Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI : Nº 3, Gestion et contrôle des privilèges d'administrateur

Série gestionnaires

ITSM.10.094

Canada

Avant-propos

La présente est un document NON CLASSIFIÉ qui fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans Les 10 mesures de sécurité des technologies de l'information visant à protéger les réseaux Internet et l'information (ITSM.10.089) [1][1].

Date d'entrée en vigueur

Le présent document entre en vigueur le 19 juillet 2022.

Historique des révisions

Révision	Modifications	Date
1	Première version.	19 juillet 2022

[1] Les numéros entre les crochets renvoient à des éléments de référence figurant à la section Contenu complémentaire du présent document.

Vue d'ensemble

Parmi les 10 mesures de sécurité des TI recommandées par le CST, une consiste à mettre en vigueur la gestion des privilèges d'administrateur. Le présent document aborde certaines des actions que votre organisation peut effectuer pour gérer et contrôler les privilèges d'administrateur. Les conseils formulés dans la présente sont fondés sur les contrôles de sécurité mentionnés dans le document intitulé La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) [2].

Le présent document fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.089 [1]. La mise en œuvre de l'ensemble des 10 mesures de sécurité recommandées peut rendre votre organisation moins vulnérable aux cybermenaces. Vous devriez toutefois passer en revue les activités que vous menez en matière de cybersécurité afin de déterminer si d'autres actions sont nécessaires. Pour de plus amples renseignements sur la mise en œuvre des 10 mesures de sécurité des TI, communiquez par téléphone ou par courriel avec le :

Centre d'appel du Centre canadien pour la cybersécurité

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

D97-4/10-094-2022F-PDF
978-0-660-43807-8

Table des matières

1 Introduction 6

1.1 Les 10 mesures de sécurité des TI 6

1.2 Processus de gestion des risques liés à la sécurité des TI 7

2 Vulnérabilités et menaces 10

3 Authentification et autorisation (IA-2, AC-6) 13

3.1 Mettre en place l'authentification multifacteur 14

3.2 Appliquer le principe du droit d'accès minimal 14

4 Gestion des comptes d'administrateur (AC-2, AC-17(100), SC-3) 16

4.1 Séparer les fonctions et les stations de travail administratives 16

4.2 Mettre en place l'intégrité par deux personnes (TPI) et la double autorisation des comptes administrateur 17

4.3 Journaliser et surveiller les comptes privilégiés 18

4.4 Supprimer les comptes et retirer les accès privilégiés 18

5 Résumé 20

5.1 Coordonnées 21

6 Contenu complémentaire 22

6.1 Liste d'abréviations, d'acronymes et de sigles 22

6.2 Glossaire 22

6.3 Références 24

Liste des figures

Figure 1 : Les 10 mesures de sécurité des TI - Nº 3, Mettre en vigueur la gestion des privilèges d'administrateur 7

Figure 2 : Classes et familles de contrôles de sécurité décrites dans l'ITSG-33 8

Liste des tableaux

Tableau 1 : Exemples des méthodes d'attaque utilisées 10

Tableau 2 : Contrôles de sécurité techniques de l'ITSG-33 : AC-2, A-6 et AC-17(100) 25

Tableau 3 : Contrôles de sécurité techniques de l'ITSG-33 : IA-2 29

Tableau 4 : Contrôles de sécurité techniques de l'ITSG-33 : SC-3 32

Liste des annexes

Annexe A : Catalogue des contrôles de sécurité tiré de l'ITSG-33 25

A.1 Contrôles de sécurité techniques : Contrôle d'accès 25

A.2 Contrôles de sécurité techniques : Identification et authentification 29

A.3 Contrôles de sécurité techniques : Protection des systèmes et des communications 32

1 Introduction

Le présent document donne des conseils sur la gestion des privilèges d'administrateur. La gestion et le contrôle des privilèges d'administrateur permettent de réduire le degré d'exposition de votre organisation aux cybermenaces susceptibles de compromettre vos réseaux, vos systèmes et vos biens de TI. La présente est fondée sur les conseils et les contrôles de sécurité formulés respectivement dans l'ITSM.10.089 [1] et l'annexe 3A de l'ITSG-33 [2].

Les conseils énoncés dans le présent document ne sauraient être exhaustifs ou complets. On y décrit seulement certains des contrôles de sécurité qu'il est possible de mettre en œuvre pour protéger l'information de votre organisation. Prière de consulter le document *Contrôles de cybersécurité de base pour les petites et moyennes organisations* [3] pour obtenir plus d'information sur les contrôles de sécurité qu'il est possible de mettre en œuvre pour protéger votre organisation à un niveau général et minimum.

Avant de mettre en œuvre une mesure de sécurité, vous devriez procéder à l'évaluation des risques afin d'identifier les exigences de votre organisation en matière de sécurité. Une fois que vous avez bien compris votre profil de risque, vous pouvez adapter ce conseil selon les besoins de votre organisation. Vous devriez prendre les mesures nécessaires pour identifier et déterminer les contrôles dont votre organisation a besoin pour protéger ses biens. Mettre en œuvre des contrôles superflus peut donner lieu à des inefficacités et entraîner des dépenses inutiles. Après avoir identifié les contrôles qui répondent le mieux aux besoins de votre organisation, vous devriez les adapter de manière à ce qu'ils conviennent à l'environnement et aux exigences propres à votre organisation.

1.1 Les 10 mesures de sécurité des TI

Les 10 mesures de sécurité des TI recommandées par le CST qui sont mentionnées à la figure 1 ci-dessous sont fondées sur une analyse des tendances inhérentes aux cybermenaces et la répercussion de telles menaces sur les réseaux connectés à Internet. La mise en œuvre de toutes les mesures permettra de corriger la plupart des vulnérabilités liées à la sécurité des TI qui pèsent sur votre organisation. Cela dit, votre organisation est unique. Pour satisfaire vos besoins en matière de sécurité, vous devez examiner les activités actuellement menées par votre organisation sur le plan de la sécurité et de la gestion des risques.

Figure 1 : Les 10 mesures de sécurité des TI - Nº 3, Mettre en vigueur la gestion des privilèges d'administrateur

1.2 Processus de gestion des risques liés à la sécurité des TI

Les 10 mesures de sécurité des TI du CST découlent des contrôles de sécurité mentionnés à l'annexe 3A de l'ITSG-33 [2].

L'ITSG-33 [2] décrit les rôles, les responsabilités et les activités qui permettent à une organisation de gérer les risques relevant de la sécurité des TI, et comprend un catalogue de contrôles de sécurité (c.-à-d., un ensemble standardisé d'exigences de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des biens de TI). Ces contrôles de sécurité sont regroupés en trois classes, puis subdivisés en plusieurs familles (ou regroupements) de contrôles de sécurité connexes :

- **Contrôles de sécurité techniques :** Contrôles de sécurité qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité que l'on retrouve dans les composants matériels, logiciels et micrologiciels;
- **Contrôles de sécurité opérationnels :** Contrôles de sécurité de système d'information qui sont mis en œuvre et exécutés principalement par des personnes et qui s'appuient normalement sur des technologies comme les logiciels de soutien;
- **Contrôles de sécurité de gestion :** Contrôles de sécurité qui portent principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.

