Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI :

N° 7, Protéger l'information au niveau de l'organisme

SÉRIE GESTIONNAIRES

ITSM.10.097

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 l'ITSM.10.089, Les 10 mesures de sécurité des technologies de l'information visant à protéger les réseaux Internet et l'information [1][1].

Date d'entrée en vigueur

Le présent document entre en vigueur le 09 février 2022.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion	09 février 2022

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

Vue d'ensemble

Parmi les 10 mesures de sécurité des TI recommandées par le CST, l'une consiste à assurer la gestion de l'information au niveau de l'organisme. L'information de votre organisation est non seulement importante pour assurer la continuité de vos opérations, mais elle est aussi une cible de premier choix pour les auteurs de menace qui cherchent à compromettre les systèmes et l'information.

Afin de protéger l'information de votre organisation au niveau de l'organisme, vous devriez envisager les mesures suivantes : évaluer et établir la valeur de l'information, la gérer tout au long de son cycle de vie, choisir le bon modèle organisationnel de déploiement des dispositifs mobiles, utiliser les systèmes d'information externes en toute sécurité et établir un programme de surveillance de la conformité.

La présente publication fait partie d'une série de documents axés sur les 10 mesures de sécurité des TI recommandées dans l'ITSM.10.089 [1]. Bien que la mise en œuvre de l'ensemble des 10 mesures de sécurité recommandées puisse rendre votre organisation moins vulnérable aux cybermenaces, vous devriez examiner les activités que vous menez sur le plan de la cybersécurité pour déterminer s'il convient de prendre des mesures supplémentaires. Pour obtenir de plus amples renseignements sur la mise en œuvre des 10 mesures de cybersécurité, veuillez communiquer par téléphone ou par courriel avec le :

Centre d'appel
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

D97-4/10-097-2023F-PDF

978-0-660-46922-5

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Introduction

Le présent document donne des indications sur les mesures que peut prendre votre organisation pour protéger l'information au niveau organisationnel. La présente est fondée sur les conseils formulés respectivement dans l'ITSM.10.089 [1] et l'annexe 3A de l'ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie [2].

Pour être en mesure de protéger l'information de votre organisation au niveau organisationnel, vous devez prendre des mesures pour gérer les risques, être conforme aux exigences législatives et politiques, et mettre en œuvre des contrôles de sécurité. Le présent document définit certaines des mesures que vous pouvez prendre, notamment les suivantes :

- évaluer et déterminer la valeur et le niveau de sensibilité de l'information;
- gérer l'information tout au long de son cycle de vie (p. ex. étiquetage, traitement, conservation et destruction des données);
- choisir un modèle organisationnel de déploiement des dispositifs mobiles pour vous aider à gérer les dispositifs utilisés au sein de votre organisation;
- comprendre les risques associés à l'utilisation de systèmes d'information externes;
- établir un programme de surveillance de la conformité.

Les conseils énoncés dans le présent document ne sont pas exhaustifs. On y décrit seulement certains des contrôles de sécurité que vous pouvez 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 minimal.

Avant de mettre en œuvre une mesure de sécurité, vous devriez procéder à l'évaluation des risques afin de cerner 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 déterminer les contrôles dont votre organisation a besoin pour protéger ses actifs. La mise en œuvre de contrôles superflus peut donner lieu à des inefficacités et entraîner des dépenses inutiles. Après avoir établi 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 activités de cybermenace et des répercussions de ces activités sur les réseaux connectés à Internet. La mise en œuvre des 10 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 menées actuellement par votre organisation sur le plan de la sécurité et de la gestion des risques.

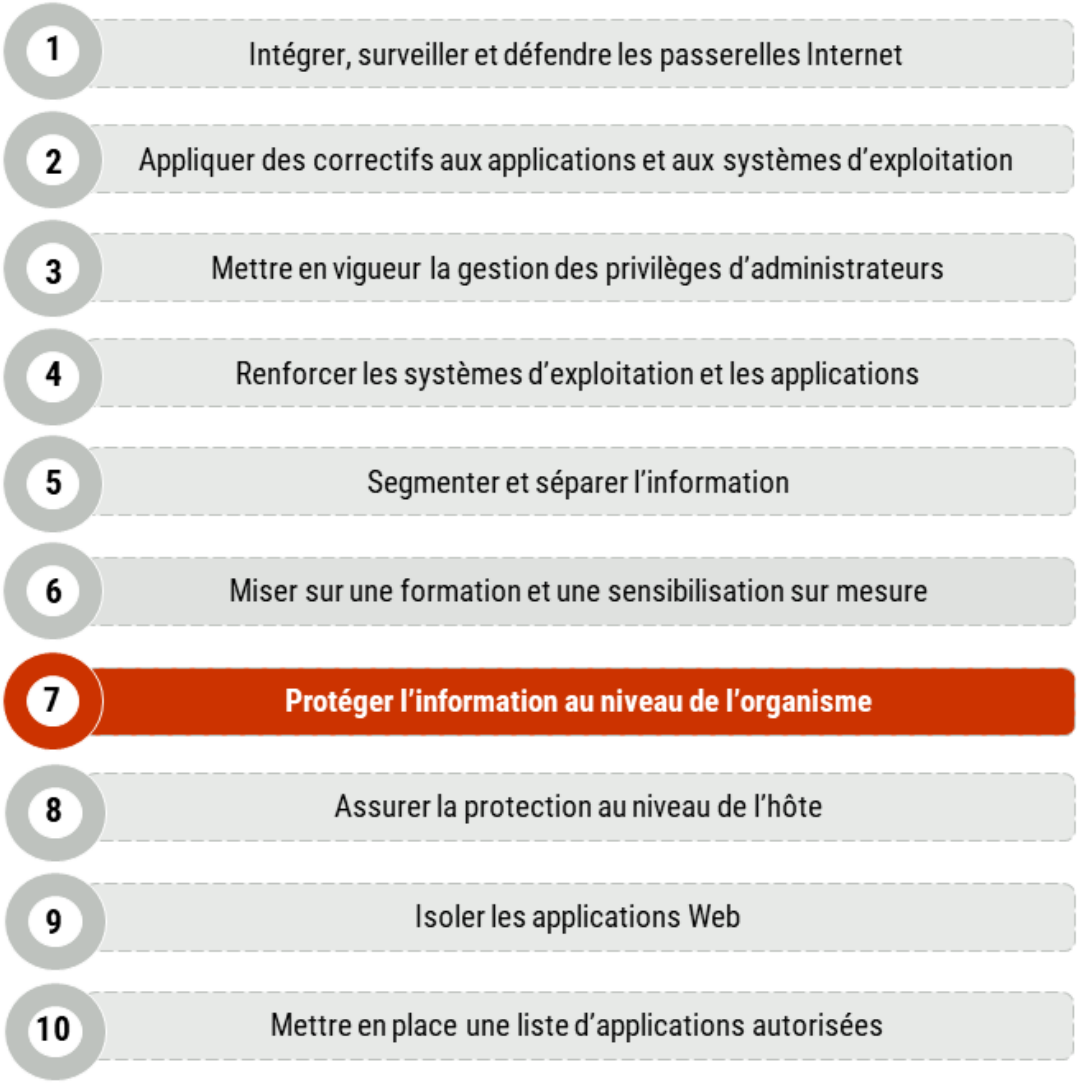

Figure 1 : Les 10 mesures de sécurité des TI – Nº 7, Protéger l'information au niveau de l'organisme

1.2 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 permettant à une organisation de gérer les risques relevant de la sécurité des TI. Il comprend un catalogue de contrôles de sécurité (c.-à-d. un ensemble normalisé d'exigences de sécurité visant à protéger la confidentialité, l'intégrité et la disponibilité des actifs 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 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, les conseils formulés dans la présente publication sont fondés sur plusieurs contrôles de sécurité techniques, opérationnels et de gestion différents, notamment les suivants :

- **Contrôle d'accès (AC pour *Access Control*) :** AC-20 Utilisation de systèmes d'information externes;
- **Vérification et responsabilité (AU pour *Audit and Accountability*) :** AU-1 Politique et procédures de vérification et de responsabilité;
- **Gestion des configurations (CM pour *Configuration Management*) :** CM-8 Inventaire des composants de système d'information;
- **Planification d'urgence (CP pour *Contingency Planning*) :** CP-9 Sauvegarde du système d'information;
- **Protection des supports (MP pour *Media Protection*) :** MP-6 Nettoyage des supports et MP-7 Utilisation des supports;
- **Évaluation des risques (RA pour *Risk Assessment*) :** RA-2 Catégorisation de sécurité;
- **Intégrité de l'information et des systèmes (SI pour *System and Information Integrity*) :** SI-12 Traitement et conservation des sorties d'information;
- **Acquisition des systèmes et des services (SA pour *System and Service Acquisition*) :** SA-9 Services de système d'information externes.

