produire, contrôler et distribuer les clés cryptographiques asymétriques en faisant appel à [Sélection (un choix) : des processus de gestion des clés approuvés par le Centre pour la cybersécurité; du matériel de chiffrement préplacé; des certificats d'infrastructure à clé publique (ICP) à assurance moyenne approuvés ou émis par le Centre pour la cybersécurité; des certificats d'ICP et des jetons de sécurité matériels qui protègent la clé privée de l'utilisatrice ou utilisateur; des certificats émis conformément aux exigences définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 12(04) | Établissement et gestion des clés cryptographi-ques | Établissement et gestion des clés cryptographiques : Certificats d'ICP<br>Annulé : Intégré au contrôle SC-12(03). | s.o. | s.o. | s.o. | s.o. |
| SC | 12(05) | Établissement et gestion des clés cryptographi-ques | Établissement et gestion des clés cryptographiques : Certificats d'ICP et jetons matériels<br>Annulé : Intégré au contrôle SC-12(03). | s.o. | s.o. | s.o. | s.o. |
| SC | 12(06) | Établissement et gestion des clés cryptographi-ques | Établissement et gestion des clés cryptographiques : Contrôle physique des clés<br>Assurer le contrôle physique des clés cryptographiques lorsque l'information stockée est chiffrée par des fournisseurs de services externes. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 13 | Protection cryptographi-que | A. Déterminer les [Affectation : utilisations cryptographiques définies par l'organisation]<br>B. Mettre en place les types de cryptographies nécessaires à chaque utilisation cryptographique indiquée : [Affectation : types de cryptographies définis par l'organisation pour chaque utilisation cryptographique indiquée] | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 13(01) | Protection cryptographique | Protection cryptographique : Cryptographie homologuée FIPS<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(02) | Protection cryptographique | Protection cryptographique : Cryptographie approuvée par la National Security Agency (NSA)<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(03) | Protection cryptographique | Protection cryptographique : Personnes ne disposant pas des approbations formelles d'accès<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(04) | Protection cryptographique | Protection cryptographique : Signatures numériques<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 13(400) | Protection cryptographique | Protection cryptographique : Données en transit PROTÉGÉ A<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(401) | Protection cryptographique | Protection cryptographique : Données en transit PROTÉGÉ B<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(402) | Protection cryptographique | Protection cryptographique : Données en transit PROTÉGÉ C<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(403) | Protection cryptographique | Protection cryptographique : Données au repos protégées<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 13(404) | Protection cryptographique | Protection cryptographique : Systèmes de sécurité nationale<br>Annulé : Intégré au contrôle SC-13. | s.o. | s.o. | s.o. | s.o. |
| SC | 14 | Protection de l'accès public | Annulé : Intégré aux contrôles AC-02, AC-03, AC-05, AC-06, SI-03, SI-04, SI-05, SI-07 et SI-10. | s.o. | s.o. | s.o. | s.o. |
| SC | 15 | Applications et dispositifs d'informatique collaborative | A. Empêcher l'activation à distance des applications et des dispositifs d'informatique collaborative, sauf pour les exceptions suivantes : [Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise]<br>B. Indiquer de manière explicite l'utilisation permise pour les utilisatrices et utilisateurs qui se trouvent physiquement à proximité des dispositifs | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 15(01) | Applications et dispositifs d'informatique collaborative | Applications et dispositifs d'informatique collaborative : Déconnexion physique ou logique<br>Permettre la déconnexion [Sélection (un choix ou plus) : physique; logique] des dispositifs d'informatique coopérative de manière à assurer la convivialité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 15(02) | Applications et dispositifs d'informatique collaborative | Applications et dispositifs d'informatique collaborative : Blocage du trafic de communications entrant et sortant<br>Annulé : Intégré au contrôle SC-07. | s.o. | s.o. | s.o. | s.o. |
| SC | 15(03) | Applications et dispositifs d'informatique collaborative | Applications et dispositifs d'informatique collaborative : Désactivation et retrait dans les zones de travail sécurisées<br>Désactiver ou retirer les applications et dispositifs d'informatique collaborative sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] dans [Affectation : zones de travail sécurisées désignées par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 15(04) | Applications et dispositifs d'informatique collaborative | Applications et dispositifs d'informatique collaborative : Indication explicite des participantes et participants<br>Fournir une indication explicite des participantes et participants actuels de [Affectation : réunions et téléconférences désignées par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 16 | Transmission des attributs de sécurité et de | Associer [Affectation : attributs de sécurité et de protection de la vie privée définis par l'organisation] à l'information échangée entre les systèmes et les composants du système. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | protection de la vie privée | | | | | |
| SC | 16(01) | Transmission des attributs de sécurité et de protection de la vie privée | Transmission des attributs de sécurité et de protection de la vie privée : Vérification de l'intégrité<br>Vérifier l'intégrité des attributs de sécurité et de protection de la vie privée transmis. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 16(02) | Transmission des attributs de sécurité et de protection de la vie privée | Transmission des attributs de sécurité et de protection de la vie privée : Mécanismes anti-usurpation<br>Mettre en place des mécanismes anti-usurpation pour empêcher les adversaires de falsifier les attributs de sécurité qui indiquent l'application réussie du processus de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 16(03) | Transmission des attributs de sécurité et de protection de la vie privée | Transmission des attributs de sécurité et de protection de la vie privée : Liaison cryptographique<br>Mettre en œuvre [Affectation : mécanismes ou techniques définis par l'organisation] pour lier les attributs de sécurité et de protection de la vie privée à l'information transmise. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 17 | Certificats d'infrastructure à clé publique | A. Émettre des certificats à clé publique en vertu de [Affectation : stratégie de certification définie par l'organisation] ou les obtenir auprès d'un fournisseur de services autorisé<br>B. Inclure uniquement les ancrages de confiance approuvés dans les magasins de confiance ou les magasins de certificats gérés par l'organisation | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 18 | Code mobile | A. Définir le code mobile et les technologies de code mobile acceptables et inacceptables<br>B. Autoriser, surveiller et contrôler l'utilisation de code mobile sur le système | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 18(01) | Code mobile | Code mobile : Établissement du code inadéquat et application de mesures correctives<br>Identifier [Affectation : code mobile inadéquat défini par l'organisation] et prendre [Affectation : mesures correctives définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 18(02) | Code mobile | Code mobile : Acquisition, développement et utilisation<br>Veiller à ce que l'acquisition, le développement ou l'utilisation du code mobile à déployer dans les systèmes répondent aux [Affectation : exigences relatives au code mobile définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 18(03) | Code mobile | Code mobile : Prévention du téléchargement et de l'exécution<br>Prévenir le téléchargement et l'exécution de [Affectation : code mobile inadéquat défini par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 18(04) | Code mobile | Code mobile : Prévention de l'exécution automatique<br>Empêcher l'exécution automatique de code mobile dans [Affectation : applications logicielles désignées par l'organisation] et exiger que [Affectation : mesures définies par l'organisation] soient prises avant d'exécuter le code. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 18(05) | Code mobile | Code mobile : Autoriser l'exécution dans les environnements clos seulement<br>Permettre l'exécution de code mobile autorisé uniquement dans les environnements clos de machines virtuelles. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 19 | Voix sur IP | A. L'organisation définit les restrictions d'utilisation et donne des conseils sur la mise en œuvre des technologies de voix sur protocole Internet (VoIP pour *Voice over Internet Protocol*) en tenant compte de la possibilité qu'une utilisation malveillante de ces technologies cause des dommages au système d'information<br>B. L'organisation autorise, surveille et contrôle l'utilisation de la voix sur IP dans le système d'information | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 19(400) | Voix sur IP | Voix sur IP : Conversion de protocole<br>Il est interdit d'utiliser un service de VoIP non classifié dans des installations classifiées, sauf si ce service est converti en service téléphonique traditionnel (POTS pour *Plain Old Telephone Service*) avant de sortir des limites de l'installation. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 19(401) | Voix sur IP | Voix sur IP : Aucun accès au réseau public<br>Dans les installations classifiées, il est interdit d'utiliser un service de VoIP non classifié dans un réseau local ayant accès à un réseau de données public. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 20 | Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) | A. Fournir des éléments additionnels d'information sur l'authentification de l'origine des données et sur la vérification de leur intégrité, en plus des données de résolution de nom faisant autorité, que le système retourne en réponse aux requêtes externes de résolution de nom ou d'adresse<br>B. Offrir des moyens d'indiquer l'état de sécurité des zones enfants et (si l'enfant prend en charge des services sécurisés de résolution) de vérifier l'existence d'une chaîne de confiance entre les domaines parents et enfants lorsque le système est utilisé dans un espace de nom hiérarchique distribué | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 20(01) | Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) | Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) : Zones enfants<br>Annulé : Intégré au contrôle SC-20. | s.o. | s.o. | s.o. | s.o. |
| SC | 20(02) | Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) | Service sécurisé de résolution de nom ou d'adresse (source faisant autorité) : Intégrité et origine des données<br>Fournir les artéfacts de protection de l'intégrité et de l'origine des données pour les requêtes internes de résolution de nom ou d'adresse. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 21 | Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache) | Soumettre une requête, puis authentifier l'origine et vérifier l'intégrité des données des réponses de la résolution de nom et d'adresse que le système reçoit de sources faisant autorité. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 21(01) | Service sécurisé de résolution de nom ou d'adresse | Service sécurisé de résolution de nom ou d'adresse (résolveur récursif ou cache) : Intégrité et origine des données<br>Annulé : Intégré au contrôle SC-21. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | (résolveur récursif ou cache) | | | | | |
| SC | 22 | Architecture et prestation de services de résolution de nom ou d'adresse | S'assurer que les systèmes qui offrent collectivement des services de résolution de nom et d'adresse pour une organisation sont tolérants aux pannes et appliquent une séparation des rôles internes et externes. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 23 | Authenticité des sessions | Protéger l'authenticité des sessions de communication. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 23(01) | Authenticité des sessions | Authenticité des sessions : Annulation de la validation des identificateurs de session lors de la fermeture de session<br>Invalider les identificateurs de session lorsque l'utilisatrice ou utilisateur ferme sa session ou lorsque la session est terminée autrement. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 23(02) | Authenticité des sessions | Authenticité des sessions : Fermetures de session exécutées par les utilisatrices et utilisateurs et affichage de messages<br>Annulé : Intégré au contrôle AC-12(01). | s.o. | s.o. | s.o. | s.o. |