Tel qu'il est illustré à la figure 2, le présent document comprend certaines actions qui appartiennent aux familles de contrôles Identification et authentification (IA), Contrôle de l'accès (AC) et Protection des systèmes et des communications (SC). Le présent document décrit les zones suivantes :

- **AC-2 Gestion de compte**;
- **AC-6 Droit d'accès minimal**;
- **AC-17 Accès à distance**;
- **IA-2 Identification et authentification (utilisateurs organisationnels)**;
- **SC-3 Isolation de la fonction de sécurité**.

De plus amples renseignements sur les contrôles AC-2, AC-6, AC-17, IA-2 et SC-3 sont fournis à l'annexe A du présent document.

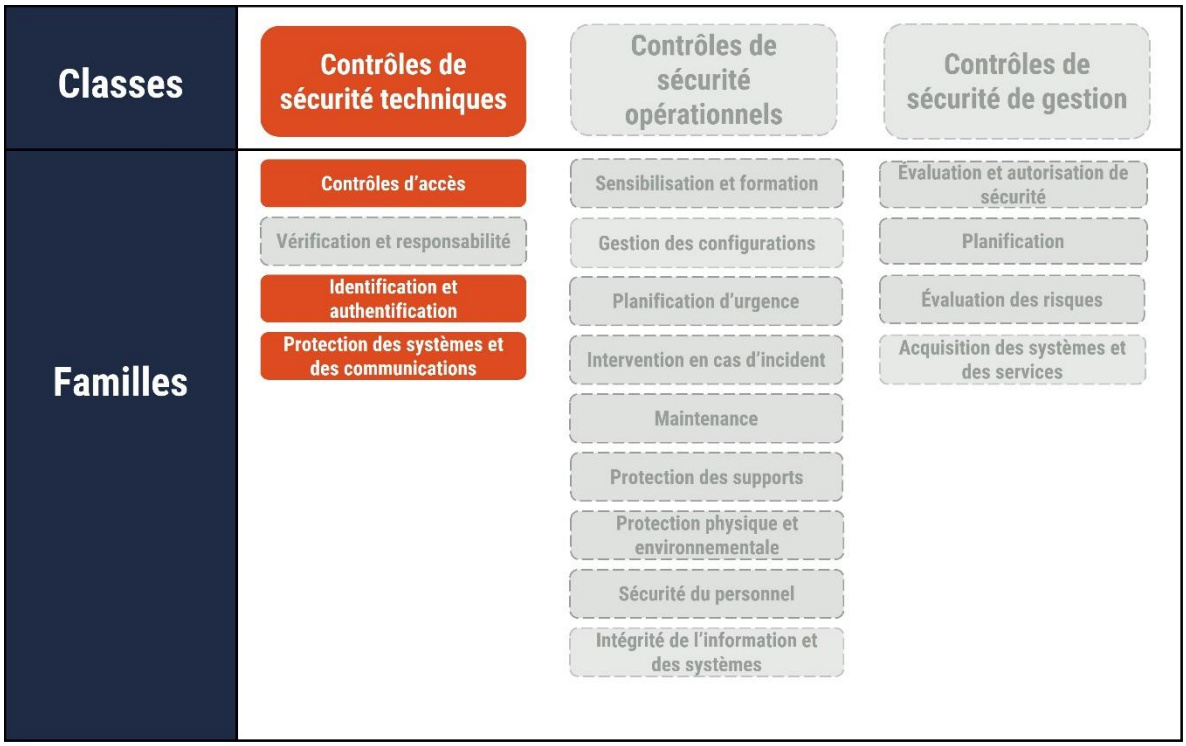

Figure 2 : Classes et familles de contrôles de sécurité décrites dans l'ITSG-33

Vous pouvez vous baser sur les contrôles de sécurité mentionnés dans le présent document et à l'annexe 3A de l'ITSG-33 [2] pour assurer la gestion des risques liés à la cybersécurité de votre organisation. Toutefois, la mise en œuvre de contrôles ne constitue qu'une partie du processus de gestion des risques liés à la sécurité des TI.

L'ITSG-33 [2] décrit également le processus de gestion des risques liés à la sécurité des TI, qui est basé sur deux niveaux d'activités : les activités associées au niveau organisationnel et celles associées au niveau du système d'information. Ces deux niveaux d'activités vous aideront à déterminer vos exigences en matière de sécurité pour l'ensemble de l'organisation et ses systèmes d'information. Après avoir compris vos exigences pour chaque niveau, vous serez en mesure d'établir les contrôles de sécurité que votre organisation devra mettre en place et maintenir pour satisfaire un niveau de risque acceptable.

2 Vulnérabilités et menaces

Les comptes d'administrateur sont des cibles de grande valeur pour les auteurs de menace. Si les auteurs de menace obtiennent accès à ces comptes, ils peuvent utiliser les privilèges élevés pour nuire à l'environnement opérationnel de votre organisation, mener leur attaque (p. ex. propager des logiciels) dans l'ensemble de votre réseau et accéder à de l'information sensible. Les auteurs de menace peuvent également prendre connaissance des activités de détection et d'atténuation menées par votre organisation pour protéger ses systèmes. Ces connaissances permettront aux auteurs de menace de contourner les mesures de détection et vous empêcheront de contrer leurs attaques.

Les auteurs de menace externes utilisent des techniques différentes, comme des maliciels et des attaques par hameçonnage, pour compromettre les réseaux et les systèmes de manière à y obtenir accès. Les compromissions peuvent découler des activités normales d'un utilisateur, comme l'ouverture de courriels ou la consultation de sites Web. Les auteurs de menace peuvent aussi exploiter des vulnérabilités connues ou utiliser des justificatifs d'identité volés pour accéder aux comptes d'administrateur. Le tableau 1 comprend quelques exemples des différentes méthodes d'attaque.

Tableau 1 : Exemples des méthodes d'attaque utilisées

Méthode d'attaque	Description
Attaque « Pass-the-Hash »	Un auteur de menace expose les justificatifs d'authentification de l'utilisateur sur un poste de travail compromis. Ces justificatifs, qui sont généralement des mots de passe hachés, sont alors utilisés dans l'ensemble du réseau pour aider l'auteur de menace à s'y déplacer latéralement.
Cassage de mot de passe	Un auteur de menace tente d'accéder aux comptes directement. Les attaques par force brute et les attaques par dictionnaire sont deux formes de cassage de mot de passe souvent utilisées. Dans le cadre d'une attaque par force brute, un auteur de menace fait appel à des outils (p. ex. un script ou un robot logiciel) pour deviner les justificatifs d'authentification, notamment les noms d'utilisateur, les mots de passe, les phrases de passe ou les numéros d'identification personnels (NIP). Dans le cadre d'une attaque par dictionnaire, un auteur de menace utilise une liste de mots souvent utilisés pour deviner le mot de passe.
Élévation des privilèges	Un auteur de menace exploite un bogue, une faille de conception ou une erreur de configuration dans le système d'exploitation ou le logiciel pour obtenir un accès privilégié et effectuer des actions non autorisées.