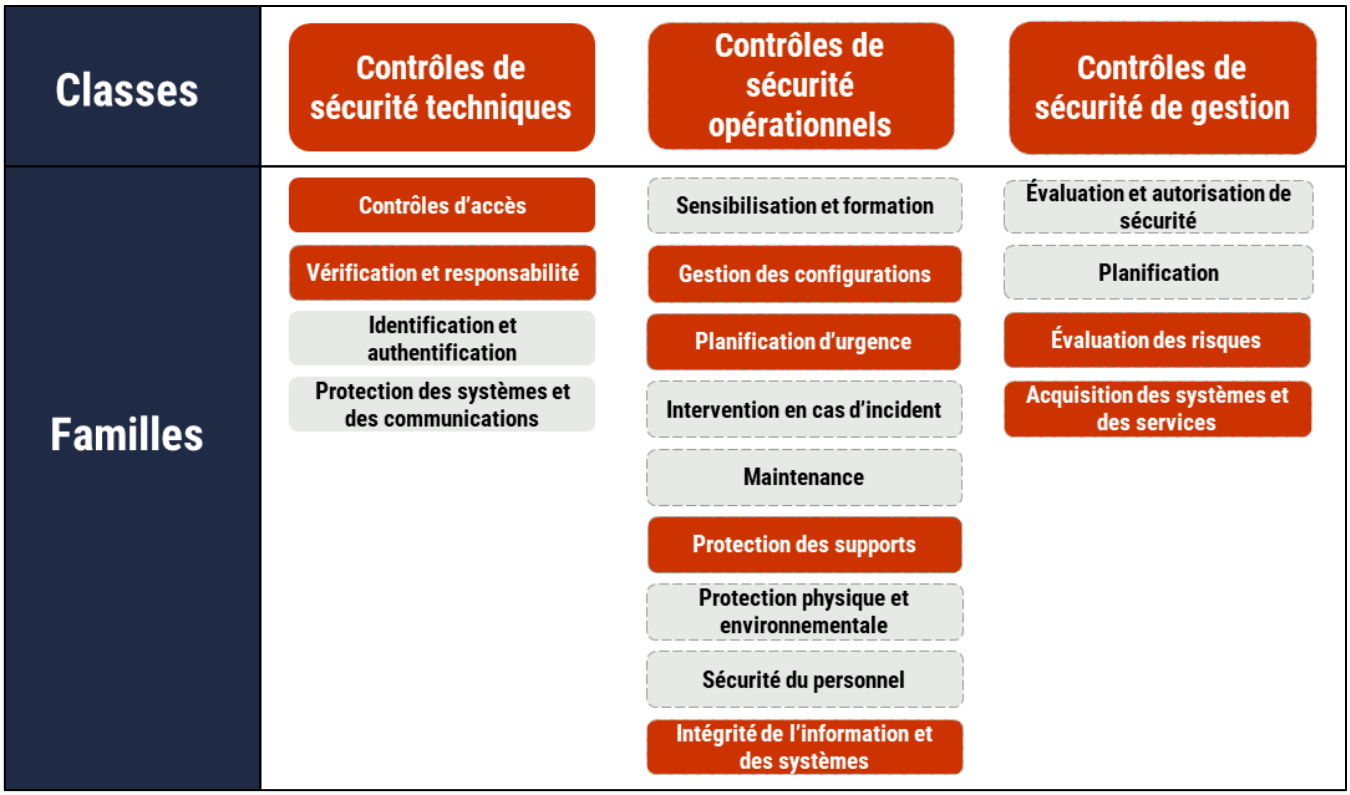

Figure 2 : Classes et familles de contrôles de sécurité applicables décrites dans l'ITSG-33

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 un processus de gestion des risques liés à la sécurité des TI qui est basé sur deux niveaux d'activités de gestion des risques : les activités menées au niveau organisationnel et les activités menées au niveau du système d'information. Ces deux niveaux d'activités vous aideront à déterminer les besoins en matière de sécurité pour l'ensemble de votre organisation et pour ses systèmes d'information. Après avoir compris vos besoins 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 Menaces pesant sur votre information organisationnelle

Votre organisation doit constamment s'adapter aux nouvelles technologies pour être en mesure de protéger ses réseaux, ses systèmes, ses actifs TI, ses données sensibles et l'information contre les cybermenaces émergentes. L'augmentation du nombre de dispositifs mobiles et connectés à Internet, et la demande accrue de régimes de travail à distance et flexibles posent de nouveaux défis associés à la protection de l'information organisationnelle.

Votre organisation peut également dépendre de systèmes et de services qui sont fournis par d'autres organisations. Par exemple, votre organisation peut avoir recours à des services infonuagiques ou à des applications de tierces parties pour stocker des renseignements commerciaux. Moins vous avez de contrôle sur les systèmes et les dispositifs qui traitent, stockent ou transmettent des renseignements commerciaux, moins vous devriez êtes confiant que les renseignements sont protégés. Quels que soient les nouvelles technologies et les nouveaux défis, la protection de la confidentialité, de l'intégrité et de la disponibilité de vos réseaux, de vos systèmes et de vos renseignements relève toujours de votre organisation.

2.1 Menaces courantes

Si un auteur de menace arrive à exploiter et à compromettre le réseau, les systèmes et l'information de votre organisation, celle-ci peut courir de sérieux risques. Il est possible que vous ne puissiez pas mener à bien les activités commerciales, votre organisation pourrait être aux prises avec un vol ou une fuite de données, et vous pourriez subir des pertes financières. Les conséquences d'une atteinte à la protection des données peuvent être importantes : entacher la réputation de votre organisation, nuire aux relations commerciales, et avoir un impact sur la vie privée de vos employés, de vos partenaires et de vos clients. Le tableau 1 présente certains exemples de menaces courantes à l'endroit de l'information de l'entreprise.

Tableau 1 : Exemples de menaces courantes à l'endroit de l'information organisationnelle

Menace	Description	Impact
Maliciel	Logiciel malveillant conçu pour s'infiltrer dans un système informatique et qui peut aussi y causer des dommages. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires. Par exemple, un rançongiciel est un type de maliciel qui empêche un utilisateur légitime d'accéder à un système ou à des données jusqu'à ce qu'il ait payé une rançon.	Lorsqu'un maliciel s'est infiltré dans vos systèmes, un auteur de menace peut l'utiliser pour créer un point d'entrée dans vos systèmes, voler de l'information ou endommager les systèmes. Lors d'une attaque par rançongiciel, un auteur de menace chiffre les données de l'organisation et compromet la disponibilité des données. Les auteurs de menace demandent le paiement d'une rançon avant de déchiffrer l'information; toutefois, même si vous payez, il n'est pas garanti qu'ils déchiffreront l'information.
Virus	Programme informatique qui se propage en se reproduisant à plusieurs reprises. Les virus informatiques se propagent d'un ordinateur à l'autre, souvent à l'insu de l'utilisateur.	Les virus informatiques causent des dommages de toutes sortes. Ils peuvent afficher des messages irritants, voler des données ou même permettre à d'autres utilisateurs de prendre le contrôle de l'ordinateur infecté.