| SC | 23(03) | Authenticité des sessions | Authenticité des sessions : Identificateurs de session uniques générés par le système<br>Générer un identificateur de session unique pour chaque session avec [Affectation : exigences relatives à la randomisation définies par l'organisation] et reconnaître uniquement les identificateurs générés par le système. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 23(04) | Authenticité des sessions | Authenticité des sessions : Identificateurs de session uniques avec randomisation<br>Annulé : Intégré au contrôle SC-23(03). | s.o. | s.o. | s.o. | s.o. |
| SC | 23(05) | Authenticité des sessions | Authenticité des sessions : Autorités de certification homologuées<br>Permettre uniquement l'utilisation de [Affectation : autorités de certification désignées par l'organisation] à des fins de vérification de l'établissement de sessions protégées. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 24 | Défaillance dans un état connu | Échec de [Affectation : état connu du système défini par l'organisation] pour les défaillances suivantes des composants indiqués tout en préservant [Affectation : information relative à l'état du système définie par l'organisation] en défaillance : [Affectation : liste des types de défaillances du système définis par l'organisation sur les composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 25 | Nœuds légers | Employer un minimum de fonctionnalités et de stockage d'information sur les composants de systèmes suivants : [Affectation : composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 26 | Leurres | Inclure des composants dans les systèmes organisationnels conçus spécifiquement pour servir de cibles aux attaques malveillantes dans le but de les détecter, de les repousser et de les analyser. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 26(01) | Leurres | Leurres : Détection de code malveillant<br>Annulé : Intégré au contrôle SC-35. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 27 | Applications indépendantes des plateformes | Inclure dans les systèmes organisationnels les applications qui sont indépendantes des plateformes suivantes : [Affectation : applications définies par l'organisation qui sont indépendantes des plateformes]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 28 | Protection de l'information au repos | Protéger [Sélection (un choix ou plus) : la confidentialité; l'intégrité] de l'information au repos suivante : [Affectation : information au repos définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 28(01) | Protection de l'information au repos | Protection de l'information au repos : Protection cryptographique<br>Mettre en place des mécanismes cryptographiques visant à prévenir la divulgation et la modification non autorisées de l'information au repos suivante sur [Affectation : composants de systèmes ou supports désignés par l'organisation] : [Affectation : information définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 28(02) | Protection de l'information au repos | Protection de l'information au repos : Stockage hors ligne<br>Supprimer l'information suivante des dispositifs de stockage en ligne et la stocker hors ligne dans des lieux sécurisés : [Affectation : information définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 28(03) | Protection de l'information au repos | Protection de l'information au repos : Clés cryptographiques<br>Protéger le stockage des clés cryptographiques [Sélection (un choix) : [Affectation : mesures de protection définies par l'organisation]; magasin de clés avec protection matérielle]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 29 | Hétérogénéité | Employer un ensemble diversifié de technologies de l'information pour les composants de systèmes pendant la mise en œuvre du système : [Affectation : composants de systèmes désignés par l'organisation]. | Contrôle | Sélectionné | [dispositifs et outils de cybersécurité] | Pour protéger le profil PBMM contre les compromissions Md4 ayant recours à un seul défaut de système inconnu (une vulnérabilité du jour zéro), désagréger les fonctions opérationnelles entre les systèmes qui ne partagent aucun point de défaillance unique. Par exemple, héberger une base de données du secteur d'activités dans Windows et une base de données différente dans Linux. |
| SC | 29(01) | Hétérogénéité | Hétérogénéité : Techniques de virtualisation<br>Utiliser des techniques de virtualisation pour faciliter le déploiement de divers systèmes d'exploitation et de diverses applications faisant l'objet de changements [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 30 | Dissimulation et détournement | Employer les techniques de dissimulation et de détournement suivantes pour [Affectation : systèmes désignés par l'organisation] à [Affectation : périodes définies par l'organisation] : [Affectation : techniques de dissimulation et de détournement définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 30(01) | Dissimulation et détournement | Dissimulation et détournement : Techniques de virtualisation<br>Annulé : Intégré au contrôle SC-29(01). | s.o. | s.o. | s.o. | s.o. |
| SC | 30(02) | Dissimulation et détournement | Dissimulation et détournement : Facteur aléatoire<br>Employer [Affectation : techniques définies par l'organisation] pour introduire le facteur aléatoire dans la gestion des activités et des biens organisationnels. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 30(03) | Dissimulation et détournement | Dissimulation et détournement : Changement des lieux de traitement et de stockage<br>Changer l'emplacement du [Affectation : traitement et/ou stockage défini par l'organisation] [Sélection (un choix) : [Affectation : fréquence définie par l'organisation]; à intervalles irréguliers]]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 30(04) | Dissimulation et détournement | Dissimulation et détournement : Information trompeuse<br>Employer de l'information en apparence réelle, mais en définitive trompeuse, dans [Affectation : composants de systèmes désignés par l'organisation] au sujet de leur posture et de leurs mesures de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 30(05) | Dissimulation et détournement | Dissimulation et détournement : Dissimulation des composants de systèmes<br>Employer les techniques suivantes pour cacher ou dissimuler [Affectation : composants de systèmes désignés par l'organisation] : [Affectation : techniques définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 31 | Analyse des voies clandestines | A. Procéder à une analyse des voies clandestines dans le but d'identifier les éléments du système qui pourraient éventuellement constituer des voies clandestines de [Sélection (un choix ou plus) : stockage; synchronisation temporelle]<br>B. Évaluer la bande passante maximale de ces voies | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 31(01) | Analyse des voies clandestines | Analyse des voies clandestines : Test d'exploitabilité des voies clandestines<br>Tester un sous-ensemble de voies clandestines identifiées afin de savoir quelles voies s'avèrent exploitables. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 31(02) | Analyse des voies clandestines | Analyse des voies clandestines : Bande passante maximale<br>Réduire la bande passante maximale pour certaines voies clandestines de [Sélection (un choix ou plus) : stockage; synchronisation temporelle] à [Affectation : valeurs définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 31(03) | Analyse des voies clandestines | Analyse des voies clandestines : Mesure de la bande passante dans les environnements opérationnels<br>Mesurer la bande passante [Affectation : sous-ensemble de voies clandestines particulières défini par l'organisation] dans l'environnement opérationnel du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 32 | Partitionnement des systèmes | Partitionner le système en [Affectation : composants de systèmes désignés par l'organisation] résidant dans des domaines ou des environnements [Sélection (un choix) : physiques et logiques] basés sur [Affectation : circonstances propices à la séparation physique ou logique des composants définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 32(01) | Partitionnement des systèmes | Partitionnement des systèmes : Séparation des domaines physiques pour les fonctions privilégiées<br>Partitionner les fonctions privilégiées dans des domaines physiques distincts. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 33 | Intégrité de la préparation des transmissions | Annulé : Intégré au contrôle SC-08. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 34 | Programmes exécutables non modifiables | Pour les [Affectation : composants de systèmes désignés par l'organisation], charger et exécuter<br>A. l'environnement d'exploitation à partir de supports matériels non inscriptibles<br>B. les applications suivantes à partir de supports matériels non inscriptibles : [Affectation : applications désignées par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 34(01) | Programmes exécutables non modifiables | Programmes exécutables non modifiables : Dispositif de stockage non inscriptible<br>Utiliser [Affectation : composants de systèmes désignés par l'organisation] avec des dispositifs de stockage qui demeurent non inscriptibles à chaque redémarrage du composant ou lors des mises sous tension et hors tension. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 34(02) | Programmes exécutables non modifiables | Programmes exécutables non modifiables : Protection de l'intégrité et des supports non inscriptibles<br>Protéger l'intégrité de l'information avant son enregistrement dans les supports non inscriptibles et contrôler ces supports après l'enregistrement de l'information. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 34(03) | Programmes exécutables non modifiables | Programmes exécutables non modifiables : Protection matérielle<br>Annulé : Transféré sous le contrôle SC-51. | s.o. | s.o. | s.o. | s.o. |
| SC | 35 | Identification des programmes malveillants externes | Inclure les composants de systèmes qui tentent proactivement d'identifier les programmes malveillants en provenance du réseau ou les sites Web malveillants. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 36 | Traitement et stockage répartis | Répartir les composants de traitement et de stockage suivants dans plusieurs [Sélection (un choix) : lieux physiques; domaines logiques] : [Affectation : composants de traitement et de stockage désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 36(01) | Traitement et stockage répartis | Traitement et stockage répartis : Techniques de scrutation<br>a. Avoir recours à des techniques de scrutation pour relever les anomalies, les erreurs et les compromissions dans les composants de traitement et stockage suivants : [Affectation : composants de traitement et de stockage répartis désignés par l'organisation]<br>b. Prendre les mesures suivantes lorsque des anomalies, des erreurs ou des compromissions sont identifiées : [Affectation : actions définies par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 36(02) | Traitement et stockage répartis | Traitement et stockage répartis : Synchronisation<br>Synchroniser les systèmes ou les composants de systèmes suivants : [Affectation : systèmes ou composants de systèmes dupliqués désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 37 | Voies d'acheminement hors bande | Employer les voies d'acheminement hors bande suivantes pour la distribution physique ou la transmission électronique de [Affectation : information, composants de systèmes ou dispositifs désignés par l'organisation] à [Affectation : personnel ou systèmes désignés par l'organisation] : [Affectation : voies d'acheminement hors bande définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 37(01) | Voies d'acheminement hors bande | Voies d'acheminement hors bande : Assurance de la distribution et de la transmission<br>Employer [Affectation : contrôles définis par l'organisation] pour garantir que seuls [Affectation : personnel ou systèmes | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | désignés par l'organisation] reçoivent l'information, les composants de systèmes ou les dispositifs suivants : [Affectation : systèmes, composants de systèmes ou dispositifs désignés par l'organisation]. | | | | |