Méthode d'attaque	Description
Maliciel	Un auteur de menace utilise un maliciel pour obtenir accès aux comptes d'administrateur locaux ou d'un domaine. Cela pourrait survenir, par exemple, si un utilisateur vérifie ses courriels alors qu'il est connecté en tant qu'administrateur, puis ouvre une pièce jointe malveillante ou visite un site Web malveillant. Le fichier malveillant ou l'exploit peut contenir du code exécutable qui s'exécute sur la machine de l'utilisateur. L'auteur de menace peut alors prendre contrôle de la machine, installer des enregistreurs de frappe ou des logiciels de contrôle à distance pour voler les justificatifs administratifs et l'information sensible.

Une fois qu'un auteur de menace prend contrôle d'un premier point terminal (p. ex. des ordinateurs de bureau, des portables, des appareils mobiles, des serveurs), il peut entamer le processus visant à obtenir accès aux informations d'identification des comptes privilégiés, à traverser plusieurs systèmes et à accéder aux données. Les auteurs de menace peuvent également obtenir accès à vos données et à vos systèmes qui se trouvent dans l'infrastructure ou les services d'infonuagique en faisant appel à des méthodes similaires à celles employées dans l'infrastructure sur site. Les auteurs de menace veulent rester sur vos réseaux et vos systèmes aussi longtemps que possible. Ils tenteront donc de cacher leur présence et leurs activités de diverses façons, notamment en installant des dissimulateurs d'activité pour masquer les fichiers malveillants, en supprimant des applications ou en trafiquant les journaux d'événements du système et de sécurité.

Les auteurs de menace ne sont pas seulement intéressés à accéder aux comptes d'administrateur, ils veulent obtenir accès au plus grand nombre de comptes possibles, y compris les comptes d'utilisateur. Selon le modèle de contrôle d'accès adopté, les comptes d'utilisateur peuvent avoir accès à des données et à des systèmes qui sont essentiels, sensibles ou importants. Les utilisateurs à qui des privilèges d'administrateur ont été accordés peuvent apporter des changements à la configuration et aux opérations sur les réseaux, les systèmes et les dispositifs de votre organisation. Ces utilisateurs disposent de droits d'accès plus grands, ce qui peut inclure l'accès aux systèmes et aux dispositifs sur les réseaux de votre organisation, ainsi qu'à l'information sensible (p. ex. les codes de hachage des mots de passe).

La gestion des privilèges d'administrateur dans un environnement en nuage peut rendre votre organisation plus vulnérable et se traduire par un contexte de menace plus vaste. Les rôles et les responsabilités de votre organisation et du fournisseur de services infonuagiques (FSI) ou du fournisseur de services gérés (FSG) dépendront des services que vous utilisez, ainsi que des modèles de services et de déploiement adoptés. Même si votre organisation fait appel à des services infonuagiques ou gérés, il lui incombe toujours d'assurer la sécurité de ses données et de rendre des comptes à cet égard. Si elle a recours aux services d'un FSI, votre organisation est tenue d'assurer la gestion des contrôles d'accès. Pour limiter les risques, votre organisation devrait garder le plein contrôle des justificatifs d'identité de ses utilisateurs et des processus d'authentification connexes. Si vous avez externalisé vos services de TI à un FSG, vous devriez savoir à quels utilisateurs il convient d'accorder des accès privilégiés.

Pour se protéger contre les menaces, votre organisation peut adopter des stratégies d'atténuation comme la restriction des privilèges d'administrateur et la gestion des contrôles d'accès (p. ex. authentification et

autorisation), qu'il s'agisse d'une mise en œuvre locale avec un FSI ou un FSG ou d'un modèle hybride. Ces stratégies d'atténuation font en sorte qu'il est plus difficile pour les auteurs de menace d'obtenir accès aux privilèges d'administrateur et de les utiliser à mauvais escient. Ces stratégies permettent également de veiller à ce que les utilisateurs puissent accéder uniquement aux systèmes et à l'information dont ils ont besoin pour remplir leurs fonctions.

3 Authentification et autorisation (IA-2, AC-6)

Cette section donne des indications sur l'authentification et l'autorisation des comptes et des privilèges d'administrateur. Ces indications sont fondées sur les contrôles de sécurité IA-2 et AC-6. Pour de plus amples renseignements sur ces contrôles et les autres contrôles de sécurité connexes, consultez l'annexe A du présent document et l'annexe 3A de l'ITSG-33 [2].

Le contrôle des accès, qui permet de restreindre de manière sélective l'accès d'un utilisateur à des réseaux, à des systèmes et à des données, se compose des deux éléments suivants :

- Authentification : Processus ou mesure permettant de vérifier l'identité d'un utilisateur;
- Autorisation : Droits d'accès accordés à un utilisateur, à un programme ou à un processus.

Votre organisation devrait mettre en place des stratégies d'authentification des utilisateurs qui permettent d'assurer la sécurité de ses systèmes sans nuire à la convivialité. La stratégie de contrôle d'accès de votre organisation doit être maintenue lorsque vous utilisez les services d'un FSI ou d'un FSG, peu importe si les données sont stockées sur place ou dans le nuage. Si votre organisation fait appel aux services d'un FSI ou d'un FSG, elle doit absolument s'entendre avec ce dernier sur les rôles et les responsabilités liés au contrôle d'accès. Vous devriez veiller à ce que tous les systèmes d'information soient en mesure d'identifier et d'authentifier les utilisateurs organisationnels ou les processus exécutés en leur nom. Vous devriez également identifier et authentifier les utilisateurs et les dispositifs qui doivent accéder à l'information et aux services hébergés dans le nuage tout en maintenant un degré de fiabilité acceptable. Le degré de fiabilité acceptable est déterminé par votre évaluation des risques. On peut mettre en œuvre le processus d'authentification au moyen d'un inventaire des appareils, d'Active Directory et des autres stratégies et procédures de gestion des identités et de l'accès (GidA) de l'organisation.