Menace	Description	Impact
Hameçonnage	Tentative visant à solliciter de l'information confidentielle (p. ex. des renseignements personnels ou des numéros de carte de crédit) appartenant à un individu, à un groupe ou à une organisation en les mystifiant ou en imitant une marque commerciale connue.	Un auteur de menace obtient l'accès à des justificatifs d'utilisateur et à des données sensibles (p. ex. la propriété intellectuelle, des renseignements financiers et des renseignements personnels). L'auteur peut vendre cette information ou l'utiliser pour commettre une fraude.
Porte dérobée	Une porte dérobée est un point d'entrée dans un système ou dans un ordinateur qui permet de contourner les mesures d'authentification, le chiffrement ou les systèmes de détection d'intrusion. Les portes dérobées sont souvent créées délibérément aux fins de dépannage, d'application de mises à jour logicielles ou de maintenance des systèmes. Les auteurs de menace peuvent utiliser ces portes dérobées légitimes à des fins malveillantes.	Les auteurs de menace qui disposent d'un tel accès à distance peuvent voler de l'information, installer des maliciels ou contrôler les processus et procédures du dispositif.
Attaque par déni de service (DoS pour *Denial of Service*) Attaque par déni de service distribué (DDoS pour *Distributed Denial of Service*)	Une attaque par DoS vise à perturber les activités normales d'un hôte précis (p. ex. un site Web, un serveur ou un réseau) en le noyant de trafic Internet (demandes). L'objectif général est de rendre l'hôte inaccessible aux demandes d'accès légitimes des utilisateurs et de rendre le système ciblé inopérant. Une attaque par DDoS inonde de trafic des sites Web à partir de sources multiples (p. ex. un réseau de zombies). Une attaque par DDoS est plus difficile à arrêter. Il est aussi difficile de faire la distinction entre le trafic généré par les utilisateurs légitimes et le trafic malveillant.	L'hôte est inaccessible aux demandes d'accès légitimes des utilisateurs et le système ciblé devient inopérant. Par exemple, le site Web de votre organisation devient inutilisable jusqu'à ce que vous puissiez arrêter l'attaque.
Attaque de l'intercepteur (PITM pour *Person-in-the-Middle*)	Une tentative visant à intercepter les communications entre deux parties (p. ex. un utilisateur et un serveur Web) à l'insu de la victime. L'utilisateur croit avoir établi une connexion directe et sécurisée avec un site Web. Les attaques PITM peuvent faire appel à différentes techniques (p. ex. hameçonnage, écoute électronique par réseau Wi-Fi).	Les attaques de l'intercepteur permettent aux auteurs de menace de surveiller les communications, de réacheminer le trafic, de modifier l'information, d'installer des maliciels et d'obtenir des renseignements personnels ou de l'information sensible.
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 utilise un nombre exhaustif de mots de passe générés aléatoirement pour deviner le bon mot de passe. Dans le cadre des attaques par dictionnaire, un auteur de menace utilise une liste de mots de passe souvent utilisés pour deviner le mot de passe.	Si un auteur de menace réussit à trouver le mot de passe d'un compte, il obtient l'accès à de l'information sensible. Un auteur de menace peut avoir un accès potentiel à d'autres comptes si la victime a utilisé le même mot de passe pour plusieurs comptes.
Catastrophes naturelles et incendies	Des catastrophes naturelles, comme des tremblements de terre et des inondations, ainsi que des incendies peuvent également nuire aux systèmes et à l'information de votre organisation.	La disponibilité de l'information et des services de votre organisation est mise en péril si les systèmes et l'information sont endommagés ou détruits. Si vous n'avez pas

Menace	Description	Impact
		de sauvegardes stockées dans un endroit différent, votre organisation pourrait alors encourir des pertes financières ou un risque juridique.

2.2 Menaces internes

Par « menace interne », on entend toute personne qui connaît l'infrastructure et l'information de votre organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à l'organisation. Les menaces internes peuvent poser des risques à vos employés, à vos clients, à vos actifs, à votre réputation et à vos intérêts.

En règle générale, lorsque nous parlons d'une menace interne, nous pensons à quelqu'un qui veut mal faire. En effet, un individu peut lancer des attaques ciblées en utilisant à mauvais escient des accès privilégiés ou des comptes généraux pour installer un maliciel ou voler de l'information sensible.

Toutefois, quiconque a accès à l'infrastructure ou à l'information de votre organisation (p. ex. les employés, les entrepreneurs ou les fournisseurs de services) peut causer des dommages involontairement. Par exemple, les comportements suivants peuvent causer des menaces internes involontaires :

- perdre un dispositif mobile ou un support amovible;
- accorder un accès d'utilisateur à l'information sensible allant au-delà des exigences requises pour l'exercice des fonctions d'un employé;
- gérer de façon inadéquate de l'information sensible (p. ex. la stocker incorrectement, ne pas appliquer des marquages de protection ou des mises en garde de distribution).

Une menace interne peut toucher la confidentialité, l'intégrité et la disponibilité des systèmes et de l'information de votre organisation. Par exemple, une menace interne peut entraîner une divulgation non intentionnelle d'information sensible ou un vol intentionnel de la propriété intellectuelle, la perturbation des services de l'organisation ou la destruction d'information essentielle.

Pour obtenir de plus amples renseignements, consultez l'ITSAP.10.003, Comment protéger votre organisation contre les menaces internes [4].

2.3 Menaces pour la chaîne d'approvisionnement

Vous devez vous assurer de gérer les risques associés à votre chaîne d'approvisionnement dans le cadre des activités liées à votre plan de cybersécurité et de gestion des risques. Votre chaîne d'approvisionnement comprend tout fournisseur, service, équipement, logiciel ou processus qu'utilise votre organisation.

Même si votre organisation dispose d'un programme de cybersécurité rigoureux, les systèmes et l'information de l'organisation demeurent à risque si votre chaîne d'approvisionnement est compromise. Les auteurs de menace peuvent tenter de compromettre la chaîne d'approvisionnement en infiltrant des fournisseurs et des vendeurs de confiance, violant ainsi la confiance présumée qui vous lie à vos fournisseurs et à vos vendeurs.

Pour obtenir de plus amples renseignements sur la protection de votre chaîne d'approvisionnement, consultez l'ITSAP.00.070, Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations [5].

3 Évaluation de l'information organisationnelle

Les conseils énoncés dans cette section sont fondés sur le contrôle **RA-2 Catégorisation de sécurité**.

Sans compréhension exhaustive de l'information que traite et conserve votre organisation, vous ne pouvez pas la protéger complètement. Dans le cadre de vos activités liées à la gestion des risques et à la cybersécurité, vous devez examiner l'information de votre organisation pour en établir la valeur, la classer en fonction de son niveau de sensibilité et la catégoriser.

3.1 Établissement de la valeur (RA-2)

En établissant la valeur de l'information de votre organisation, vous pouvez classer par ordre de priorité ce qui nécessite d'être protégé.

Vous pouvez déterminer la valeur de l'information organisationnelle en évaluant les préjudices possibles pouvant résulter d'une inaptitude à protéger sa confidentialité, son intégrité et sa disponibilité. Lorsque vous déterminez la valeur de l'information, tenez compte des types d'information suivants :

- **Information essentielle aux activités :** Information sur laquelle compte votre organisation pour ses activités courantes (p. ex. information sur les ventes, plans d'intervention en cas d'urgence);
- **Information sensible :** Information devant rester confidentielle ou à laquelle seules certaines personnes peuvent accéder (p. ex. données personnelles ou financières, propriété intellectuelle);
- **Documents et preuves :** Information devant être protégée contre toute modification non autorisée (p. ex. contrats ou reçus).

Pour obtenir de plus amples renseignements sur la façon de déterminer la valeur des actifs et des systèmes d'information, consultez l'ITSAP.40.001, Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations [6] et la section 2.3 des Contrôles de cybersécurité de base pour les petites et moyennes organisations [3].

3.2 Classification et catégorisation (RA-2)

Parallèlement à l'établissement de la valeur de l'information organisationnelle, vous devriez également la classer par groupes ou classes en fonction de son niveau de sensibilité. Les marquages de classification qu'applique votre organisation peuvent varier selon que vous faites partie d'un ministère ou d'une organisation non gouvernementale ou privée. La classification appropriée de l'information vous permet de mieux gérer l'information et de la protéger contre tout accès non autorisé ou toute distribution non autorisée, ainsi que contre la conservation et l'élimination inappropriées.