| SC | 38 | Sécurité des opérations | Employer les contrôles de sécurité des opérations suivants pour protéger l'information organisationnelle tout au long du cycle de vie de développement des systèmes : [Affectation : contrôles de sécurité des opérations définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 39 | Isolation des processus | Maintenir un domaine d'exécution distinct pour chaque processus exécuté sur le système. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 39(01) | Isolation des processus | Isolation des processus : Séparation du matériel<br>Mettre en place des mécanismes de séparation du matériel pour faciliter l'isolation des processus. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 39(02) | Isolation des processus | Isolation des processus : Domaine d'exécution distinct pour chaque fil d'exécution<br>Conserver un domaine d'exécution distinct pour chacun des fils d'exécution dans [Affectation : traitement multifil défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 40 | Protection des liaisons sans fil | Protéger les [Affectation : liaisons sans fil définies par l'organisation] externes et internes contre les attaques suivantes qui visent les paramètres de signaux : [Affectation : types de paramètres de signaux définis par l'organisation ou références aux sources de telles attaques]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 40(01) | Protection des liaisons sans fil | Protection des liaisons sans fil : Interférence électromagnétique<br>Mettre en œuvre des mécanismes cryptographiques visant à appliquer [Affectation : niveau de protection défini par l'organisation] dans le but de contrer les effets de l'interférence électromagnétique internationale. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 40(02) | Protection des liaisons sans fil | Protection des liaisons sans fil : Atténuation du potentiel de détection<br>Appliquer des mécanismes cryptographiques visant à réduire le potentiel de détection des liaisons sans fil [Affectation : niveau de réduction défini par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 40(03) | Protection des liaisons sans fil | Protection des liaisons sans fil : Déception des communications par imitation ou par manipulation<br>Mettre en œuvre des mécanismes cryptographiques visant à identifier et à rejeter les transmissions sans fil qui constituent des tentatives délibérées de communications trompeuses par imitation ou par manipulation, qui sont fondées sur des paramètres de signaux. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 40(04) | Protection des liaisons sans fil | Protection des liaisons sans fil : Identification des paramètres de signaux<br>Mettre en œuvre des mécanismes cryptographiques visant à prévenir l'identification des [Affectation : émetteurs sans fil désignés par l'organisation] par l'utilisation des paramètres de signaux d'un émetteur. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 41 | Accès des ports et des périphériques d'entrée et de sortie | Procéder à une désactivation ou à un retrait [Sélection (un choix) : physique; logique] de [Affectation : ports de connexion ou périphériques d'entrée et de sortie désignés par l'organisation] sur les systèmes ou les composants de systèmes suivants : [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 42 | Capacité des capteurs et données | A. Interdire [Sélection (un choix ou plus) : l'utilisation de dispositifs dotés de [Affectation : capacités de captation environnementale définies par l'organisation] dans [Affectation : installations, secteurs ou systèmes désignés par l'organisation]; l'activation à distance des capacités de captation environnementale sur les systèmes ou les composants de systèmes organisationnels, sauf pour les exceptions suivantes : [Affectation : exceptions définies par l'organisation | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | pour lesquelles l'activation à distance de capteurs est permise]]<br>B. Indiquer explicitement l'utilisation de capteurs pour [Affectation : groupes d'utilisatrices et utilisateurs désignés par l'organisation] | | | | |
| SC | 42(01) | Capacité des capteurs et données | Capacité des capteurs et données : Signalement auprès du personnel ou des rôles autorisés<br>Veiller à ce que le système soit configuré de telle sorte que l'information ou les données collectées par [Affectation : capteurs désignés par l'organisation] ne soit signalées qu'au personnel ou aux rôles autorisés à cette fin. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 42(02) | Capacité des capteurs et données | Capacité des capteurs et données : Utilisation autorisée<br>Employer les mesures suivantes pour que l'information ou les données collectées par [Affectation : capteurs désignés par l'organisation] ne soient utilisées qu'aux fins autorisées : [Affectation : mesures définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 42(03) | Capacité des capteurs et données | Capacité des capteurs et données : Dispositifs interdits d'utilisation<br>Annulé : Intégré au contrôle SC-42. | s.o. | s.o. | s.o. | s.o. |
| SC | 42(04) | Capacité des capteurs et données | Capacité des capteurs et données : Avis de collecte<br>Appliquer les mesures suivantes pour informer plus facilement les individus que leurs renseignements personnels ont été collectés par [Affectation : capteurs désignés par l'organisation] : [Affectation : mesures définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 42(05) | Capacité des capteurs et données | Capacité des capteurs et données : Minimisation de la collecte<br>Employer des [Affectation : capteurs désignés par l'organisation] qui sont configurés pour minimiser la collecte de renseignements non nécessaires sur les individus. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 42(400) | Capacité des capteurs et données | Capacité des capteurs et données : Désactivation des zones de sécurité et de haute sécurité<br>S'assurer que l'organisation désactive tous les capteurs sur tous les dispositifs si ces derniers ne sont pas autorisés à traiter de l'information au plus haut niveau de classification dans la zone de sécurité ou de haute sécurité dans laquelle ils se trouvent. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 43 | Restrictions relatives à l'utilisation | A. Établir des restrictions concernant l'utilisation et les directives en matière de mise en œuvre pour les composants de système suivants : [Affectation : composants de systèmes désignés par l'organisation]<br>B. Autoriser, surveiller et contrôler l'utilisation de tels composants sur le système | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 44 | Chambres de détonation | Employer une chambre de détonation dans [Affectation : système, composant de système ou lieu désigné par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 45 | Synchronisation temporelle des systèmes | Synchroniser les horloges des systèmes et des composants de systèmes. | Contrôle | Sélectionné | s.o. | s.o. |
| SC | 45(01) | Synchronisation temporelle des systèmes | Synchronisation temporelle des systèmes : Synchronisation avec une source de temps faisant autorité<br>a. Comparer les horloges système internes [Affectation : fréquence définie par l'organisation] en utilisant [Affectation : source de temps faisant autorité définie par l'organisation]<br>b. Synchroniser les horloges systèmes internes avec la source de temps faisant autorité si la différence temporelle est supérieure à [Affectation : période définie par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 45(02) | Synchronisation temporelle des systèmes | Synchronisation temporelle des systèmes : Deuxième source de temps faisant autorité<br>a. Déterminer une deuxième source de temps faisant autorité dans une région géographique différente de la première source de temps faisant autorité<br>b. Synchroniser les horloges système internes avec la deuxième source de temps faisant autorité si la première n'est pas disponible | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 46 | Application des stratégies interdomaines | Mettre en œuvre un mécanisme d'application des stratégies [Sélection (un choix) : physiquement; logiquement] entre les interfaces physiques et/ou réseau pour la connexion des domaines de sécurité. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 46(400) | Application des stratégies interdomaines | Application des stratégies interdomaines : Transfert manuel de données<br>Limiter l'utilisation du transfert manuel de données. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 47 | Chemins de communications secondaires | Mettre en place des [Affectation : chemins de communication secondaires définis par l'organisation] pour la fonction organisationnelle de commande et de contrôle et l'exploitation des systèmes. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 48 | Relocalisation des capteurs | Relocaliser [Affectation : capteurs et capacités de surveillance désignés par l'organisation] à [Affectation : emplacements désignés par l'organisation] dans les circonstances et les situations suivantes : [Affectation : conditions ou circonstances définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 48(01) | Relocalisation des capteurs | Relocalisation des capteurs : Relocalisation dynamique des capteurs ou des capacités de surveillance<br>Relocaliser dynamiquement [Affectation : capteurs et capacités de surveillance désignés par l'organisation] à [Affectation : emplacements désignés par l'organisation] dans les circonstances et les situations suivantes : [Affectation : conditions ou circonstances définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 49 | Application de la séparation et des stratégies matérielles | Mettre en œuvre des mécanismes pour l'application de la séparation et des stratégies matérielles entre [Affectation : domaines de sécurité définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 50 | Séparation imposée par logiciel et application de la stratégie | Mettre en œuvre des mécanismes pour la séparation imposée par logiciel et l'application de la stratégie entre [Affectation : domaines de sécurité définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 51 | Protection matérielle | A. Appliquer la protection d'écriture matérielle pour [Affectation : composants micrologiciels de systèmes désignés par l'organisation]<br>B. Mettre en œuvre des procédures particulières pour [Affectation : personnes autorisées désignées par l'organisation] à désactiver manuellement la protection d'écriture matérielle contre les modifications des micrologiciels et à réactiver la protection d'écriture avant de revenir au mode opérationnel | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 400 | Authentification de la source de l'entité | Le système d'information permet à la ou au destinataire d'un message de vérifier l'identificateur présumé de la source dans un message. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SC | 400(01) | Authentification de la source de l'entité | Authentification de la source de l'entité : Authentification de l'identifiant présumé<br>L'authentification de l'identifiant présumé du message repose sur la cryptographie. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 400(02) | Authentification de la source de l'entité | Authentification de la source de l'entité : Signature numérique<br>L'organisation utilise la cryptographie validée selon le Programme de validation des modules cryptographiques (PVMC) pour la génération et la vérification des signatures numériques. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 400(03) | Authentification de la source de l'entité | Authentification de la source de l'entité : Mise en œuvre de l'authentification<br>L'organisation utilise la cryptographie et les protocoles approuvés par le Centre pour la cybersécurité pour effectuer l'authentification. | Contrôle | Non sélectionné | s.o. | s.o. |