L'authentification unique (SSO pour *Single Sign-On*) est une approche que l'on peut adopter pour éviter d'avoir à s'authentifier sur plusieurs applications. Selon l'approche de SSO, les utilisateurs obtiennent une seule identité et un seul ensemble de justificatifs d'identité qu'ils peuvent utiliser pour se connecter aux logiciels employés par votre organisation. En compromettant l'authentifiant d'un utilisateur, les auteurs de menaces peuvent obtenir un accès étendu aux systèmes, ce qui représente un risque particulièrement élevé s'il s'agit de comptes d'administrateur. Il est possible de réduire le risque associé à l'utilisation du SSO pour les comptes d'administrateur en misant sur l'authentification multifacteur, l'application du principe de droit d'accès minimal et la séparation des fonctions administratives de celles effectuées par des utilisateurs normaux.

3.1 Mettre en place l'authentification multifacteur

Vous devriez utiliser l'authentification multifacteur pour limiter l'accès réseau et local aux comptes d'administrateur, privilégiés et non privilégiés. L'authentification multifacteur fait appel à des justificatifs d'identité qui ne se limitent pas aux noms d'utilisateur et aux mots de passe pour se connecter aux comptes. Ces justificatifs d'identité additionnels peuvent comprendre des numéros d'identification personnels (NIP), des jetons physiques ou numériques, des cartes à puce ou des données biométriques. Pour ajouter une couche additionnelle à la sécurité de vos comptes, il convient de combiner l'authentification multifacteur à ce qui suit :

1. quelque chose que vous connaissez (p. ex. un mot de passe, une phrase de passe ou un NIP);
2. quelque chose que vous avez (p. ex. un jeton physique, une carte à puce);
3. quelque chose qui vous caractérise (p. ex. une donnée biométrique comme une empreinte digitale).

Pour être considérée comme une solution valide, l'authentification multifacteur doit utiliser des justificatifs d'identité appartenant à au moins deux des trois différentes catégories mentionnées précédemment (p. ex. la saisie de deux mots de passe n'est pas considérée un mécanisme d'authentification multifacteur valide).

Si votre organisation a déjà recours à un FSI ou prévoit le faire éventuellement, assurez-vous que les applications fournies par l'infrastructure en nuage ou le FSI prennent en charge l'authentification multifacteur. Vous devriez également appliquer l'authentification multifacteur aux comptes d'administration du service de portail infonuagique et aux comptes de récupération connexes. Il est également important de veiller à ce que tous les comptes du service en nuage, y compris les comptes de récupération et d'administration du service de portail infonuagique, utilisent des mots de passe et des facteurs d'authentification différents de ceux employés dans l'infrastructure locale de l'organisation.

Les méthodes d'attaque utilisées par les auteurs de menace continuent d'évoluer. Ces derniers ont recours à des méthodes comme des attaques par force brute, des enregistreurs de frappe, l'hameçonnage et le piratage psychologique pour voler les mots de passe. L'authentification multifacteur est la mesure de protection la plus efficace contre les attaques par vol de mot de passe.

Pour de plus amples renseignements sur les phrases de passe et les mots de passe complexes, voir Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) [4] at and Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.015) [5]

3.2 Appliquer le principe du droit d'accès minimal

Le principe du droit d'accès minimal est un principe selon lequel il convient de n'accorder à l'utilisateur que les autorisations d'accès dont il a besoin pour accomplir les tâches autorisées. Ce principe permet de limiter les dommages pouvant résulter de l'utilisation ou de la consultation accidentelle, incorrecte ou non autorisée des systèmes ou de l'information.

Les fonctions administratives devraient se limiter aux personnes qui ont besoin de ce niveau de privilège. Vous pourriez considérer la création de processus, de rôles et de comptes de système d'information additionnels, au

besoin, pour maintenir le principe du droit d'accès minimal. Vous pouvez accorder des privilèges aux utilisateurs de façon plus précise en utilisant des domaines de traitement séparés. Par exemple, vous pouvez avoir recours à des techniques de virtualisation pour permettre à un utilisateur d'avoir des privilèges additionnels lorsqu'il utilise une machine virtuelle et des privilèges limités dans d'autres environnements.

Il convient de tenir compte des questions clés ci-dessous au moment d'accorder des privilèges d'administrateur :

- Quelles tâches exigent des privilèges d'administrateur et combien d'employés sont nécessaires pour accomplir ces tâches?
- Comment les activités de nature administrative sont-elles journalisées et qui est responsable de passer en revue et de vérifier ces journaux d'activités?
- Des mesures de protection de la sécurité adéquates ont-elles été mises en place pour gérer et contrôler ces privilèges d'administrateur?

Le modèle de contrôle de l'accès que vous décidez de mettre en œuvre varie selon le type et le degré de sensibilité des données gérées et traitées par votre organisation. Faire appel à la classification des données et accorder les accès en fonction de ces classifications peut faciliter la gestion des accès et le maintien du droit d'accès minimal. Le contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*) peut également être considéré comme un modèle de contrôle des accès. Le RBAC met en correspondance les droits d'accès des utilisateurs au rôle qu'ils jouent dans l'organisation. Plusieurs FSI permettent de sélectionner un modèle de classification des données et de contrôle d'accès dans leurs ensembles de services prêts à l'emploi. Si votre organisation dispose d'un modèle de nuage hybride sur site, elle peut demander à une entreprise tierce de travailler avec son personnel de TI pour classifier les données dans ses référentiels locaux et distants.

4 Gestion des comptes d'administrateur (AC-2, AC-17(100), SC-3)

Cette section offre des conseils sur la gestion des comptes d'administrateur et les privilèges connexes qu'il convient d'utiliser si votre organisation utilise un modèle sur site, en nuage ou hybride. Ces indications sont fondées sur les contrôles de sécurité AC- 2, AC-17(100) et SC-3. Pour de plus amples renseignements sur ces contrôles et les autres contrôles connexes, consultez l'annexe A du présent document et l'annexe 3A de l'ITSG-33 [2].

En assurant la gestion et le contrôle des comptes d'administrateur et des privilèges connexes, votre organisation veille à ce que son environnement d'exploitation soit stable, fiable et plus facile à soutenir et à gérer. Une bonne gestion des comptes et un contrôle approprié des accès font en sorte que moins d'utilisateurs peuvent apporter des changements importants à l'environnement opérationnel. Il est également possible de simplifier l'administration et le soutien de votre réseau.

Si vous gérez vos comptes d'administrateur et les privilèges connexes, il est plus difficile pour les auteurs de menace de compromettre vos réseaux et vos systèmes. Les auteurs de menace ciblent ces comptes dans l'intention de mener à bien leurs attaques (p. ex. propager un maliciel, élever les privilèges) dans l'ensemble du réseau et d'accéder à l'information sensible.

4.1 Séparer les fonctions et les stations de travail administratives

Les compromissions peuvent découler des activités normales d'un utilisateur, comme l'ouverture de courriels ou la consultation de sites Web. Votre organisation s'expose à de plus grands risques si vos utilisateurs sont en mesure d'accéder aux services de courrier et aux sites Web lorsqu'ils sont connectés à leur compte d'administrateur. Un utilisateur n'a pas besoin d'avoir un compte lui accordant à la fois un accès utilisateur normal aux réseaux, dont Internet et les services de courrier, et des privilèges d'administrateur. Les utilisateurs disposant de privilèges d'administrateur devraient avoir un compte d'administrateur séparé avec des justificatifs d'identité distincts, peu importe l'environnement de votre organisation (en nuage, sur site ou hybride).