La catégorisation de l'information organisationnelle répond à plusieurs objectifs, comme le démontrent les exemples suivants :

- il reflète la valeur que votre organisation a attribuée à l'information;
- il représente la tolérance au risque de l'organisation;
- il détermine comment votre organisation assure la confidentialité, l'intégrité et la disponibilité de l'information.

Lorsque l’information organisationnelle est correctement classifiée et catégorisée, votre organisation est mieux placée pour la gérer tout au long de son cycle de vie, la conserver et l’éliminer de façon appropriée, ainsi que la protéger contre tout accès et toute distribution non autorisés. De plus, en ayant une bonne connaissance de votre information, vous pouvez mettre en œuvre les contrôles de sécurité appropriés et gérer les risques en fonction de la tolérance au risque définie par votre organisation.

4 Gestion de l'information

Les conseils énoncés dans cette section sont fondés sur les contrôles de sécurité suivants : **SI-12 Traitement et conservation des sorties d'information**, **MP-6 Nettoyage des supports**, **CM-8 Inventaire des composants de système d'information** et **CP-9 Sauvegarde du système d'information**. Ces contrôles de sécurité ne sont que quelques exemples des mesures que votre organisation peut mettre en place pour gérer son information.

En fait, pour protéger l'information de votre organisation, vous devez vous assurer que cette information est adéquatement gérée tout au long de son cycle de vie. Dès la création ou la réception de l'information, celle-ci doit être traitée conformément aux politiques de l'organisation et selon son niveau de sensibilité.

La sensibilisation au traitement adéquat de l'information est une étape essentielle de la protection de l'information organisationnelle, car quiconque a accès à l'infrastructure ou à l'information de votre organisation (p. ex. les employés, les entrepreneurs ou les fournisseurs de services) peut causer des dommages involontairement. Par exemple, des fuites ou des atteintes à la protection des données involontaires peuvent être causées par les comportements suivants :

- perdre un dispositif mobile ou un support amovible;
- accorder un accès d'utilisateur à l'information sensible allant au-delà des exigences requises pour l'exercice des fonctions d'un employé;
- conserver l'information de façon inadéquate (p. ex. l'information sensible n'est pas chiffrée);
- appliquer des marquages ou des mises en garde incorrectes à l'information (ou ne pas les appliquer).

4.1 Conservation et élimination (SI-12 et MP-6)

Vous devez vous assurer que l'information, les documents et les supports sont conservés aussi longtemps qu'ils sont nécessaires à des fins professionnelles pour répondre aux exigences réglementaires et juridiques. L'information a différentes exigences en matière de conservation selon l'usage qui en est fait. Par exemple, d'un point de vue législatif et réglementaire, vous devez conserver les renseignements financiers plus longtemps que les renseignements d'ordre administratif, comme les notes de comités ou de réunions. Votre organisation a la responsabilité de créer et de tenir un calendrier de conservation qui décrit la durée de conservation de l'information et les mesures à prendre pour l'éliminer entièrement (p. ex. la détruire ou la conserver).

Lorsque l'information atteint la fin de son cycle de vie, vous devez vous assurer qu'elle est éliminée adéquatement (p. ex. déchiquetage, incinération, démagnétisation) pour empêcher la rémanence et les atteintes à la protection des données. Si l'information ou les supports ne sont pas correctement détruits, il pourrait rester des données résiduelles ou des données pourraient être récupérées et reconstituées.

Remarque : Si vous réutilisez un support physique ou électronique, ou si celui-ci n'est plus sous le contrôle de votre organisation, vous devez vous assurer qu'il a été bien nettoyé. Dans certains cas, il pourrait s'avérer judicieux de nettoyer le support, comme un disque dur, avant de le détruire. Une telle intervention assure une meilleure protection.

Si votre organisation utilise des fournisseurs de services infonuagiques (FSI), vous devriez prendre connaissance de certains défis liés à la destruction adéquate de l'information. Vous avez moins de contrôle en ce qui a trait à garantir que l'information est correctement retirée des actifs physiques. Vous devez inclure les détails relatifs à la conservation et à l'élimination de l'information dans votre accord sur les niveaux de service avec un fournisseur de services. Un aspect de l'élimination des données à prendre en compte dans le nuage est le cryptodéchiquetage.

Grâce à cette méthode d'élimination des données, la clé de chiffrement affectée à la protection des données est intentionnellement supprimée ou écrasée. Cette méthode ne peut s'appliquer qu'aux données qui ont été chiffrées. Votre organisation devrait chiffrer ses données sensibles et exclusives lorsqu'elles sont au repos, en transit et utilisées, pour ainsi assurer la protection de la confidentialité, de l'intégrité et de la disponibilité de vos données.

4.2 Inventaire et suivi (CM-8)

Votre organisation devrait disposer d'un inventaire de tous les systèmes d'information et de leurs composants (p. ex. le matériel, les logiciels, les bases de données, les réseaux et les personnes). Vous avez la responsabilité de déterminer les critères concernant les types de composants de système d'information (p. ex. les microprocesseurs, les cartes mères, les logiciels, les contrôleurs programmables et les dispositifs réseau) qui font partie de l'inventaire.

Les renseignements concernant les composants doivent être suffisamment détaillés pour répondre aux exigences de votre organisation en matière de suivi et de production de rapports. Pour chaque composant, vous devriez dresser une liste des renseignements concernant sa configuration, y compris toutes les déviations approuvées, ainsi que toutes les personnes, avec leurs coordonnées, qui sont responsables de ce composant. Assurez-vous d'inclure des renseignements propres au système (p. ex. association de systèmes, propriétaire du système, licence de logiciel, versions logicielles) et des spécifications d'inventaire matériel (p. ex. fabricant, type de dispositif, modèle, numéro de série et emplacement physique). Pour ce qui est des composants ou des dispositifs en réseau, vous devriez également inclure les noms des machines et les adresses réseau.

Assurez-vous de passer cet inventaire en revue. Vous devriez mettre à jour l'inventaire lorsque, par exemple, les systèmes d'information sont mis à jour et lorsque des composants sont installés et retirés. Vous pourriez également utiliser des mécanismes automatisés pour vous permettre de tenir votre inventaire à jour, complet et exact.

Dans le cadre de la tenue d'un inventaire, assurez-vous de passer en revue les configurations cryptographiques de vos logiciels et de votre matériel. Pour permettre une agilité cryptographique, votre inventaire devrait comporter les algorithmes cryptographiques configurés pour chaque composant. L'agilité cryptographique constitue une pratique exemplaire permettant de changer facilement les algorithmes de chiffrement utilisés dans les applications et les protocoles pour maintenir la sécurité des systèmes malgré la découverte de nouvelles vulnérabilités cryptographiques. Cette pratique repose principalement sur la configuration et ne nécessite pas d'importantes mises à jour logicielles ou matérielles. Pour obtenir de plus amples détails, consultez l'ITSAP.40.01, Conseils sur la mise en œuvre de l'agilité cryptographique [7].

4.3 Sauvegarde (CP-9)

Sauvegarder l'information de votre organisation est une autre mesure que vous pouvez prendre pour protéger l'information. Lorsque vous sauvegardez l'information, vous créez un double exemplaire qui est stocké dans un emplacement différent. Votre organisation doit déterminer un emplacement de stockage adéquat en fonction de l'évaluation des risques et du niveau de sensibilité de l'information.

Les sauvegardes protègent la disponibilité de l'information advenant une panne ou la compromission d'un système. Par exemple, si votre organisation est victime d'une attaque par rançongiciel, vous détenez une copie de l'information qui a été chiffrée par l'auteur de menace. Si les données sont perdues, vous pouvez avoir recours aux sauvegardes pour récupérer les données et poursuivre vos activités commerciales.