| SC | 401 | Systèmes de télécommunications non classifiés dans les installations sécurisées | A. Les systèmes de télécommunications non classifiés dans les installations sécurisées ne doivent ni laisser passer ni transmettre de discussions audio sensibles lorsqu'ils sont au repos et non utilisés. De plus, ils doivent être configurés de manière à en empêcher le contrôle ou l'activation externes. Les concepts de protection audio de type « combiné raccroché » mentionnés dans les publications 5002 et 5006 du CNSSI doivent être intégrés aux systèmes de télécommunications des installations sécurisées<br>B. Les systèmes et services téléphoniques non classifiés doivent être configurés de manière à empêcher les exploits techniques ou l'intrusion. De plus, ils doivent intégrer des contrôles d'accès physique et logiciels pour empêcher la divulgation ou la manipulation de la programmation système et des données stockées<br>C. L'organisation doit veiller à appliquer aux systèmes de télécommunications non classifiés les exigences particulières suivantes<br>1. assurer la protection audio de type « combiné raccroché » par l'utilisation d'équipement CNSSI 5006, de dispositifs de déconnexion approuvés CNSSI 5006, ou d'une configuration système CNSSI 5002 équivalente<br>2. assurer l'isolation par l'utilisation d'un système téléphonique informatisé doté d'un contrôle de configuration logicielle et matérielle, et d'un contrôle des rapports de vérification (enregistrement détaillé des données d'appel, rapports sur les données d'appel, etc.). La programmation système n'offre pas la capacité de placer ou de maintenir le combiné en position non raccrochée. La configuration du système doit faire en sorte d'identifier et d'atténuer toutes les vulnérabilités associées à l'état du combiné (raccroché ou non)<br>3. veiller à ce que l'équipement utilisé pour administrer les systèmes téléphoniques soit installé dans une zone dont l'accès est réservé au personnel autorisé Lorsque les terminaux d'administration locaux (d'un système téléphonique informatisé) ne sont pas ou ne peuvent pas être hébergés dans la zone contrôlée, ni protégés contre les manipulations non autorisées, alors l'utilisation d'un équipement téléphonique approuvé CNSSI 5006 doit être exigée, quelle que soit la configuration du système téléphonique informatisé<br>4. veiller à ne pas utiliser la maintenance à distance à l'extérieur des installations sécurisées<br>5. veiller à ne pas utiliser de téléphones à haut-parleur ni de systèmes d'audioconférences avec les systèmes de télécommunications non classifiés dans les installations sécurisées. Le CST peut approuver les exceptions à cette exigence dans le cas où l'isolation audio est suffisante entre ces systèmes et les autres pièces de discussion classifiée dans l'installation sécurisée et lorsque des procédures sont en place pour empêcher la transmission par inadvertance d'information classifiée<br>6. veiller à ce que les fonctions utilisées pour la messagerie vocale ou les systèmes unifiés de messagerie soient configurées de manière à empêcher l'accès non autorisé aux ports de diagnostic distants ou à la tonalité d'invitation à numéroter interne<br>7. veiller à ce que les répondeurs téléphoniques (TAD) et les télécopieurs ne comportent pas de fonctions qui présentent | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | des vulnérabilités sur le plan de la sécurité, comme la surveillance des locaux à distance, la programmation à distance ou autres fonctions similaires qui peuvent permettre un accès à distance aux sons de la pièce. Le CST doit donner son approbation avant l'installation ou l'utilisation de tels dispositifs<br>D. Tous les systèmes de télécommunications non classifiés et leurs infrastructures doivent être isolés physiquement et électriquement de tout système d'information ou de télécommunications classifié, conformément aux exigences du CNSS ou de toute autre norme de séparation appliquée au système d'information classifié en place<br>E. Il faut respecter les exigences de sécurité et les lignes directrices en matière d'installation formulées dans la publication CNSSI 5000 pour les systèmes de VoIP installés dans toute zone de sécurité physique où est traitée de l'information classifiée | | | | |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| SI | 01 | Politique et procédures d'intégrité de l'information et des systèmes | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique d'intégrité de l'information et des systèmes [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures visant à faciliter la mise en œuvre de la politique d'intégrité de l'information et des systèmes ainsi que des contrôles connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures d'intégrité de l'information et des systèmes<br>C. Passer en revue et mettre à jour, par rapport à l'intégrité de l'information et des systèmes,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| SI | 02 | Correction des défauts | A. Établir, signaler et corriger les défauts du système<br>B. Tester les mises à jour logicielles visant la correction des défauts pour en vérifier l'efficacité et les répercussions potentielles sur les systèmes avant leur application<br>C. Installer les mises à jour de sécurité appropriées des logiciels et des micrologiciels dans une période de [Affectation : période définie par l'organisation] suivant la date de publication des mises à jour<br>D. Intégrer la correction des défauts au processus de gestion des configurations de l'organisation | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 02(01) | Correction des défauts | Correction des défauts : Gestion centrale<br>Annulé : Intégré au contrôle PL-09. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 02(02) | Correction des défauts | Correction des défauts : État automatisé de la correction des défauts<br>Déterminer si les mises à jour logicielles et micrologicielles de sécurité pertinentes ont été installées sur les composants de systèmes au moyen de [Affectation : mécanismes automatisés désignés par l'organisation] [Affectation : fréquence définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 02(03) | Correction des défauts | Correction des défauts : Délais de correction des défauts et repères liés aux mesures correctives<br>a. Mesurer le temps écoulé entre la détection de l'anomalie et sa correction<br>b. Fixer les repères suivants pour la prise de mesures correctives : [Affectation : repères définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 02(04) | Correction des défauts | Correction des défauts : Outils automatisés de gestion des correctifs<br>Annulé : Intégré au contrôle SI-02. | s.o. | s.o. | s.o. | s.o. |
| SI | 02(05) | Correction des défauts | Correction des défauts : Mises à jour logicielles ou micrologicielles automatiques<br>Installer [Affectation : mises à jour logicielles et micrologicielles de sécurité pertinentes définies par l'organisation] automatiquement sur [Affectation : composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 02(06) | Correction des défauts | Correction des défauts : Retrait des versions antérieures des logiciels et des micrologiciels<br>Supprimer les versions antérieures de [Affectation : éléments logiciels et micrologiciels définis par l'organisation] une fois qu'une version mise à jour a été installée. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 03 | Protection contre les programmes malveillants | A. Mettre en œuvre des mécanismes de protection contre les programmes malveillants [Sélection (un choix ou plus) : basés sur les signatures; non basés sur les signatures) aux points d'entrée et de sortie du système afin de détecter et d'éliminer le code malveillant<br>B. Mettre à jour automatiquement les mécanismes de protection contre les programmes malveillants dès que de nouvelles versions sont disponibles, conformément à la stratégie et aux procédures organisationnelles de gestion des configurations<br>C. Configurer les mécanismes de protection contre les programmes malveillants de façon à<br>1. effectuer des analyses périodiques du système [Affectation : fréquence définie par l'organisation] et des analyses en temps réel des fichiers de sources externes aux [Sélection (un choix ou plus) : points d'extrémité; point d'entrée ou sortie du réseau] lors de leur téléchargement, de leur ouverture ou de leur exécution, conformément à la stratégie organisationnelle<br>2. [Sélection (un choix ou plus) : bloquer le code malveillant; mettre en quarantaine le code malveillant; effectuer [Affectation : action définie par l'organisation]]; et envoyer une alerte à [Affectation : personnel ou rôles définis par l'organisation] suivant la détection de code malveillant<br>D. Traiter les faux positifs résultant de la détection et de l'élimination de code malveillant et leurs répercussions potentielles sur la disponibilité des systèmes | Contrôle | Sélectionné | C. 1) fréquence [au moins tous les 30 jours]<br>C. 2) sélection [mettre en quarantaine le code malveillant] | s.o. |
| SI | 03(01) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Gestion centrale<br>Annulé : Intégré au contrôle PL-09. | s.o. | s.o. | s.o. | s.o. |
| SI | 03(02) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Mises à jour automatiques<br>Annulé : Intégré au contrôle SI-03. | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 03(03) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Utilisatrices ou utilisateurs non privilégiés<br>Annulé : Intégré au contrôle AC-06(10). | s.o. | s.o. | s.o. | s.o. |
| SI | 03(04) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Mises à jour effectuées seulement par des utilisatrices et utilisateurs privilégiés<br>Mettre à jour les mécanismes de protection contre les programmes malveillants uniquement lorsqu'une utilisatrice ou un utilisateur privilégié le demande. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 03(05) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Dispositifs de stockage portatifs<br>Annulé : Intégré au contrôle MP-07. | s.o. | s.o. | s.o. | s.o. |
| SI | 03(06) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Tests et vérifications<br>a. Tester les mécanismes de protection contre les programmes malveillants [Affectation : fréquence définie par l'organisation] en introduisant du code bénin connu dans le système<br>b. Vérifier que la détection du code et le signalement des incidents qui lui sont associés s'effectuent comme il se doit | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 03(07) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Détection non axée sur les signatures<br>Annulé : Intégré au contrôle SI-03. | s.o. | s.o. | s.o. | s.o. |
| SI | 03(08) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Détection des commandes non autorisées<br>a. Détecter les commandes non autorisées du système d'exploitation dans l'interface de programmation d'application du noyau de [Affectation : composants matériels des systèmes désignés par l'organisation] : [Affectation : commandes non autorisées du système d'exploitation définies par l'organisation]<br>b. [Sélection (un choix ou plus) : Émettre un avertissement; vérifier l'exécution de la commande; empêcher l'exécution de la commande] | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 03(09) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Authentification des commandes à distance<br>Annulé : Transféré sous le contrôle AC-17(10). | s.o. | s.o. | s.o. | s.o. |
| SI | 03(10) | Protection contre les programmes malveillants | Protection contre les programmes malveillants : Analyse des programmes malveillants<br>a. Employer des outils et des techniques pour analyser les caractéristiques et les comportements des programmes malveillants : [Affectation : techniques et outils définis par l'organisation]<br>b. Intégrer les résultats des analyses des programmes malveillants au processus d'intervention en cas d'incident et de correction des défauts de l'organisation | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04 | Surveillance des systèmes | A. Surveiller le système afin de détecter<br>1. des attaques et des signes indiquant de possibles attaques conformément aux objectifs de surveillance : [Affectation : objectifs de surveillance définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 2. des connexions locales, réseau ou à distance non autorisées<br>B. Détecter les utilisations non autorisées du système au moyen des techniques et des méthodes suivantes : [Affectation : techniques et méthodes définies par l'organisation]<br>C. Évoquer les capacités de surveillance interne ou déployer des dispositifs de surveillance<br>1. stratégiquement dans le système pour collecter l'information que l'organisation juge essentielle<br>2. de manière aléatoire pour faire le suivi des types de transactions qui l'intéressent particulièrement<br>D. Analyser les anomalies et les événements détectés<br>E. Ajuster le niveau d'activité de la surveillance du système lorsqu'il y a un changement dans le risque associé aux activités et aux biens organisationnels, aux individus, à d'autres organisations ou au Canada<br>F. Obtenir un avis juridique concernant les activités de surveillance des systèmes<br>G. Fournir [Affectation : renseignements liés à la surveillance du système définis par l'organisation] à [Affectation : personnel ou rôles définis par l'organisation] [Sélection (un choix ou plus) : au besoin; [Affectation : fréquence définie par l'organisation]] | | | | |