Pour déterminer et séparer les fonctions administratives des fonctions non administratives, il convient de tenir compte de ce qui suit :

- les rôles d'utilisateur exigeant un accès aux données sensibles (y compris les utilisateurs de votre FSI et FSG);
- les responsabilités, l'imputabilité et les tâches associées à chaque rôle d'utilisateur;
- les tâches exigeant des privilèges d'administrateur;
- les utilisateurs qui doivent effectuer des tâches administratives et sont autorisés à le faire;
- la période (c.-à-d., en permanence ou pour une durée prédéterminée) durant laquelle les utilisateurs doivent accomplir des tâches administratives (p. ex. tâches permanentes ou urgentes).

Il est fortement recommandé de créer des comptes d'administrateur séparés pour les utilisateurs qui en ont besoin. Assurez-vous que ces comptes d'administrateur ne permettent pas d'accéder à Internet ou aux services de

courrier, puisque cela pourrait exposer inutilement votre organisation aux auteurs de menace. Assurez-vous que les tâches administratives sont effectuées sur des ordinateurs administratifs dédiés qui ne peuvent pas accéder à Internet ou aux services de courrier. Pour ce qui est de l'accès à distance, la section AC-17(100) de l'annexe 3A de l'ITSG-33 [22] stipule que l'accès à distance à des comptes privilégiés devrait s'effectuer à partir de consoles de gestion spécialisées régies entièrement par les stratégies de sécurité du système et utilisées exclusivement à cette fin (p. ex. l'accès à Internet n'est pas autorisé). Pour l'administration du nuage à partir de cette station de travail dédiée, il convient d'utiliser un RPV ou des listes d'applications autorisées pour accéder à l'architecture du nuage.

Votre organisation devrait créer et maintenir un inventaire de tous ses comptes d'administrateur, dont les comptes locaux et de domaine. Vous pourriez vouloir mettre en place des restrictions (p. ex. l'heure du jour, le jour de la semaine, l'emplacement de connexion) pour les comptes d'administrateur utilisés dans un environnement sur site. Il importe de souligner que dans certaines circonstances, de telles restrictions peuvent empêcher les utilisateurs d'effectuer des actions, comme prendre les mesures d'intervention nécessaires si un incident survient en dehors de la plage horaire établie ou ailleurs que dans les emplacements déterminés.

Peu importe les restrictions appliquées à la gestion des comptes d'administrateur et des privilèges connexes de votre organisation, il convient de les stipuler dans l'accord sur les niveaux de service conclu avec votre FSG, car ce dernier doit se conformer aux mêmes stratégies et restrictions.

4.2 Mettre en place l'intégrité par deux personnes (TPI) et la double autorisation des comptes administrateur

La validation et la vérification des tâches administratives sensibles associées aux données hautement sensibles ou aux systèmes essentiels peuvent aider à protéger l'environnement de votre organisation. Pour ce faire, on peut faire appel à l'intégrité par deux personnes (TPI pour *Two Person Integrity*) et à la double autorisation.

Selon le principe de la TPI, au moins deux personnes autorisées doivent simultanément accéder au système pour effectuer une tâche critique. Il est ainsi possible de réduire le risque lié à l'utilisation de justificatifs d'identité volés pour accéder à vos processus ou à votre information sensible. La TPI permet également de garantir que seules les personnes ayant un besoin de connaître peuvent accéder à l'information sensible. L'utilisation d'un système à deux clés constitue un exemple d'application de la TPI au niveau d'accès administrateur. Une clé est remise aux deux administratrices ou administrateurs et ces deux clés sont nécessaires pour effectuer une tâche ou la mener à bien.

La double autorisation garantit que les tâches sensibles ou les opérations administratives effectuées sur les systèmes exigent l'approbation d'au moins deux personnes autorisées avant que des changements ne soient apportés au système.

Votre organisation pourrait aussi mettre en place une forme de TPI pour la diffusion des justificatifs d'identité aux utilisatrices et utilisateurs. Une administratrice ou un administrateur peut fournir à ces derniers la moitié du mot de passe ou de la phrase de passe nécessaire pour se connecter à l'environnement, alors qu'une autre personne en mesure de les authentifier, comme leur gestionnaire, leur fournit l'autre moitié. Selon cette approche, aucun

accès immédiat aux systèmes et aux données critiques n'est accordé et une deuxième personne doit effectuer le processus d'authentification avant d'autoriser le moindre accès.

Pour de plus amples renseignements sur l'accès à distance sécurisé, prière de consulter Conseils de sécurité pour les organisations dont les employés travaillent à distance (ITSAP.10.016,) [6].

4.3 Journaliser et surveiller les comptes privilégiés

Votre organisation doit décrire les conditions ou les circonstances particulières selon lesquelles les comptes d'administrateur et privilégiés peuvent être utilisés (p. ex. certains jours de la semaine, à certaines heures du jour ou pour une durée précise). Les systèmes d'information devraient utiliser des journaux de vérification qui détaillent les actions effectuées au moyen des comptes privilégiés (p. ex. changements apportés au système, connexions aux comptes et déconnexions). Aux fins d'attribution, tous les comptes d'administrateur devraient être liés à une personne identifiable.

On recommande de configurer vos systèmes d'information de manière à journaliser le moindre changement apporté à un compte d'administrateur (p. ex. quand un compte est ajouté ou supprimé). Les journaux de vos systèmes devraient également faire mention des tentatives infructueuses de connexion aux comptes. Les actions et les événements enregistrés dans les journaux devraient indiquer l'estampille temporelle.

Si votre organisation fait appel aux services d'un FSI ou d'un FSG, il convient d'assurer une surveillance continue des événements et des performances des systèmes. Le FSI ou le FSG devrait vous remettre les journaux de vérification réguliers qui contiennent les rapports d'accès pour tous les comptes d'administrateur [7].

Vous pouvez utiliser les journaux de vos systèmes et ceux fournis par le FSI ou le FSG pour établir une base de référence en ce qui a trait au comportement d'un utilisateur administratif ou privilégié normal. Vous devriez régulièrement passer en revue les journaux de vérification pour détecter tout comportement inhabituel. Veillez à ce qu'un horaire soit en place pour déterminer à quelle fréquence les journaux et l'information de vérification sont passés en revue.

Assurez-vous que toute l'information de vérification (p. ex. les enregistrements de vérification, les rapports) est bien recueillie et conservée. Dans la mesure du possible, vous devriez stocker l'information de vérification dans un système ou un référentiel inviolable physiquement séparé.