5 Gestion des dispositifs mobiles

La présente section est basée sur les contrôles de sécurité **MP-7 Utilisation des supports** et **SA-9 Services de système d'information externes**. Elle décrit certaines des mesures que votre organisation peut prendre pour gérer ses dispositifs mobiles; toutefois, votre organisation devrait déterminer si des contrôles additionnels sont requis.

Les dispositifs mobiles jouent un rôle essentiel dans les activités commerciales quotidiennes, mais ils peuvent accroître le niveau de risque pour l'organisation et son information. Les dispositifs mobiles peuvent contenir beaucoup de renseignements sensibles et personnels, ce qui en fait des cibles attrayantes pour les auteurs de menace qui tentent de recueillir des renseignements.

En tirant parti d'un dispositif compromis, les auteurs de menace peuvent accéder aux réseaux, aux systèmes et à l'information de votre organisation. Ces auteurs utilisent différentes méthodes pour recueillir l'information, y compris :

- l'accès distant à des dispositifs et leur contrôle à distance;
- le trafiquage physique de dispositifs;
- l'utilisation de fonctions de suivi de l'emplacement sur les dispositifs;
- l'envoi de courriels et de messages textes contenant des pièces jointes et des liens malveillants.

Pour obtenir de plus amples renseignements sur l'utilisation des dispositifs mobiles en toute sécurité, consultez l'ITSAP.00.001, Utiliser son dispositif mobile en toute sécurité [8] et l'ITSM.80.001, Sécurisation de l'entreprise et des technologies mobiles [9].

5.1 Modèles organisationnels de déploiement de dispositifs mobiles (MP-7 et SA-9)

Les dispositifs mobiles sont essentiels pour la majorité des organisations, mais votre organisation doit convenir d'un modèle de propriété pour ces dispositifs.

Votre organisation devrait envisager l'utilisation de l'un des quatre modèles organisationnels de déploiement de dispositifs mobiles existants. Optez pour un modèle qui répond le mieux à vos objectifs commerciaux, à vos exigences en matière de sécurité et à votre cadre de gestion des risques. Voici les quatre modèles de déploiement :

- dispositifs réservés au travail et appartenant à l'organisation (COBO pour *Corporately owned and for business only*);
- dispositifs pouvant servir à des fins personnelles et appartenant à l'organisation (COPE pour *Corporately owned and personally enabled*);
- dispositifs au choix (CYOD pour *Choose your own device*);
- dispositifs personnels (BYOD pour *Bring your own device*).

Vous devez définir clairement le modèle de déploiement de dispositifs mobiles que votre organisation a mis en place, en vous assurant qu'il est conforme aux exigences en matière de politique et que les employés comprennent les implications du modèle. Au moment de choisir un modèle, veillez à tenir compte des aspects suivants :

- Quels types de dispositifs sont compris dans ce modèle (p. ex. fournisseur, téléphones intelligents, tablettes, ordinateurs portables et autres dispositifs de l'IdO)?
- Qui est chargé de payer le dispositif?
- Qui gère les dispositifs et qui est responsable du soutien connexe?
- Quelles applications sont autorisées à être exécutées sur les dispositifs?
- Quel est le niveau d'intégration du dispositif au réseau organisationnel?

Bien que l'intégration de dispositifs mobiles en milieu de travail comporte des avantages, vous devez trouver un équilibre entre cette intégration et la capacité à réduire les risques associés aux dispositifs non gérés qui se connectent à votre réseau.

Au moment de déployer des dispositifs mobiles dans votre organisation, vous devriez tenir compte des risques et des avantages liés aux différents modèles de déploiement. Dans certains cas, il peut s'avérer pratique de fournir l'équipement (p. ex. des serveurs, des postes de travail, des ordinateurs portables et des dispositifs mobiles) aux employés, à condition de s'être doté d'un cadre de gestion des dispositifs et d'avoir instauré un processus de gestion des changements de configuration. Si votre organisation décide d'autoriser les employés à utiliser leurs propres dispositifs mobiles à des fins professionnelles, il conviendra de mettre en place une stratégie de contrôle rigoureuse et de passer en revue les technologies et les exigences juridiques en matière de séparation des renseignements personnels et organisationnels. Votre organisme peut utiliser la gestion unifiée des terminaux (UEM pour *Unified Endpoint Management*) pour assurer la sécurité des dispositifs mobiles. L'UEM combine les fonctionnalités de la gestion des dispositifs mobiles et des processus organisationnels de gestion du déploiement de dispositifs mobiles.

5.1.1 Modèle COBO

Dans un modèle COBO, les dispositifs mobiles sont fournis par l'organisation et lui appartiennent. Ce modèle interdit l'utilisation de dispositifs personnels dans le cadre des activités professionnelles, et il interdit un usage personnel des dispositifs de l'organisation. Dans certains cas, il peut s'avérer pratique de fournir aux employés l'équipement dont ils ont besoin pour accomplir leurs tâches (p. ex. des serveurs, des postes de travail, des ordinateurs portables et des dispositifs mobiles), car cela permet à votre organisation de contrôler plus étroitement les mécanismes de sécurité mis en place sur les dispositifs. Vous pouvez également installer un logiciel antivirus et d'autres mesures de protection pour protéger les dispositifs.

5.1.2 Modèle COPE

Dans un modèle COPE, votre organisation fournit aux employés des dispositifs, mais vous permettez aussi aux employés de les utiliser comme dispositifs personnels. L'équipement et les dispositifs COPE vous permettent de mieux contrôler les mécanismes de sécurité mis en place. De plus, lorsqu'un employé quitte votre organisation, vous conservez l'équipement et les dispositifs.

Vous devez vous assurer que l'information sensible et votre infrastructure TI organisationnelle sont adéquatement protégées. Il est recommandé que les données professionnelles et personnelles, y compris les applications, les comptes de courriel et les contacts, soient séparées sur ces dispositifs. Différentes solutions sont offertes pour séparer les données personnelles des données professionnelles. Certains exemples de solutions comprennent l'utilisation d'applications distinctes pour le travail ou l'utilisation de fonctions de verrouillage ou de dossiers sécurisés pour les renseignements commerciaux. Vous devez vous assurer que toutes les données sensibles sont chiffrées et stockées de manière sécurisée.

Votre organisation doit prendre des mesures supplémentaires pour protéger les dispositifs mobiles, car ils risquent davantage d'être exploités par des auteurs de menace que les dispositifs appartenant à l'organisation (p. ex. les ordinateurs de bureau et les ordinateurs portables) qui ne sont utilisés qu'en milieu de travail et qui fonctionnent sur les réseaux de l'organisation.

5.1.3 Modèle CYOD

Dans un modèle CYOD, vous permettez à vos employés de choisir des dispositifs figurant sur une liste de dispositifs que votre organisation a approuvés pour un usage professionnel. Votre organisation choisit les dispositifs et elle continue à les gérer, ce qui signifie que vous avez un meilleur contrôle sur les mesures de sécurité mises en œuvre, les applications exécutées sur les dispositifs et les fonctions auxquelles ont accès les utilisateurs.

5.1.4 Modèle BYOD

De nombreuses raisons expliquent pourquoi votre organisation pourrait permettre aux employés d'utiliser les dispositifs personnels pour le travail. Lorsque le modèle PAP est en place, l'organisation peut économiser de l'argent qui autrement aurait été dépensé pour l'achat de dispositifs mobiles pour tous les employés et pour l'utilisation d'une technologie moderne avec laquelle les employés sont à l'aise.

Toutefois, votre organisation doit tenir compte des risques connexes liés à la sécurité avant d'informer les employés qu'ils peuvent utiliser leurs dispositifs personnels. Bien que cette section ne couvre pas tous les risques connexes, vous devriez envisager ce qui suit :

- Comment allez-vous gérer et prendre en charge différents dispositifs?
- Comment allez-vous limiter l'accès ou le partage de l'information effectué au moyen des dispositifs personnels?
- Quels contrôles techniques (p. ex. applications conteneurisées, gestion des dispositifs mobiles) allez-vous mettre en œuvre?
- Quelles sont vos responsabilités légales en ce qui concerne la protection des renseignements personnels?
- Comment allez-vous régler les incidents de sécurité si un téléphone personnel est perdu ou volé?
- Comment allez-vous vous assurer que l'information contenue dans les dispositifs personnels est sauvegardée ou nettoyée lorsqu'un employé quitte l'organisation?