| SI | 04(01) | Surveillance des systèmes | Surveillance des systèmes : Système de détection d'intrusion dans l'ensemble du système<br>Connecter et configurer les outils individuels de détection d'intrusion en un système de détection panorganisationnel. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(02) | Surveillance des systèmes | Surveillance des systèmes : Outils et mécanismes automatisés aux fins d'analyse en temps réel<br>Utiliser des outils et mécanismes automatisés pour prendre en charge l'analyse des événements en temps quasi réel. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(03) | Surveillance des systèmes | Surveillance des systèmes : Intégration d'outils et de mécanismes automatisés<br>Employer des outils et des mécanismes automatisés afin d'intégrer des outils et mécanismes de détection d'intrusion dans les mécanismes de contrôle d'accès et de flux. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(04) | Surveillance des systèmes | Surveillance des systèmes : Trafic de communications entrant et sortant<br>a. Déterminer les critères à utiliser pour détecter les activités ou conditions inhabituelles ou non autorisées relatives au trafic de communications entrant et sortant<br>b. Surveiller le trafic de communications entrant et sortant [Affectation : fréquence définie par l'organisation] pour détecter toute [Affectation : activité ou condition inhabituelle ou non autorisée définie par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(05) | Surveillance des systèmes | Surveillance des systèmes : Alertes générées par le système<br>Alerter [Affectation : personnel ou rôles définis par l'organisation] lorsque les indications de compromission réelle ou potentielle suivantes se présentent : [Affectation : indicateurs de compromission définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(06) | Surveillance des systèmes | Surveillance des systèmes : Restriction des utilisatrices et utilisateurs non privilégiés<br>Annulé : Intégré au contrôle AC-06(10). | s.o. | s.o. | s.o. | s.o. |
| SI | 04(07) | Surveillance des systèmes | Surveillance des systèmes : Réponse automatisée à des événements suspects<br>a. Informer [Affectation : personnel responsable de l'intervention en cas d'incident désigné par l'organisation (par nom ou rôle)] des événements suspects ayant été détectés<br>b. Prendre les mesures suivantes lors de la détection : [Affectation : mesures les moins perturbatrices définies par l'organisation visant à mettre fin aux événements suspects] | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 04(08) | Surveillance des systèmes | Surveillance des systèmes : Protection de l'information de surveillance<br>Annulé : Intégré au contrôle SI-04. | s.o. | s.o. | s.o. | s.o. |
| SI | 04(09) | Surveillance des systèmes | Surveillance des systèmes : Mise à l'essai des outils et des mécanismes de surveillance<br>Mettre à l'essai les outils et les mécanismes de surveillance des intrusions [Affectation : fréquence définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(10) | Surveillance des systèmes | Surveillance des systèmes : Visibilité des communications chiffrées<br>Prendre les mesures nécessaires pour rendre [Affectation : trafic de communications chiffrées défini par l'organisation] visible aux [Affectation : mécanismes et outils de surveillance du système désignés par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(11) | Surveillance des systèmes | Surveillance des systèmes : Analyse des anomalies du trafic de communications<br>Analyser le trafic de communications sortant des interfaces externes au système et [Affectation : points internes dans le système définis par l'organisation] afin de relever les anomalies. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(12) | Surveillance des systèmes | Surveillance des systèmes : Alertes automatisées générées par l'organisation<br>Alerter [Affectation : personnel ou rôles définis par l'organisation] au moyen de [Affectation : mécanismes automatisés définis par l'organisation] lors de répercussions potentielles des activités inhabituelles ou inappropriées suivantes sur la sécurité ou la protection de la vie privée : [Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(13) | Surveillance des systèmes | Surveillance des systèmes : Analyse des modèles de trafic et d'événements<br>a. Analyser les modèles de trafic et d'événements pour le système<br>b. Développer des profils représentant les modèles de trafic et d'événements communs<br>c. Utiliser les profils de trafic et d'événements pour calibrer les dispositifs de surveillance des systèmes | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(14) | Surveillance des systèmes | Surveillance des systèmes : Détection d'intrusion sans fil<br>Utiliser un système de détection d'intrusions sans fil (WIDS pour *Wireless Intrusion Detection System*) pour identifier les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions ou infractions potentielles liées au système. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(15) | Surveillance des systèmes | Surveillance des systèmes : Communications entre un réseau sans fil et un réseau filaire<br>Utiliser un système de détection d'intrusion pour surveiller le trafic de communications sans fil lorsqu'il passe d'un réseau sans fil à un réseau filaire. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 04(16) | Surveillance des systèmes | Surveillance des systèmes : Corrélations entre les résultats des activités de surveillance<br>Établir des corrélations entre les outils et les mécanismes de surveillance employés dans l'ensemble du système. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(17) | Surveillance des systèmes | Surveillance des systèmes : Connaissance intégrée de la situation<br>Mettre en corrélation les résultats de la surveillance des activités physiques, des cyberactivités et des activités de la chaîne d'approvisionnement pour développer une connaissance intégrée de la situation à l'échelle organisationnelle. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 04(18) | Surveillance des systèmes | Surveillance des systèmes : Analyse du trafic et exfiltrations masquées<br>Analyser le trafic des communications sortant en destination des interfaces externes du système et des points intérieurs suivants pour y détecter des exfiltrations masquées d'information : [Affectation : points intérieurs dans le système définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(19) | Surveillance des systèmes | Surveillance des systèmes : Risque envers les personnes<br>Mettre en œuvre [Affectation : surveillance supplémentaire définie par l'organisation] des personnes qui ont été identifiées par [Affectation : sources définies par l'organisation], car elles représentent un plus grand risque. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(20) | Surveillance des systèmes | Surveillance des systèmes : Utilisatrice ou utilisateur privilégié<br>Mettre en œuvre la surveillance supplémentaire suivante des utilisatrices et utilisateurs privilégiés : [Affectation : surveillance supplémentaire définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(21) | Surveillance des systèmes | Surveillance des systèmes : Périodes d'essai<br>Mettre en œuvre la surveillance supplémentaire suivante des personnes pendant [Affectation : période probatoire définie par l'organisation] : [Affectation : surveillance supplémentaire définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(22) | Surveillance des systèmes | Surveillance des systèmes : Services réseau non autorisés<br>a. Détecter les services réseau qui n'ont pas été autorisés ou approuvés par [Affectation : processus d'autorisation et d'approbation définis par l'organisation]<br>b. [Sélection (un choix ou plus) : Vérifier; Alerter [Affectation : personnel ou rôles définis par l'organisation] lorsqu'une menace est détectée | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(23) | Surveillance des systèmes | Surveillance des systèmes : Dispositifs au niveau de l'hôte<br>Mettre en œuvre les mécanismes de surveillance au niveau de l'hôte suivants sur [Affectation : composants de systèmes désignés par l'organisation] : [Affectation : mécanismes de surveillance au niveau de l'hôte désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(24) | Surveillance des systèmes | Surveillance des systèmes : Indicateurs de compromission<br>Découvrir, collecter et distribuer à [Affectation : personnel ou rôles définis par l'organisation] les indicateurs de compromission fournis par [Affectation : sources définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 04(25) | Surveillance des systèmes | Surveillance des systèmes : Optimisation de l'analyse du trafic réseau<br>Fournir de la visibilité du trafic réseau aux interfaces des systèmes externes et internes clés afin d'optimiser l'efficacité des dispositifs de surveillance. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 05 | Alertes, avis et directives de sécurité | A. Recevoir régulièrement de [Affectation : organisations externes désignées par l'organisation] des alertes, des avis et des directives de sécurité concernant les systèmes<br>B. Générer les alertes, les avis et les directives de sécurité internes, au besoin<br>C. Diffuser les alertes, les avis et les directives de sécurité à : [Sélection (un choix ou plus) : [Affectation : personnel ou rôles définis par l'organisation]; [Affectation : éléments au sein de l'organisation définis par l'organisation]; [Affectation : organisations externes désignées par l'organisation]] | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | D. Mettre en œuvre les directives de sécurité dans les délais prescrits ou informer l'organisation émettrice du degré de non-respect | | | | |
| SI | 05(01) | Alertes, avis et directives de sécurité | Alertes, avis et directives de sécurité : Alertes et avis automatisés<br>Utiliser [Affectation : mécanismes automatisés définis par l'organisation] pour diffuser l'information contenue dans les alertes et les avis de sécurité à l'ensemble de l'organisation. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 06 | Vérification des fonctions de sécurité et de protection de la vie privée | A. Vérifier l'exploitation correcte de [Affectation : fonctions de sécurité et de confidentialité définies par l'organisation]<br>B. Procéder à la vérification des fonctions indiquées dans le contrôle SI-06A [Sélection (un choix ou plus) : [Affectation : états transitionnels du système définis par l'organisation]; à la demande d'une utilisatrice ou un utilisateur qui possède les privilèges appropriés; [Affectation : période définie par l'organisation]]<br>C. Alerter [Affectation : personnel ou rôles définis par l'organisation] advenant l'échec des tests de vérification de la sécurité et de la protection de la vie privée<br>D. [Sélection (un choix ou plus) : Arrêter le système; redémarrer le système; [Affectation : autres mesures définies par l'organisation]] lorsque des anomalies sont relevées | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 06(01) | Vérification des fonctions de sécurité et de protection de la vie privée | Vérification des fonctions de sécurité et de protection de la vie privée : Notification des tests de sécurité infructueux<br>Annulé : Intégré au contrôle SI-06. | s.o. | s.o. | s.o. | s.o. |
| SI | 06(02) | Vérification des fonctions de sécurité et de protection de la vie privée | Vérification des fonctions de sécurité et de protection de la vie privée : Soutien automatisé pour les tests distribués<br>Mettre en œuvre des mécanismes automatisés pour soutenir la gestion des tests distribués des fonctions de sécurité et de protection de la vie privée. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 06(03) | Vérification des fonctions de sécurité et de protection de la vie privée | Vérification des fonctions de sécurité et de protection de la vie privée : Rapports sur les résultats des vérifications<br>Faire rapport des résultats de la vérification des fonctions de sécurité et de protection de la vie privée à [Affectation : personnel ou rôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07 | Intégrité des logiciels, des micrologiciels et de l'information | A. Employer des outils de vérification pour détecter les changements non autorisés qui sont apportés aux logiciels, aux micrologiciels et à l'information suivants : [Affectation : logiciels, micrologiciels et information désignés par l'organisation]<br>B. Prendre les mesures suivantes lorsque des changements non autorisés sont détectés dans les logiciels, les micrologiciels et l'information : [Affectation : actions définies par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 07(01) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Contrôles d'intégrité<br>Effectuer un contrôle de l'intégrité de [Affectation : logiciels, micrologiciels et information définis par l'organisation] [Sélection (un choix ou plus) : au démarrage; à [Affectation : états transitionnels ou événements touchant la sécurité définis par l'organisation]; [Affectation : fréquence définie par l'organisation]]. | Contrôle | Sélectionné | [4] [fréquence au moins tous les 30 jours] | s.o. |