4.4 Supprimer les comptes et retirer les accès privilégiés

Les besoins de votre organisation pour certains comptes d'administrateur et privilèges connexes peuvent changer. Les utilisateurs peuvent, par exemple, assumer de nouvelles fonctions ou quitter votre organisation. Vous devriez passer en revue l'ensemble des comptes d'utilisateur sur une base régulière, en particulier les comptes d'administrateur et les privilèges connexes, afin de confirmer qu'ils sont toujours utilisés par les utilisateurs à qui ils ont été attribués. Au moment de vérifier ces comptes et privilèges, déterminez si les besoins opérationnels et les exigences en matière de sécurité font en sorte qu'il est nécessaire de les réattribuer ou de les retirer. Cette

vérification devrait également inclure les comptes et les privilèges associés à votre FSI ou FSG et être ajoutée en tant qu'exigence dans les ententes touchant la prestation de services.

Il ne faut pas oublier que les comptes temporaires et d'urgence sont différents des comptes utilisés peu fréquemment (p. ex. les comptes locaux utilisés pour réaliser des tâches particulières définies par les organisations ou lorsque les ressources réseau ne sont pas disponibles). Ces comptes demeurent activés et ne sont pas assujettis aux dates de retrait ou de désactivation automatique. Les conditions de désactivation des comptes peuvent inclure ce qui suit :

- lorsque les comptes partagés, temporaires, de groupe ou d'urgence ne sont plus requis;
- lorsque des employés ou des entrepreneurs quittent l'organisation;
- advenant le départ ou le transfert des employés ou des entrepreneurs.

Vous devriez déterminer le délai après lequel les comptes inactifs sont désactivés.

5 Résumé

Parmi les 10 mesures de sécurité des TI recommandées par le CST, une consiste à assurer la gestion et le contrôle des privilèges d'administrateur. Ce document traite des pratiques exemplaires recommandées par le CST pour ce qui est de protéger les comptes d'administrateur de votre organisation et les privilèges connexes contre les compromissions, peu importe si un modèle hybride, sur site, en nuage ou avec FSG a été adopté. Au moment d'attribuer des comptes d'administrateur ou des accès privilégiés à des employés, gardez à l'esprit les considérations suivantes :

- créer des comptes non administratifs séparés de ceux utilisés pour effectuer des fonctions non administratives (p. ex. vérification des courriels);
- utiliser des méthodes d'authentification robustes :
  - utiliser un mot de passe ou une phrase de passe unique pour chaque compte privilégié;
  - modifier les mots de passe par défaut pour les applications et les dispositifs;
  - authentifier les utilisateurs avant qu'ils obtiennent accès aux applications ou aux dispositifs;
  - utiliser l'authentification multifacteur;
- veiller à ce que des comptes uniques et identifiables soient remis à chaque utilisateur (c.-à-d., attribution);
- fournir de la formation sur les comportements attendus des utilisateurs disposant de comptes privilégiés (p. ex. se déconnecter des comptes privilégiés lorsqu'ils ne sont pas utilisés);
- retirer ou supprimer les privilèges d'accès spéciaux dès qu'un utilisateur n'en a plus besoin.

Ces pratiques exemplaires sont fondées sur les contrôles de sécurité décrits à l'annexe A du présent document et à l'annexe 3A de l'ITSG-33 [2]. Une gestion efficace des comptes privilégiés et des droits d'accès empêche les auteurs de menace de prendre le contrôle des comptes privilégiés et de propager les exploits dans l'ensemble de votre réseau ou de vos systèmes, ou dans les données stockées dans le nuage. Selon la taille de votre organisation, il pourrait être difficile de sécuriser adéquatement tous les aspects de votre infrastructure de TI. Vous pouvez toutefois concentrer vos efforts sur les comptes privilégiés qui pourraient, advenant leur compromission, exposer votre organisation à de plus grands risques.

La gestion des comptes privilégiés n'est toutefois qu'un aspect du renforcement de votre posture de cybersécurité. Pour mieux protéger votre organisation contre les cybermenaces, vous devriez passer en revue et mettre en place l'ensemble des mesures recommandées dans l'ITSM.10.089 [1]. Parmi les autres mesures que votre organisation devrait prendre, on retrouve la sensibilisation des employés à la cybersécurité, la protection des points terminaux par l'application de correctifs ou la mise en œuvre d'une liste d'applications autorisées, et l'isolation des applications Web.

5.1 Coordonnées

Pour de plus amples renseignements sur la mise en œuvre des conseils formulés dans la présente ou d'une autre des 10 mesures de sécurité des TI, communiquez par téléphone ou par courriel avec le :

Centre d'appel

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

6 Contenu complémentaire

6.1 Liste d'abréviations, d'acronymes et de sigles

Acronyme ou sigle	Définition
AC	Contrôle d'accès (*Access Control*) (famille de contrôles de sécurité)
FSG	Fournisseur de services gérés
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
GIdA	Gestion de l'identité et de l'accès
IA	Identification et authentification (famille de contrôles de sécurité)
MFA	Authentification multifacteur (*Multi-Factor Authentication*)
NIP	Numéro d'identification personnel
RBAC	Contrôle d'accès basé sur les rôles (*Rule-Based Access Control*)
SC	Protection des systèmes et des communications (familles de contrôles de sécurité)
SSO	Authentification unique (*Single Sign-On*)
TI	Technologies de l'information

6.2 Glossaire

Acronyme ou sigle	Définition
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Autorisation	Droits d'accès accordés à un utilisateur, à un programme ou à un processus.
Bien de TI	Composante d'un système d'information, ce qui comprend notamment les applications opérationnelles, les données, le matériel et les logiciels.
Compte par défaut	Autorisations utilisateur génériques, généralement des droits d'accès administratifs, et les mots de passe fournis par défaut pour les applications et le matériel. Le compte par défaut est utilisé lors de la configuration initiale des applications et du matériel.
Confidentialité	Aptitude à protéger l'information sensible contre les accès non autorisés.
Contrôle d'accès	Attestation confirmant que seul un accès autorisé est donné aux biens (tant physiques qu'électroniques). Pour les biens physiques, des contrôles d'accès peuvent être nécessaires pour les installations ou les zones d'accès limité (p. ex. le contrôle des visiteurs et du matériel aux points d'entrée, l'accompagnement des visiteurs). Pour les biens de TI, des contrôles d'accès peuvent être nécessaires pour les réseaux, les systèmes et l'information (p. ex. limiter l'accès à certains systèmes à des utilisateurs, limiter les privilèges du compte).
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité, qu'il convient d'appliquer à un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs TI connexes. Ces contrôles peuvent être appliqués au moyen de diverses solutions de sécurité, notamment des produits, des stratégies, des pratiques et des procédures de sécurité.