Il est recommandé d'effectuer une évaluation des menaces et des risques (EMR) avant de mettre en œuvre un modèle BYOD. Étant donné que l'utilisation de dispositifs personnels peut avoir une incidence sur la vie privée, vous devriez évaluer les risques relatifs à la vie privée qui pourraient survenir.

Il vous faudrait également créer une politique visant à informer les utilisateurs de l'utilisation acceptable qui doit être faite d'un dispositif personnel et des comportements auxquels on s'attend de leur part. Les politiques doivent être communiquées au personnel au moyen de programmes de formation afin de vous assurer que chacun comprend ses rôles et ses responsabilités.

Pour de plus amples renseignements sur ce modèle de déploiement, prière de consulter l'ITSM.70.003, Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels *(PAP)* [10].

5.2 Dispositifs mobiles et déplacements

Vous devez tenir compte de certains risques si vos employés se déplacent avec des dispositifs professionnels. En effet, les auteurs de menace sont plus susceptibles de cibler des personnes qui occupent des postes supérieurs ou de direction. N'oubliez pas que, dans certains pays, les centres d'affaires et les réseaux téléphoniques des hôtels peuvent être surveillés, et les chambres sont parfois fouillées. Lors d'un voyage, il faut donc supposer que les bureaux, les hôtels, les cafés Internet et les autres lieux publics ne sont pas privés.

Au moment de déterminer les endroits qui posent problème, il faut définir les configurations nécessaires pour les dispositifs, s'assurer que les dispositifs sont configurés selon l'usage prévu avant le déplacement et appliquer des mesures de protection au dispositif au retour du déplacement.

Avant le déplacement, vous devez déterminer si la destination ou la nature de l'événement pourrait susciter une préoccupation et vous assurer que les dispositifs sont configurés adéquatement. Il serait de mise d'aviser les employés de prendre des mesures de précaution en désactivant des fonctionnalités comme la technologie Bluetooth et le casque d'écoute, et en faisant une sauvegarde des données sur les dispositifs qu'ils transportent avec eux. Il faut prévenir les employés de ne pas utiliser de réseaux Wi-Fi inconnus, non sécurisés ou publics.

Lorsque les employés reviennent d'un voyage d'affaires, les services TI doivent analyser tous les dispositifs avant qu'ils ne soient connectés aux systèmes ou aux réseaux de l'organisation. Vous devez appliquer des mesures de protection particulières aux dispositifs à la fin du voyage. Par exemple, il convient d'examiner les dispositifs afin de détecter tout signe de trafiquage physique, ainsi que de nettoyer ou de recréer l'image du lecteur de disque dur.
Il peut y avoir des scénarios dans lesquels il serait approprié d'utiliser des dispositifs réservés aux déplacements ou « jetables ». Parfois, la mise hors service d'un dispositif peut s'avérer préférable que de l'autoriser à se reconnecter à votre réseau.

6 Sécurisation des systèmes d'information externes

Les conseils énoncés dans cette section sont fondés sur les contrôles **AC-20 Utilisation de systèmes d'information externes** et **SA-9 Services de système d'information externes**. Pour en savoir plus sur ces contrôles, consultez l'annexe A.1 de ce document. Cette section décrit certaines des mesures que vous pouvez prendre pour protéger votre organisation contre les cybermenaces et les compromissions lorsque des systèmes d'information externes sont utilisés.

Votre organisation peut se servir de systèmes et de services qui sont fournis par d'autres organisations. Par exemple, votre organisation peut faire appel à des services infonuagiques pour stocker l'information organisationnelle, ou vos employés peuvent utiliser leurs dispositifs personnels dans le cadre des activités professionnelles. Dans le présent document, nous désignons les systèmes fournis par d'autres organisations comme étant des *systèmes d'information externes*.

Votre organisation pourrait être aux prises avec des situations où les employés ou d'autres personnes autorisées (comme des entrepreneurs) doivent accéder aux systèmes de l'organisation en passant par des systèmes externes. Les systèmes d'information externes peuvent comprendre des dispositifs personnels (p. ex. des tablettes et d'autres dispositifs mobiles), des systèmes et des dispositifs de propriété privée qui se trouvent dans des établissements commerciaux ou publics (p. ex. des hôtels, des centres de congrès, des aéroports) ou des systèmes appartenant et contrôlés par d'autres organisations (p. ex. des services infonuagiques). Nous recommandons d'interdire l'utilisation de dispositifs de stockage accessibles par réseau sur des systèmes d'information externes.

6.1 Identification des risques connexes (AC-20 et SA-9)

Les systèmes d'information externes, comme les applications Internet et infonuagiques, peuvent s'avérer économiques et efficaces. Toutefois, votre organisation n'assure habituellement pas la supervision directe des contrôles de sécurité mis en œuvre sur des systèmes externes ou n'a aucune autorité sur ces contrôles. À titre d'exemple, votre organisation est vulnérable aux cyberattaques si les employés utilisent leurs dispositifs personnels pour le travail et que ces dispositifs sont dotés de logiciels désuets ou non corrigés, ou d'applications utilisées par les employés sans que ceux-ci aient reçu les permissions appropriées préalables pour les utiliser. Un autre exemple est lorsque les employés de votre organisation utilisent des plateformes sur Internet pour partager des fichiers ou participer à des appels vidéo, car ces plateformes ne sont pas contrôlées par l'architecture ou l'infrastructure de sécurité des TI de votre organisation. Moins vous avez de contrôle sur les systèmes et les dispositifs qui traitent, stockent ou transmettent de l'information organisationnelle, moins vous devriez êtes confiant que votre information est protégée. Il est recommandé que votre organisation effectue une évaluation des risques et une évaluation de la chaîne d'approvisionnement avant de sanctionner l'utilisation de dispositifs personnels, d'applications ou de systèmes Internet et infonuagiques pour les employés. Pour obtenir de plus amples renseignements sur l'évaluation des risques et l'évaluation des risques liés à la chaîne d'approvisionnement, consultez l'ITSG-33 [2] et l'ITSAP.10.070, La cybersécurité et la chaîne d'approvisionnement : Évaluation des risques [11].

Avant de passer un contrat avec un fournisseur de services potentiel, comme un FSI, vous devez établir les données qui seront accessibles au fournisseur de services et le niveau de sensibilité de ces données. En comprenant vos données et leur niveau de sensibilité, vous pourrez déterminer les contrôles de sécurité requis pour les protéger adéquatement.

La sensibilité des données se mesure par l'incidence que peut avoir une compromission sur la capacité de votre organisation à réaliser son mandat. Il existe trois niveaux de sensibilité des données :

- **Élevé (E)** : La compromission a une incidence cruciale ou prohibitive sur la capacité de votre organisation à s'acquitter de son mandat;
- **Moyen (M)** : La compromission a une incidence majeure sur la capacité de votre organisation à s'acquitter de son mandat;
- **Faible (F)** : La compromission a une incidence modérée sur la capacité de votre organisation à s'acquitter de son mandat.

Votre organisation a toujours la responsabilité de protéger la confidentialité, l'intégrité et la disponibilité de vos réseaux, de vos systèmes et de votre information. Pour protéger vos systèmes en cas de compromission, de dommage ou de préjudice, vous ne devriez autoriser l'utilisation d'un système externe que si vous vous êtes assuré que ce système est doté de contrôles de sécurité qui sont en conformité avec vos plans et politiques de sécurité. Afin de vérifier les contrôles, vous pourriez, par exemple, faire appel à un tiers ou utiliser des évaluations ou attestations indépendantes. Choisissez une méthode qui répond au niveau de confiance requis par votre organisation.