| SI | 07(02) | Intégrité des logiciels, des | Intégrité des logiciels, des micrologiciels et de l'information : Automatisation des avis d'atteinte à l'intégrité<br>Utiliser des outils automatisés qui notifient [Affectation : personnel ou rôles définis par l'organisation] lors de la découverte d'écarts durant la vérification de l'intégrité. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | micrologiciels et de l'information | | | | | |
| SI | 07(03) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Outils de vérification de l'intégrité gérés centralement<br>Utiliser des outils de vérification de l'intégrité gérés centralement. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 07(04) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Emballage avec sceau d'inviolabilité<br>Annulé : Intégré au contrôle SA-12. | s.o. | s.o. | s.o. | s.o. |
| SI | 07(05) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Automatisation des interventions en cas d'atteinte à l'intégrité<br>[Sélection (un choix ou plus) : Arrêter le système; Redémarrer le système; Mettre en œuvre [Affectation : contrôles définis par l'organisation]] automatiquement lorsque des atteintes à l'intégrité sont relevées. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(06) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Protection cryptographique<br>Mettre en œuvre des mécanismes de chiffrement pour détecter les modifications non autorisées apportées aux logiciels, aux micrologiciels et à l'information. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(07) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Intégration de la détection et de l'intervention<br>Intégrer la détection des changements non autorisés apportés à la capacité d'intervention en cas d'incident de l'organisation : [Affectation : changements de sécurité apportés au système définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 07(08) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Vérification des capacités en cas d'événements importants<br>Après avoir détecté une possible atteinte à l'intégrité, fournir les capacités nécessaires pour vérifier l'événement et mettre en œuvre les mesures suivantes : [Sélection (un choix ou plus) : générer un enregistrement de vérification; alerter les utilisatrices et utilisateurs actuels; alerter [Affectation : personnel ou rôles définis par l'organisation]; [Affectation : autres mesures définies par l'organisation]]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(09) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Vérification du processus de démarrage<br>Vérifier l'intégrité du processus de démarrage des composants de systèmes suivants : [Affectation : composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(10) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Protection des micrologiciels de démarrage<br>Mettre en œuvre les mécanismes suivants pour protéger l'intégrité du micrologiciel de démarrage dans [Affectation : composants de systèmes désignés par l'organisation] : [Affectation : mécanismes définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(11) | Intégrité des logiciels, des | Intégrité des logiciels, des micrologiciels et de l'information : Environnements clos aux privilèges restreints<br>Annulé : Transféré sous le contrôle CM-07(06). | s.o. | s.o. | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | micrologiciels et de l'information | | | | | |
| SI | 07(12) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Vérification de l'intégrité<br>Exiger que l'intégrité des logiciels suivants soit vérifiée avant exécution : [Affectation : logiciels désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(13) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Exécution de code dans des environnements protégés<br>Annulé : Transféré sous le contrôle CM-07(07). | s.o. | s.o. | s.o. | s.o. |
| SI | 07(14) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Code binaire ou exécutable sur machine<br>Annulé : Transféré sous le contrôle CM-07(08). | s.o. | s.o. | s.o. | s.o. |
| SI | 07(15) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Authentification du code<br>Mettre en œuvre des mécanismes cryptographiques pour authentifier les composants logiciels ou micrologiciels suivants avant leur installation : [Affectation : composants logiciels ou micrologiciels désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(16) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Limite temporelle sur l'exécution des processus sans supervision<br>Faire en sorte que les processus ne puissent pas s'exécuter sans supervision pour plus de [Affectation : période définie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 07(17) | Intégrité des logiciels, des micrologiciels et de l'information | Intégrité des logiciels, des micrologiciels et de l'information : Autoprotection des applications d'exécution<br>Mettre en œuvre [Affectation : contrôles définis par l'organisation] pour assurer l'autoprotection des applications d'exécution. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 08 | Protection contre les pourriels | A. Utiliser des mécanismes de protection contre les pourriels aux points d'entrée et de sortie du système pour détecter les messages non sollicités et intervenir, le cas échéant<br>B. Mettre à jour les mécanismes de protection contre les pourriels dès la diffusion de nouvelles versions, conformément à la stratégie et aux procédures de gestion des configurations de l'organisation | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 08(01) | Protection contre les pourriels | Protection contre les pourriels : Gestion centrale<br>Annulé : Intégré au contrôle PL-09. | s.o. | s.o. | s.o. | s.o. |
| SI | 08(02) | Protection contre les pourriels | Protection contre les pourriels : Mises à jour automatiques<br>Mettre à jour automatiquement les mécanismes de protection contre les pourriels [Affectation : fréquence définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 08(03) | Protection contre les pourriels | Protection contre les pourriels : Capacité de perfectionnement continu<br>Mettre en œuvre des mécanismes de protection contre les pourriels avec une capacité d'apprentissage pour reconnaître le trafic de communications légitime plus efficacement. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 09 | Restrictions relatives à la saisie d'information | Annulé : Intégré aux contrôles AC-02, AC-03, AC-05 et AC-06. | s.o. | s.o. | s.o. | s.o. |
| SI | 10 | Validation de la saisie d'information | Vérifier la validité des saisies d'information suivantes : [Affectation : saisies d'information dans le système définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 10(01) | Validation de la saisie d'information | Validation de la saisie d'information : Fonction de correction manuelle<br>a. Fournir une fonction de correction manuelle pour la validation de la saisie de l'information suivante : [Affectation : saisies définies par l'organisation dans le contrôle de base (SI-10)]<br>b. Restreindre l'utilisation de la fonction de correction manuelle à [Affectation : personnes autorisées désignées par l'organisation]<br>c. Vérifier l'utilisation de la fonction de correction manuelle | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 10(02) | Validation de la saisie d'information | Validation de la saisie d'information : Examen et résolution des erreurs<br>Examiner et résoudre les erreurs de validation en entrée dans les [Affectation : délais définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 10(03) | Validation de la saisie d'information | Validation de la saisie d'information : Comportements prévisibles<br>Vérifier que le système se comporte d'une manière prévisible et informée lorsque des saisies non valides sont reçues. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 10(04) | Validation de la saisie d'information | Validation de la saisie d'information : Chronométrage des interactions<br>Tenir compte du chronométrage des interactions entre les composants de systèmes lorsque vient le temps de déterminer les interventions appropriées à mettre en œuvre advenant des saisies non valides. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 10(05) | Validation de la saisie d'information | Validation de la saisie d'information : Restriction des saisies provenant de sources de confiance et de formats approuvés<br>Restreindre l'utilisation des saisies d'information à [Affectation : sources de confiance définies par l'organisation] et à [Affectation : formats définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 10(06) | Validation de la saisie d'information | Validation de la saisie d'information : Prévention de l'injection<br>Prévenir les injections de données non fiables. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 11 | Traitement des erreurs | A. Générer des messages d'erreur qui fournissent l'information nécessaire à l'application de mesures correctives sans toutefois révéler des données qui pourraient être exploitées<br>B. Révéler les messages d'erreur seulement à [Affectation : personnel ou rôles définis par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 12 | Gestion et conservation de l'information | Gérer et conserver l'information au sein du système et les sorties d'information du système conformément aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes, aux lignes directrices et aux exigences opérationnelles applicables. | Contrôle | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 12(01) | Gestion et conservation de l'information | Gestion et conservation de l'information : Limitation des éléments liés aux renseignements personnels<br>Limiter le traitement des renseignements personnels dans le cycle de vie de l'information aux éléments de renseignements personnels suivants : [Affectation : éléments des renseignements personnels définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 12(02) | Gestion et conservation de l'information | Gestion et conservation de l'information : Réduction des renseignements personnels utilisés aux fins de tests, de formation et de recherche<br>Utiliser les techniques suivantes pour limiter l'utilisation de renseignements personnels aux fins de recherche, de test ou de formation : [Affectation : techniques définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 12(03) | Gestion et conservation de l'information | Gestion et conservation de l'information : Élimination de l'information<br>Utiliser les techniques suivantes pour éliminer, détruire ou supprimer l'information à la fin de la période de conservation : [Affectation : techniques définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 13 | Prévention des pannes prévisibles | A. Déterminer la durée moyenne de fonctionnement avant défaillance (MTTF pour *Mean Time to Failure*) des composants de systèmes suivants dans des environnements d'exploitation donnés : [Affectation : composants de systèmes désignés par l'organisation]<br>B. Fournir des composants de système de remplacement et un mécanisme d'échange des rôles actifs et passifs des composants conformément aux critères suivants : [Affectation : critères de remplacement de la MTTF définis par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 13(01) | Prévention des pannes prévisibles | Prévention des pannes prévisibles : Transfert des responsabilités d'un composant<br>Mettre les composants de systèmes hors service en transférant ses responsabilités à un composant de remplacement à l'intérieur de [Affectation : fraction ou pourcentage définis par l'organisation] de la durée moyenne de fonctionnement avant défaillance. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 13(02) | Prévention des pannes prévisibles | Prévention des pannes prévisibles : Limite temporelle sur l'exécution des processus sans supervision<br>Annulé : Intégré au contrôle SI-07(16). | s.o. | s.o. | s.o. | s.o. |