Acronyme ou sigle	Définition
Contrôle de sécurité de gestion	Contrôle de sécurité qui porte principalement sur la gestion de la sécurité des TI et les risques liés à la sécurité des TI.
Contrôle de sécurité opérationnel	Contrôle de sécurité qui est principalement mis en œuvre et exécuté par des personnes, mais habituellement fondé sur l'utilisation de la technologie (p. ex. un logiciel de soutien).
Contrôle de sécurité technique	Contrôles de sécurité techniques qui sont mis en œuvre et exécutés par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité intégrés aux composants matériels, logiciels et micrologiciels.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un dispositif.
Défense en profondeur	Concept de sécurité des TI (aussi appelé approche *Castle*) en vertu duquel plusieurs couches de sécurité sont utilisées pour protéger l'intégrité de l'information. Ces couches peuvent comprendre un antivirus et un antimaliciel, un coupe-feu, des mots de passe hiérarchiques, une détection d'intrusion et une identification biométrique.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Hachage	Fonction mathématique servant à convertir un bloc ou groupe de données en une valeur de longueur fixe, habituellement plus courte que les données d'origine. Le hachage masque les données d'origine par une autre valeur qu'on ne peut décoder qu'en recherchant la valeur dans un tableau de hachage.
Hameçonnage	Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à une personne, à un groupe ou à une organisation en usurpant ou en imitant une certaine marque généralement bien connue dans le but d'obtenir habituellement des gains financiers. Les hameçonneurs incitent les utilisateurs à donner leurs renseignements personnels (numéros de cartes de crédit, données bancaires ou autres renseignements sensibles) afin de s'en servir pour commettre des actes frauduleux.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Les maliciels les plus courants sont les virus informatiques, les rançongiciels, les logiciels espions et les logiciels publicitaires.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs et à l'information de TI.
Point terminal	Dispositif informatique distant (p. ex. un portable, un ordinateur de bureau, un téléphone mobile) qui communique avec un réseau auquel il est connecté.
Rançongiciels	Type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'il ait payé une rançon.
Risque	Degré de probabilité qu'un auteur de menace exploite une vulnérabilité pour accéder à un bien et répercussions connexes.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée par un auteur de menace en vue de compromettre les biens ou les activités d'une organisation.

6.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, *ITSM.10.089, Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information*, septembre 2021.
2	Centre canadien pour la cybersécurité, *ITSG-33, La gestion des risques liés à la sécurité des TI :Une méthode axée sur le cycle de vie*, novembre 2012.
3	Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, version 1.1, juin 2019.
4	Centre canadien pour la cybersécurité, *ITSAP.30.032 – Pratiques exemplaires de création de phrases de passe et de mots de passe*, septembre 2019.
5	Centre canadien pour la cybersécurité, Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.015), mai 2023.
6	Centre canadien pour la cybersécurité, consulter Conseils de sécurité pour les organisations dont les employés travaillent à distance (ITSAP.10.016), mai 2020.
7	Gouvernement du Canada, *GC Cloud Guardrails* (en anglais seulement).

Annexe A : Catalogue des contrôles de sécurité tiré de l'ITSG-33

A.1 Contrôles de sécurité techniques : Contrôle d'accès

Le tableau 2 décrit les contrôles **AC-2 Gestion de compte** et **AC-6 Droit d'accès minimal**, mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 2 : Contrôles de sécurité techniques de l'ITSG-33 : AC-2, A-6 et AC-17(100)

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
AC-2	Gestion de compte	(A) L'organisation établit et sélectionne les types de comptes de système d'information suivants pour appuyer les fonctions opérationnelles et ses missions : [*types de compte de système d'information définis par l'organisation*]. (B) L'organisation nomme des gestionnaires de compte pour les comptes de système d'information. (C) L'organisation établit les conditions pour les membres des groupes et des rôles. (D) L'organisation précise les utilisateurs autorisés du système d'information, les membres des groupes et des rôles, ainsi que les autorisations d'accès (c.-à-d. les droits d'accès) et autres attributs (au besoin) pour chaque compte. (E) L'organisation doit obtenir l'approbation de [*personnel ou rôles définis par l'organisation*] pour les demandes de création de comptes de système d'information.	**Gestion automatisée de compte de système :** L'organisation fait appel à des mécanismes automatisés pour appuyer la gestion des comptes du système d'information. **Retrait des comptes temporaires d'urgence :** Le système d'information [*Sélection : retire ou désactive*] automatiquement les comptes temporaires et d'urgence après [*délai défini par l'organisation pour chaque type de compte*]. **Désactivation des comptes inactifs :** Le système d'information désactive automatiquement les comptes inactifs après [*délai défini par l'organisation*]. **Vérification automatisée :** Le système d'information vérifie automatiquement les activités de création, de modification, d'activation, de	AC-3 AC-4 AC-5 AC-6 AC-10 AC-17 AC-19 AC-20 AU-9 IA-2 IA-4 IA-5 IA-8 CM-5 CM-6 CM-11 MA-3 MA-4 MA-5 PL-4

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
		(F) L'organisation crée, active, modifie, désactive et retire les comptes de système d'information conformément aux [*conditions ou procédures définies par l'organisation*]. (G) L'organisation surveille l'utilisation des comptes de système d'information. (H) L'organisation informe les gestionnaires de compte : i. lorsque les comptes ne sont plus requis; ii. lorsque les utilisateurs quittent leur poste ou sont transférés; iii. lorsque l'utilisation du système d'information ou le besoin de connaître d'un utilisateur change. (I) L'organisation autorise l'accès au système d'information selon : i. une autorisation d'accès valide; ii. l'utilisation prévue du système; iii. d'autres attributs exigés par l'organisation ou des missions ou fonctions opérationnelles connexes. (J) L'organisation examine les comptes pour s'assurer qu'ils sont conformes aux exigences en matière de gestion des comptes tous les [*fréquence définie par l'organisation*]. (K) L'organisation établit un processus de réattribution des justificatifs d'identité de compte partagé ou de groupe (s'ils sont	désactivation et de retrait des comptes, et envoie des avis à [*personnel ou rôles définis par l'organisation*]. Voir les contrôles connexes AU-2 et AU-12. **Fermeture de session après un délai d'inactivité :** L'organisation exige que les utilisateurs ferment leur session après [*délai d'inactivité prévu ou description du moment de la fermeture de session défini par l'organisation*]. Voir le contrôle connexe SC-23. **Gestion dynamique des droits d'accès :** Le système d'information met en œuvre les capacités suivantes de gestion dynamique des droits d'accès : [*liste des capacités de gestion dynamique des droits d'accès définie par l'organisation*]. Voir le contrôle connexe AC-16. **Plans basés sur les rôles :** i. L'organisation établit et administre les comptes utilisateur privilégiés conformément à un plan de contrôle d'accès basé sur les rôles qui regroupe l'accès et les droits d'accès au système d'information permis par rôle. ii. L'organisation surveille les attributions de rôles privilégiés. iii. L'organisation prend [*mesures définies par l'organisation*] lorsque les attributions de rôles privilégiés ne conviennent plus.	SC-13