Votre organisation peut déterminer qu'il existe un niveau de risque plus élevé si l'utilisation de ces dispositifs est interdite; nous recommandons donc de limiter l'utilisation de ces dispositifs de la manière suivante :

- veiller à ce que des contrôles de sécurité approuvés soient appliqués sur les dispositifs avant qu'il soit possible de les connecter aux systèmes de l'organisation;
- restreindre l'accès des dispositifs à certains types d'informations, de services ou d'applications;
- utiliser des techniques de virtualisation pour limiter les activités de traitement et de stockage des serveurs ou d'autres composants des systèmes de l'organisation;
- s'assurer que les utilisateurs consentent aux conditions de l'organisation.

Au moment de conclure une entente avec un FSI ou un fournisseur de services gérés (FSG), la question du stockage des données doit faire l'objet de discussions, et les termes de l'accord doivent être convenus. Lorsque les données sont stockées à l'extérieur de l'infrastructure de votre organisation, vous devez savoir exactement où ces données seront stockées, par exemple, l'emplacement géographique du centre de données du FSI ou du FSG. L'emplacement de vos données est important, car les données stockées à l'extérieur du Canada sont assujetties à des lois et à des règlements différents en matière de protection des renseignements personnels, de sécurité et de propriété des données. Selon le domaine ou le secteur auquel appartient votre organisation, les données pourraient également être assujetties à des normes et à des règlements différents qui régissent la conservation, la divulgation à des tiers et la chaîne de possession. Assurez-vous de documenter les termes de la résidence des données dans votre accord sur les niveaux de service (ANS) avec le FSI ou le FSG.

6.2 Documentation des accords (AC-20 et SA-9)

Lorsque des systèmes d'information appartiennent à une autre organisation ou à un fournisseur de services et qu'ils sont exploités ou maintenus par ceux-ci, vous devez documenter tous les accords avec les tiers. Par exemple, vous devriez vous assurer d'avoir un accord sur les niveaux de service avec les FSI. Ces accords décrivent le niveau de service auquel vous vous attendez du FSI. Ils définissent également les attentes à l'égard du rendement des

contrôles de sécurité, les résultats mesurables ainsi que les exigences en matière de solution et d'intervention pour les situations de non-respect ou les incidents de sécurité. Les ANS doivent refléter les politiques et les procédures de sécurité de l'organisation. Il vous faut également revoir tous les accords régulièrement.

Votre organisation et le fournisseur de services ont tous deux un rôle à jouer dans la protection des systèmes et des données. À titre de propriétaire des données, votre organisation est légalement responsable de leur sécurité.
Par conséquent, il est crucial que vous définissiez explicitement les exigences de votre organisation en matière de sécurité et que vous posiez les bonnes questions à un FSI ou à un FSG avant de vous inscrire à un service.
Cette information vous permettra de définir une entente de niveau de service efficace avec des fournisseurs de services tiers.

7 Surveillance de la conformité

Il est recommandé de mettre en place un programme de conformité pour appliquer les politiques de sécurité de l'organisation et assurer que la réglementation externe est suivie. À titre d'exemple, en mettant en place un cadre adéquat de surveillance de la conformité, votre organisation peut démontrer qu'elle est capable de traiter correctement l'information de nature délicate, comme les renseignements personnels.

Vous pouvez également utiliser votre programme de surveillance de la conformité pour identifier et analyser les risques, de même que pour évaluer l'efficacité de vos contrôles de sécurité. Le cadre de surveillance de la conformité peut servir d'outil de référence pour atténuer adéquatement les risques.

7.1 Surveillance continue (AU-1)

Vous devez vous assurer que tous les terminaux sont surveillés en permanence. Grâce à la surveillance des dispositifs, vous pouvez détecter et suivre tout comportement inhabituel ou toute compromission suspecte.

Les systèmes d'information de votre organisation doivent comporter des journaux d'audit pour s'assurer que les événements (p. ex. les mises à jour, les changements, les tentatives d'authentification) sont enregistrés aux fins d'examen. Vous devez veiller à ce que les journaux ne soient accessibles qu'aux personnes autorisées. N'oubliez pas que si vous avez externalisé certains services, il peut alors être plus difficile d'obtenir les journaux.

Nous recommandons également d'utiliser des mécanismes automatisés, comme le balayage périodique, pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information. Si des composants non autorisés sont détectés, vous devriez désactiver leur accès au réseau et isoler ces composants (p. ex. dans un bac à sable).

8 Sommaire

Parmi les 10 mesures de sécurité des TI recommandées par le CST, l'une consiste à protéger l'information au niveau de l'organisme. Les conseils formulés dans le présent document sont basés sur plusieurs des contrôles de sécurité détaillés à l'annexe 3A de l'ITSG-33 [2]. Le présent document n'est pas exhaustif. Dans le but de protéger le mieux possible l'information organisationnelle, vous devriez également passer en revue les 10 autres mesures de sécurité des TI recommandées par le CST. Vous pouvez consulter nos autres publications, telles que l'ITSM.10.093, Les 10 mesures de sécurité des TI : Miser sur une formation sur mesure en matière de cybersécurité [12] ou l'ITSM.10.094, Les 10 mesures de sécurité des TI : Gestion et contrôle des privilèges d'administrateur [13].

Les actifs TI et l'information de votre organisation sont importants et permettent à votre organisation de poursuivre ses activités. Ces actifs représentent également une cible précieuse pour les auteurs de menace. Votre organisation a toujours la responsabilité de protéger la confidentialité, l'intégrité et la disponibilité de vos réseaux, de vos systèmes et de votre information. Vous devriez mettre en œuvre des contrôles de sécurité qui répondent aux exigences opérationnelles et de sécurité de votre organisation.

8.1 Coordonnées

Pour de plus amples renseignements sur la mise en œuvre des conseils formulés dans ce document ou sur une autre des 10 mesures de sécurité des TI, veuillez communiquer par téléphone ou par courriel avec le :

Centre d'appel

contact@cyber.gc.ca

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

9 Contenu complémentaire

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

Abréviation, acronyme ou sigle	Expression au long
AC	Contrôle d'accès (*Access control*) (code de la famille de contrôles de sécurité)
AU	Vérification et responsabilité (*Audit and accountability*) (code de la famille de contrôles de sécurité)
BYOD	Déploiement de dispositifs personnels (*Bring your own device*)
CM	Gestion des configurations (*Configuration management*) (code de la famille de contrôles de sécurité)
COBO	Déploiement de dispositifs réservés au travail et appartenant à l'organisation (*Corporately owned and for business only*)
COPE	Déploiement de dispositifs pouvant servir à des fins personnelles et appartenant à l'organisation (*Corporately owned and personally enabled*)
CP	Planification d'urgence (*Contingency planning*) (code de la famille de contrôles de sécurité)
FSI	Fournisseur de services infonuagiques
CYOD	Déploiement de dispositifs au choix (*Choose your own device*)
TI	Technologies de l'information
MP	Protection des supports (*Media protection*) (code de la famille de contrôles de sécurité)
FSG	Fournisseur de services gérés
RA	Évaluation des risques (*Risk assessment*) (code de la famille de contrôles de sécurité)
SA	Acquisition des systèmes et des services (*System and Services Acquisition*) (code de la famille de contrôles de sécurité)
SI	Intégrité de l'information et des systèmes (*System and Information Integrity*) (code de la famille de contrôles de sécurité)
ANS	Accord sur les niveaux de service
EMR	Évaluation des menaces et des risques

9.2 Glossaire

Terme	Définition
Disponibilité	Valeur qui est accordée aux actifs d'information, aux logiciels et au matériel (l'infrastructure et ses composantes). Les données ayant la cote de disponibilité la plus élevée doivent être accessibles en permanence. Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Porte dérobée	Utilisation de méthodes clandestines pour contourner les exigences d'authentification et accéder aux logiciels et aux dispositifs.
Confidentialité	Valeur qui est accordée à un ensemble d'information pour indiquer son niveau de sensibilité et les restrictions d'accès mises en place pour empêcher les utilisateurs non autorisés d'y accéder.