| SI | 13(03) | Prévention des pannes prévisibles | Prévention des pannes prévisibles : Transfert manuel entre les composants<br>Procéder manuellement aux transferts entre les composants de systèmes actifs et passifs lorsque l'utilisation d'un composant actif atteint [Affectation : pourcentage défini par l'organisation] de la MTTF. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 13(04) | Prévention des pannes prévisibles | Prévention des pannes prévisibles : Installation des composants passifs et notification<br>Lors de la détection d'une défaillance d'un composant de système :<br>a. s'assurer que les composants passifs sont bien installés de manière transparente dans les [Affectation : délais définis par l'organisation]<br>b. [Sélection (un choix ou plus) : activer [Affectation : alarme définie par l'organisation]; mettre automatiquement le système hors tension; [Affectation : action définie par l'organisation]] | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 13(05) | Prévention des pannes prévisibles | Prévention des pannes prévisibles : Capacité de basculement<br>Fournir [Affectation : capacité de basculement définie par l'organisation] en [Sélection (un choix) : temps réel; temps quasi réel]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 14 | Non-persistance | Mettre en œuvre des [Affectation : composants du système et services désignés par l'organisation] non persistants initialisés dans un état connu et interrompus [Sélection (un choix ou plus) : à la fin de la période d'utilisation; périodiquement [Affectation : fréquence déterminée par l'organisation]]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 14(01) | Non-persistance | Non-persistance : Restauration à partir de sources de confiance<br>Obtenir les données et les logiciels utilisés au cours de la restauration des composants de systèmes et des services à partir des sources de confiance suivantes : [Affectation : sources de confiance définies par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 14(02) | Non-persistance | Non-persistance : Information non persistante<br>a. [Sélection (un choix) : Restaurer [Affectation : information définie par l'organisation] [Affectation : fréquence définie par l'organisation]; Générer [Affectation : information définie par l'organisation] sur demande]<br>b. Supprimer l'information qui n'est plus nécessaire | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 14(03) | Non-persistance | Non-persistance : Connectivité non persistante<br>Établir des connexions au système sur demande et mettre fin aux connexions [Sélection (un choix) : une fois la demande terminée; après une période de non-utilisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 15 | Filtrage des sorties d'information | Valider les sorties d'information des applications et/ou des programmes informatiques suivants pour s'assurer que l'information est conforme au contenu auquel l'on s'attend : [Affectation : applications et/ou programmes informatiques désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 16 | Protection de la mémoire | Mettre en place les contrôles suivants pour protéger la mémoire du système contre l'exécution de code non autorisé : [Affectation : contrôles définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 17 | Procédures de sécurité intégrée | Mettre en place les procédures de sécurité intégrée indiquées lorsque les défaillances suivantes se produisent : [Affectation : liste des conditions de défaillance et des procédures de sécurité intégrée connexes établie par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 18 | Opérations liées à la qualité des renseignements personnels | A. Assurer l'exactitude, la pertinence, la rapidité et l'exhaustivité des renseignements personnels utilisés à des fins administratives tout au long du cycle de vie de l'information [Affectation : fréquence définie par l'organisation]<br>B. Corriger ou supprimer les renseignements personnels inexacts ou obsolètes | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 18(01) | Opérations liées à la qualité des renseignements personnels | Opérations liées à la qualité des renseignements personnels : Soutien à l'automatisation<br>Corriger ou supprimer les renseignements personnels inexacts ou obsolètes, ceux dont l'incidence a été mal déterminée ou ceux qui ont été mal dépersonnalisés au moyen de [Affectation : mécanismes automatisés définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 18(02) | Opérations liées à la qualité des renseignements personnels | Opérations liées à la qualité des renseignements personnels : Étiquetage des données<br>Employer les étiquettes de données pour automatiser la correction ou la suppression des renseignements personnels tout au long du cycle de vie de l'information dans les systèmes organisationnels. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 18(03) | Opérations liées à la qualité des | Opérations liées à la qualité des renseignements personnels : Collecte<br>Collecter les renseignements personnels directement des individus. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | renseignements personnels | | | | | |
| SI | 18(04) | Opérations liées à la qualité des renseignements personnels | Opérations liées à la qualité des renseignements personnels : Demandes individuelles<br>Corriger ou supprimer les renseignements personnels lorsque des individus ou leurs représentantes ou représentants en font la demande. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 18(05) | Opérations liées à la qualité des renseignements personnels | Opérations liées à la qualité des renseignements personnels : Avis de correction ou de suppression<br>Notifier [Affectation : destinataires des renseignements personnels désignés par l'organisation] et les individus que les renseignements personnels ont été corrigés ou supprimés. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19 | Dépersonnalisation | A. Supprimer les éléments de renseignements personnels suivants des jeux de données : [Affectation : éléments des renseignements personnels définis par l'organisation]<br>B. Évaluer l'efficacité de la dépersonnalisation [Affectation : fréquence définie par l'organisation]<br>AA. Tenir compte des préjudices découlant de l'atteinte à la vie privée si les renseignements pouvant être accessibles au public permettent de réidentifier les individus | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(01) | Dépersonnalisation | Dépersonnalisation : Collecte<br>Dépersonnaliser les jeux de données au moment de la collecte en ne collectant pas les renseignements personnels. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(02) | Dépersonnalisation | Dépersonnalisation : Archivage<br>Interdire l'archivage des éléments de renseignements personnels si ces éléments dans le jeu de données ne sont pas nécessaires une fois le jeu de données archivé. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(03) | Dépersonnalisation | Dépersonnalisation : Diffusion<br>Supprimer les éléments de renseignements personnels d'un jeu de données avant sa diffusion si ces éléments n'ont pas à faire partie de la diffusion des données. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(04) | Dépersonnalisation | Dépersonnalisation : Suppression, masquage, chiffrement, hachage ou remplacement des identificateurs directs<br>Supprimer, masquer, chiffrer, hacher ou remplacer les identificateurs directs dans un jeu de données. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(05) | Dépersonnalisation | Dépersonnalisation : Contrôle de la divulgation de statistiques<br>Manipuler les données numériques, les tableaux croisés et les résultats statistiques de manière à ce qu'on ne puisse pas identifier un individu ou une organisation dans les résultats de l'analyse. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(06) | Dépersonnalisation | Dépersonnalisation : Confidentialité différentielle<br>Prévenir la divulgation de renseignements personnels en ajoutant du bruit non déterministe aux résultats des opérations mathématiques avant de faire rapport des résultats. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 19(07) | Dépersonnalisation | Dépersonnalisation : Algorithmes et logiciels validés<br>Procéder à la dépersonnalisation au moyen d'algorithmes validés et de logiciels homologués pour assurer la mise en œuvre des algorithmes. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SI | 19(08) | Dépersonnalisation | Dépersonnalisation : Intrus motivé<br>Effectuer un test d'intrus motivé dans le jeu de données dépersonnalisé pour déterminer si ce dernier contient toujours des données identifiables ou si les données dépersonnalisées peuvent être réidentifiées. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 20 | Contamination | Intégrer les données ou les capacités dans les systèmes ou les composants de systèmes suivants pour déterminer si les données organisationnelles ont été exfiltrées ou ont été supprimées de façon inappropriée de : [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 21 | Actualisation de l'information | Actualiser [Affectation : information définie par l'organisation] [Affectation : fréquences définies par l'organisation] ou générer l'information sur demande et la supprimer lorsqu'elle n'est plus nécessaire. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 22 | Diversité de l'information | A. Relever les autres sources d'information pour [Affectation : fonctions et services essentiels définis par l'organisation] : [Affectation : autres sources d'information définies par l'organisation]<br>B. Utiliser une autre source d'information pour l'exécution des fonctions et des services essentiels sur [Affectation : systèmes ou composants de systèmes désignés par l'organisation] lorsque la source principale d'information est corrompue ou non disponible | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 23 | Fragmentation de l'information | Selon [Affectation : circonstances définies par l'organisation]<br>A. fragmenter l'information suivante : [Affectation : information définie par l'organisation]<br>B. distribuer l'information fragmentée dans l'ensemble des systèmes ou des composants de systèmes suivants : [Affectation : systèmes ou composants de systèmes désignés par l'organisation] | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 400 | Station de travail administrative dédiée | Exiger que les opérations administratives ou de superutilisatrices ou superutilisateurs soient réalisées à partir d'une station de travail physique dédiée à ces tâches précises et isolée des autres fonctions et réseaux. La station ne devrait pas, entre autres, avoir accès à Internet. | Contrôle | Sélectionné | s.o. | s.o. |
| SI | 400(01) | Station de travail administrative dédiée | Station de travail administrative dédiée : Station de travail administrative dédiée avec client léger<br>Mettre en œuvre une STAD virtualisée à l'intérieur d'une STAD client léger physique isolée du réseau. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 400(02) | Station de travail administrative dédiée | Station de travail administrative dédiée : RPV sur réseau privé d'opérateur<br>Connecter une STAD à un réseau cible au moyen d'un réseau privé d'opérateur (par exemple, un service LAN privé virtuel [VPLS pour *Virtual Private LAN*] ou une commutation multiprotocole par étiquette [MPLS pour *Multiprotocol Label Switching*]) avec chiffrement de RPV. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 400(03) | Station de travail administrative dédiée | Station de travail administrative dédiée : Réseau local<br>Connecter une STAD à un réseau cible au moyen d'un réseau local seulement. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 400(04) | Station de travail | Station de travail administrative dédiée : Accès par console seulement<br>Connecter une STAD au système cible par l'intermédiaire des ports de la console seulement. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | administrative dédiée | | | | | |
| SI | 400(05) | Station de travail administrative dédiée | Station de travail administrative dédiée : Station de travail physique dédiée<br>Utiliser une station de travail physique unique comme STAD. | Contrôle | Non sélectionné | s.o. | s.o. |
| SI | 400(06) | Station de travail administrative dédiée | Station de travail administrative dédiée : Accès administratif hétérogène<br>Utiliser un système d'exploitation différent pour la STAD et le système cible. | Contrôle | Non sélectionné | s.o. | s.o. |

| Famille | ID | Nom | Description | Contrôle/ Activité | Suggéré pour ce profil | Valeurs suggérées de paramètres substituables | Remarques concernant le profil |
|---|---|---|---|---|---|---|---|