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
		déployés) lorsque des utilisateurs sont retirés du groupe.	**Création dynamique de comptes :** Le système d'information crée [*comptes de système d'information définis par l'organisation] de façon dynamique*. Voir le contrôle connexe AC-16. **Restrictions liées à l'utilisation de comptes partagés et de comptes de groupe :** L'organisation autorise uniquement l'utilisation des comptes partagés et de groupe qui répondent aux [*conditions relatives à l'établissement de comptes partagés et de groupe définies par l'organisation*]. **Suppression des justificatifs d'identité de comptes partagés et de comptes de groupe :** Le système d'information supprime les justificatifs d'identité des comptes partagés ou de groupe lorsque les membres quittent le groupe. **Conditions d'utilisation :** Le système d'information applique [*circonstances et/ou conditions d'utilisation définies par l'organisation*] aux [*comptes du système d'information définis par l'organisation*]. **Surveillance et utilisation irrégulière des comptes :** i. L'organisation surveille les comptes de système d'information afin de détecter	

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
			[*utilisation irrégulière définie par l'organisation*]. ii. L'organisation signale l'utilisation irrégulière des comptes de système d'information à [*personnel ou rôles définis par l'organisation*]. Voir le contrôle connexe CA-7. **Désactivation des comptes des utilisateurs à risque élevé :** L'organisation désactive les comptes des utilisateurs qui présentent un risque élevé dans un délai de [*délai défini par l'organisation]* après la découverte du risque.	
AC-6	Droit d'accès minimal	(A) L'organisation adhère au principe du droit d'accès minimal, ce qui autorise l'accès uniquement aux utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées conformément aux missions et aux fonctions opérationnelles de l'organisation.	**Domaines de traitement séparés :** Le système d'information fournit des domaines de traitement séparés pour permettre une granularité plus fine dans l'attribution des droits d'accès utilisateur. Voir les contrôles connexes AC-4, SC-3, SC-30 et SC-32.	AC-2 AC-3 AC-5 CM-6 CM-7 PL-2
AC-17	Accès à distance	(A) L'organisation définit et consigne 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. (B) L'organisation autorise l'accès à distance au système d'information avant d'autoriser de telles connexions.	L'accès à distance à des comptes privilégiés s'effectue à partir de consoles de gestion spécialisées régies entièrement par les stratégies de sécurité du système et utilisées exclusivement à cette fin (p. ex. l'accès à Internet n'est pas autorisé).	s.o.

A.2 Contrôles de sécurité techniques : Identification et authentification

Le tableau 3 décrit les contrôles **IA-2 Identification et authentification (utilisateurs organisationnels)**, mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 3 : Contrôles de sécurité techniques de l'ITSG-33 : IA-2

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
IA-2	Identification et authentification (utilisateurs organisationnels)	(A) Le système d'information identifie de façon unique et authentifie les utilisateurs organisationnels (ou les processus exécutés en leur nom).	**Accès réseau aux comptes privilégiés :** Le système d'information utilise l'authentification multifacteur pour l'accès réseau aux comptes privilégiés. Voir le contrôle connexe AC-6. **Accès réseau aux comptes non privilégiés :** Le système d'information utilise l'authentification multifactoreur pour l'accès réseau aux comptes non privilégiés. **Accès local aux comptes privilégiés :** Le système d'information applique l'authentification multifacteur pour l'accès local aux comptes privilégiés. Voir le contrôle connexe AC-6. **Accès local aux comptes non privilégiés :** Le système d'information applique l'authentification multifacteur pour l'accès local aux comptes non privilégiés.	AC-2 AC-3 AC-14 AC-17 AC-18 IA-4 IA-5 IA-8

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
			Authentification de groupe : L'organisation exige des utilisateurs qu'ils soient authentifiés par un authentifiant individuel lorsqu'un authentifiant de groupe est utilisé. **Accès réseau aux comptes privilégiés – dispositif distinct :** Le système d'information utilise l'authentification multifacteur pour l'accès réseau aux comptes privilégiés de la manière suivante : un des facteurs est fourni par un dispositif distinct du système demandant l'accès et le dispositif satisfait [*exigences de la force du mécanisme définies par l'organisation*]. Voir le contrôle connexe AC-6. **Accès réseau aux comptes non privilégiés – résistance à la réinsertion :** Le système d'information applique des mécanismes d'authentification résistants à la réinsertion pour l'accès réseau aux comptes non privilégiés. **Authentification unique (SSO) :** Le système d'information offre une fonctionnalité d'authentification unique (SSO) pour [*liste définie par l'organisation des services et des comptes du système d'information*].	

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
			Accès à distance – dispositif distinct : Le système d'information applique l'authentification multifacteur pour l'accès local aux comptes non privilégiés où l'un des facteurs est fourni par un dispositif distinct du système d'information auquel l'utilisateur accède. Le dispositif satisfait [*exigences de la force du mécanisme définies par l'organisation*]. Voir le contrôle connexe AC-6. **Acceptation des justificatifs de vérification de l'identité personnelle (PIV) :** Le système d'information accepte et vérifie électroniquement les justificatifs de vérification de l'identité personnelle (PIV pour *Personal Identity Verification*). Voir les contrôles connexes AU-2, PE 3 et SA-4. **Authentification hors bande :** Le système d'information applique [*authentification hors bande définie par l'organisation*] si les circonstances suivantes sont présentes : [*conditions définies par l'organisation*]. Voir les contrôles connexes IA-10, IA-11 et SC-37.	

A.3 Contrôles de sécurité techniques : Protection des systèmes et des communications

Le tableau 4 décrit les contrôles **SC-3 Isolation de la fonction de sécurité** mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 4 : Contrôles de sécurité techniques de l'ITSG-33 : SC-3

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
SC-3	Isolement des fonctions de sécurité	(A) Le système d'information isole les fonctions de sécurité des autres fonctions.	**Séparation du matériel :** Le système d'information a recours à des mécanismes sous-jacents de séparation matérielle pour mettre en œuvre l'isolement des fonctions de sécurité. **Accès et fonctions de contrôle des flux :** Le système isole 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. **Réduction des fonctionnalités n'ayant pas trait à la sécurité :** L'organisation réduit à son minimum le nombre des fonctions non liées à la sécurité appelées à intégrer le périmètre isolé qui comprend les fonctions de sécurité. **Jumelage et cohésion des modules :** L'organisation applique les fonctions de sécurité sous forme de modules essentiellement indépendants qui maximisent la cohésion interne des modules et réduisent les jumelages entre modules.	AC-3 AC-6 SA-4 SA-5 SA-8 SA-13 SC-2 SC-7 SC-39

Numéro	Contrôle	Exigence	Améliorations de contrôle	Contrôles de l'ITSG-33 connexes
			Structures en couches : L'organisation applique 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.	