| SR | 01 | Politique et procédures de gestion des risques liés à la chaîne d'approvisionnement | A. Développer, documenter et diffuser à [Affectation : personnel ou rôles définis par l'organisation]<br>1. une politique de gestion des risques liés à la chaîne d'approvisionnement (GRCA) [Sélection (un choix ou plus) : au niveau organisationnel; au niveau du processus lié à une mission ou à une activité; au niveau du système] qui<br>a. définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité<br>b. est conforme aux lois, aux décrets, aux directives, à la réglementation, aux politiques, aux normes et aux lignes directrices applicables<br>2. des procédures pour faciliter la mise en œuvre de la politique de GRCA et des contrôles connexes<br>B. Désigner une ou un [Affectation : responsable désigné par l'organisation] pour gérer l'élaboration, la documentation et la diffusion de la politique et des procédures liées à la GRCA<br>C. Passer en revue et mettre à jour, par rapport à la GRCA,<br>1. la politique actuelle [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation]<br>2. les procédures [Affectation : fréquence définie par l'organisation] ou à la suite de [Affectation : événements définis par l'organisation] | Activité | Sélectionné | s.o. | s.o. |
| SR | 02 | Plan de gestion des risques liés à la chaîne d'approvisionnement | A. Élaborer un plan pour gérer les risques liés à la chaîne d'approvisionnement associés à la recherche, au développement, à la conception, à la fabrication, à l'acquisition, à la livraison, à l'intégration, à l'exploitation, à la maintenance et à l'élimination des systèmes, des composants de systèmes ou des services qui s'y rapportent : [Affectation : systèmes, composants de systèmes ou services désignés par l'organisation]<br>B. Passer en revue et mettre à jour le plan de GRCA [Affectation : fréquence définie par l'organisation] ou au besoin pour tenir compte des changements organisationnels, environnementaux ou en matière de menaces<br>C. Protéger le plan de GRCA contre les divulgations ou les modifications non autorisées | Activité | Sélectionné | s.o. | s.o. |
| SR | 02(01) | Plan de gestion des risques liés | Plan de gestion des risques liés à la chaîne d'approvisionnement : Établissement d'une équipe de GRCA<br>Mettre en place une équipe de GRCA composée de [Affectation : personnel, rôles et responsabilités définis par | Activité | Sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | à la chaîne d'approvisionnement | l'organisation] pour diriger et soutenir les activités de GRCA suivantes : [Affectation : Activités de gestion des risques liés à la chaîne d'approvisionnement définies par l'organisation]. | | | | |
| SR | 03 | Contrôles et processus de la chaîne d'approvisionnement | A. Mettre en place un ou plusieurs processus pour relever et corriger les faiblesses ou les lacunes dans les éléments et les processus de la chaîne d'approvisionnement de [Affectation : systèmes ou composants de systèmes désignés par l'organisation] en coordination avec [Affectation : personnel de la chaîne d'approvisionnement désigné par l'organisation]<br>B. Utiliser les contrôles suivants pour offrir une protection contre les risques liés à la chaîne d'approvisionnement pour les systèmes, les composants de systèmes ou les services qui s'y rapportent ainsi que pour limiter les conséquences ou les dommages potentiels associés aux événements de la chaîne d'approvisionnement : [Affectation : contrôles de la chaîne d'approvisionnement définis par l'organisation]<br>C. Documenter les processus et les contrôles liés à la chaîne d'approvisionnement qui ont été sélectionnés et mis en œuvre dans [Sélection (un choix) : plans de sécurité et de confidentialité; plan de GRCA; [Affectation : document défini par l'organisation]] | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 03(01) | Contrôles et processus de la chaîne d'approvisionnement | Contrôles et processus de la chaîne d'approvisionnement : Base d'approvisionnement diversifiée<br>Employer un ensemble diversifié de sources pour les composants de systèmes et les services suivants : [Affectation : composants de systèmes et services désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 03(02) | Contrôles et processus de la chaîne d'approvisionnement | Contrôles et processus de la chaîne d'approvisionnement : Limitation des dommages<br>Employer les contrôles suivants pour limiter les dommages pouvant être causés par d'éventuels adversaires qui pourraient identifier et cibler la chaîne d'approvisionnement organisationnelle : [Affectation : contrôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 03(03) | Contrôles et processus de la chaîne d'approvisionnement | Contrôles et processus de la chaîne d'approvisionnement : Transfert d'exigences à des sous-traitants<br>S'assurer que les contrôles compris dans les contrats conclus avec les entrepreneurs principaux sont également inclus dans les contrats des sous-traitants. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 04 | Provenance | Documenter, surveiller et maintenir une provenance valide des systèmes et des composants de systèmes suivants, ainsi que de leurs données connexes : [Affectation : systèmes et composants de systèmes désignés par l'organisation et données connexes]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 04(01) | Provenance | Provenance : Identité<br>Établir et maintenir une identification unique des éléments de la chaîne d'approvisionnement, des processus et du personnel associé au système désigné et aux composants de systèmes essentiels : [Affectation : éléments de la chaîne d'approvisionnement, processus et personnel associé aux systèmes et aux composants de systèmes essentiels désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SR | 04(02) | Provenance | Provenance : Suivi et localisation<br>Établir et maintenir une identification unique des systèmes et des composants de systèmes essentiels suivants aux fins de suivi tout au long de la chaîne d'approvisionnement : [Affectation : systèmes et composants de systèmes essentiels désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 04(03) | Provenance | Provenance : Attestation de l'authenticité et de la non-altérité<br>Employer les contrôles suivants pour attester que le système ou le composant de système qui a été livré n'a pas été altéré : [Affectation : contrôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 04(04) | Provenance | Provenance : Intégrité de la chaîne d'approvisionnement – Pedigree<br>Employer [Affectation : contrôles définis par l'organisation] et procéder à [Affectation : analyse définie par l'organisation] pour assurer l'intégrité du système ou des composants de systèmes en validant la composition interne et la provenance des technologies, des produits et des services critiques ou essentiels à la mission. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 05 | Stratégies, outils et méthodes d'acquisition | Utiliser les stratégies d'acquisition, les méthodes d'approvisionnement et les outils de passation de marchés suivants afin de déterminer, de contrer et d'atténuer les risques associés à la chaîne d'approvisionnement : [Affectation : stratégies d'acquisition, outils de passation de marchés et méthodes d'approvisionnement définis par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 05(01) | Stratégies, outils et méthodes d'acquisition | Stratégies, outils et méthodes d'acquisition : Approvisionnement adéquat<br>Employer les contrôles suivants pour assurer un approvisionnement adéquat de [Affectation : composants de systèmes essentiels désignés par l'organisation] : [Affectation : contrôles définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 05(02) | Stratégies, outils et méthodes d'acquisition | Stratégies, outils et méthodes d'acquisition : Évaluation préalable à la sélection, à l'acceptation, à la modification ou à la mise à jour<br>Procéder à l'évaluation d'un système, d'un composant du système ou d'un service qui s'y rapporte préalablement à la sélection, à l'acceptation, à la modification ou à la mise à jour. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 06 | Évaluations et examens des fournisseurs | Évaluer et examiner les risques liés à la chaîne d'approvisionnement associés aux fournisseurs, aux entrepreneures ou aux entrepreneurs ainsi que le système, le composant de système ou le service fourni par ces derniers [Affectation : fréquence définie par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 06(01) | Évaluations et examens des fournisseurs | Évaluations et examens des fournisseurs : Tests et analyse<br>Employer [Sélection (un choix ou plus) : analyse organisationnelle; analyse d'une tierce partie indépendante; tests par l'organisation; tests par une tierce partie indépendante] des éléments de la chaîne d'approvisionnement, des parties prenantes et des processus suivants relativement au système, au composant de système ou au service qui s'y rapporte : [Affectation : éléments de la chaîne d'approvisionnement, processus, intervenantes et intervenants désignés par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SR | 07 | Sécurité opérationnelle de la chaîne d'approvisionnement | Employer les contrôles de sécurité opérationnelle (OPSEC pour *Operational Security*) pour protéger l'information relative à la chaîne d'approvisionnement pour le système, le composant de système ou le service qui s'y rapporte : [Affectation : contrôles d'OPSEC définis par l'organisation]. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 08 | Ententes de notification | Mettre en place des ententes et des procédures avec les entités qui prennent part à la chaîne d'approvisionnement du système, du composant de système ou du service qui s'y rapporte pour [Sélection (un choix ou plus) : la notification des compromissions touchant la chaîne d'approvisionnement; les résultats des évaluations ou des vérifications; [Affectation : information définie par l'organisation]]. | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 09 | Résistance au trafiquage et détection | Mettre en œuvre un programme de protection contre le trafiquage pour le système, le composant de système ou le service qui s'y rapporte. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 09(01) | Résistance au trafiquage et détection | Résistance au trafiquage et détection : Phases multiples du cycle de développement de systèmes<br>Avoir recours à des technologies, des outils et des techniques de protection contre le trafiquage tout au long du cycle de développement de systèmes. | Contrôle | Non sélectionné | s.o. | s.o. |
| SR | 10 | Inspection des systèmes ou des composants | Inspecter les systèmes ou les composants de systèmes suivants [Sélection (un choix ou plus) : de façon aléatoire; tous les [Affectation : fréquence définie par l'organisation], lorsque [Affectation : indications concernant le besoin de mener une inspection définies par l'organisation]] pour détecter le trafiquage : [Affectation : systèmes ou composants de systèmes désignés par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 11 | Authenticité des composants | A. Développer et mettre en œuvre une stratégie et des procédures qui visent à combattre la contrefaçon et qui prévoient la mise en place de mesures visant à détecter et à prévenir l'entrée de dispositifs contrefaits dans les systèmes<br>B. Signaler les composants de systèmes qui ont été contrefaits à [Sélection (un choix ou plus) : source de composant contrefait; [Affectation : organisations externes responsables du signalement désignées par l'organisation]; [Affectation : personnel ou rôles définis par l'organisation]] | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 11(01) | Authenticité des composants | Authenticité des composants : Formation anticontrefaçon<br>Former [Affectation : personnel ou rôles définis par l'organisation] dans le domaine de la détection des composants contrefaits de systèmes (y compris les composants matériels, logiciels et microgiciels). | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 11(02) | Authenticité des composants | Authenticité des composants : Contrôle des configurations pour l'entretien et la réparation des composants<br>Maintenir le contrôle des configurations pour les composants de systèmes suivants appelés à subir un entretien ou une réparation, ainsi que des composants réparés ou entretenus qui sont appelés à retourner à leur lieu de service : [Affectation : composants de systèmes désignés par l'organisation] | Contrôle | Sélectionné | s.o. | s.o. |
| SR | 11(03) | Authenticité des composants | Authenticité des composants : Analyse anticontrefaçon<br>Analyser les composants de systèmes [Affectation : fréquence définie par l'organisation] pour détecter la contrefaçon. | Contrôle | Non sélectionné | s.o. | s.o. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| SR | 12 | Mise hors service des composants | Éliminer [Affectation : données, documents, outils ou composants de systèmes désignés par l'organisation] au moyen des techniques et des méthodes suivantes : [Affectation : techniques et méthodes définies par l'organisation]. | Contrôle | Sélectionné | s.o. | s.o. |