Terme	Définition
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à infiltrer un système informatique, un réseau ou un dispositif.
Intégrité	Valeur qui est accordée à l'information pour indiquer dans quelle mesure elle est susceptible à la perte de données. Il est également entendu que l'intégrité comprend l'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.
Système d'information	Ensemble intégré de composants qui permet de recueillir, de stocker et de traiter des données. Le système permet de fournir de l'information, d'apporter des connaissances et d'offrir des produits numériques.
Composant de système d'information	Élément clé constitutif d'un système d'information, lequel est composé de matériel informatique, de logiciels, de bases de données, de réseaux et de personnes.
Menace interne	Toute personne qui connaît l'infrastructure ou l'information d'une organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à cette organisation.
Actif TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
Maliciel	Logiciel malveillant (p. ex. un virus informatique, un ver informatique, un cheval de Troie, un logiciel espion ou un logiciel publicitaire) conçu pour s'infiltrer dans un système informatique et qui peut aussi y causer des dommages.
Contrôle de sécurité de gestion	Classe de contrôles 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	Classe de contrôles de sécurité qui est principalement mise en œuvre et exécutée par des personnes, mais habituellement fondée sur l'utilisation de la technologie, par exemple, un logiciel de soutien.
Rançongiciel	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 à l'auteur de menace.
Risque	Degré de probabilité qu'un auteur de menace exploite une vulnérabilité pour accéder à un actif, et répercussions connexes.
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.
Chaîne d'approvisionnement	Réseau et processus qui existent entre une organisation et ses fournisseurs pour assurer la production et la distribution d'un produit.
Contrôle de sécurité technique	Classe de contrôles de sécurité qui est mise en œuvre et exécutée par les systèmes d'information, principalement par l'intermédiaire de mécanismes de sécurité intégrés aux composants matériels, logiciels et micrologiciels.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice à l'information et aux actifs TI.
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 actifs ou les activités d'une organisation.

9.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)*, septembre 2021.
2	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*, décembre 2014.
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. *Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)*, février 2020.
5	Centre canadien pour la cybersécurité. *Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations (ITSAP.00.070)*, mars 2019.
6	Centre canadien pour la cybersécurité. *Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations (ITSAP.40.001)*, avril 2019.
7	Centre canadien pour la cybersécurité. *Conseils sur la mise en œuvre de l'agilité cryptographique (ITSAP.40.018)*, mai 2022.
8	Centre canadien pour la cybersécurité. *Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)*, décembre 2020.
9	Centre canadien pour la cybersécurité. *Sécurisation de l'entreprise et des technologies mobiles (ITSM.80.001)*, juillet 2016.
10	Centre canadien pour la cybersécurité. *Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP) (ITSM.70.003)*, mai 2022.
11	Centre canadien pour la cybersécurité. *La cybersécurité et la chaîne d'approvisionnement : évaluation des risques (ITSAP.10.070)*, juillet 2022.
12	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI : Nº 6, Miser sur une formation sur mesure en matière de cybersécurité (ITSM.10.093)*, février 2020.
13	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI : Nº 3, Gestion et contrôle des privilèges d'administrateur (ITSM.10.094)*, juillet 2022.

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

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

A.1.1 Contrôle d'accès

Le tableau 2 décrit le contrôle de sécurité du contrôle d'accès applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 2 : Contrôles de sécurité techniques de l'ITSG-33 : contrôle d'accès

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
AC-20	Utilisation de systèmes d'information externes	(A) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent ou maintiennent des systèmes d'information externes, définit les modalités permettant aux personnes autorisées d'accéder au système d'information à partir de systèmes d'information externes. (B) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent ou maintiennent des systèmes d'information externes, définit les modalités permettant aux personnes autorisées de traiter, de stocker ou de transmettre de l'information contrôlée par l'organisation à l'aide de systèmes d'information externes.	**Limites relatives à l'utilisation autorisée :** L'organisation permet à des personnes autorisées d'utiliser un système d'information externe pour accéder à son système d'information ou pour traiter, stocker ou transmettre de l'information sous son contrôle seulement lorsqu'elle : i. vérifie si les contrôles de sécurité requis ont été mis en œuvre dans le système externe, tel qu'il est stipulé dans la politique de sécurité et dans le plan de sécurité de l'organisation liés à l'information; ou ii. conserve les ententes approuvées de connexion au système d'information ou de traitement avec l'entité organisationnelle qui héberge le système d'information externe. Consultez l'annexe 3A de l'ITSG-33 pour le contrôle connexe CA-2.	AC-3 AC-17 AC-19 CA-2 CA-3 PL-4 SA-9

			Dispositifs de stockage portatifs : L'organisation [*Sélection : limite; interdit*] l'utilisation de dispositifs mobiles qu'elle contrôle par des personnes autorisées sur les systèmes d'information externes. **Systèmes, composants et dispositifs n'appartenant pas à l'organisation :** L'organisation [*Sélection : limite, interdit*] l'utilisation de systèmes d'information, de composants système et de dispositifs ne lui appartenant pas, à des fins de traitement, de stockage ou de transmission d'information organisationnelle. **Dispositifs de stockage accessibles par réseau :** L'organisation interdit l'utilisation de [dispositifs de stockage accessibles par réseau, définis par l'organisation] dans des systèmes d'information externes.	

A.1.2 Vérification et responsabilité

Le tableau 3 décrit le contrôle de sécurité de vérification et de responsabilité mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 3 : Contrôles de sécurité techniques de l'ITSG-33 : vérification et responsabilité

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
AU-1	Politique et procédures de vérification et de responsabilité	(A) L'organisation élabore, documente et diffuse à [*liste des employés et des rôles définie par l'organisation*] : i. une politique de vérification et de responsabilité qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect; ii. des procédures pour faciliter la mise en œuvre de la politique de vérification et de responsabilité ainsi que les contrôles connexes. (B) L'organisation examine et met à jour : i. la politique de vérification et de responsabilité [*fréquence définie par l'organisation*]; ii. les procédures de vérification et de responsabilité [*fréquence définie par l'organisation*].	Aucune	

A.2 Contrôles de sécurité opérationnels

A.2.1 Gestion des configurations

Le tableau 4 décrit le contrôle de sécurité de la gestion des configurations applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 4 : Contrôles de sécurité opérationnels de l'ITSG-33 : gestion des configurations

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
CM-8	Inventaire des composants de système d'information	(A) L'organisation élabore et tient un inventaire des composants de système d'information qui illustre exactement le système d'information actuel. (B) L'organisation élabore et tient un inventaire des composants de système d'information qui contient tous les composants se trouvant à l'intérieur de la limite d'autorisation du système d'information. (C) L'organisation élabore et tient un inventaire des composants de système d'information qui est au niveau de granularité jugé nécessaire aux fins de suivi et de production de rapports. (D) L'organisation élabore et tient un inventaire des composants de système d'information qui comprend [*Affectation : information définie par l'organisation et jugée nécessaire à la comptabilisation efficace des composants de système d'information*]. (E) L'organisation examine et met à jour l'inventaire des composants de système d'information [*Affectation : fréquence définie par l'organisation*].	**Mises à jour durant les installations et les retraits :** L'organisation met à jour l'inventaire des composants de système d'information dans le cadre des activités d'installation et de retrait des composants et de mise à jour du système d'information. **Automatisation de la maintenance :** L'organisation utilise des mécanismes automatisés pour faciliter la tenue d'un inventaire des composants du système d'information qui soit à jour, complet, exact et facilement accessible. Consultez également l'annexe 3A de l'ITSG-33 pour le contrôle connexe SI-7. **Détection automatisée de composants non autorisés:** i. L'organisation utilise des mécanismes automatisés [*Affectation : fréquence définie par l'organisation*] pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information. ii. L'organisation prend les mesures suivantes lorsqu'elle détecte des composants non autorisés : [*Sélection (un choix ou plus) : désactiver l'accès réseau de ces composants; isoler les composants; aviser [Affectation : liste des employés ou des rôles définie par l'organisation]*].	AC-17 AC-18 AC-19 CA-7 CM-2 CM-6 RA-5 SA-4 SI-3 SI-4 SI-7

			Consultez également l'annexe 3A de l'ITSG-33 pour les contrôles connexes AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7 et RA-5. **Information sur la comptabilisation :** L'organisation inclut 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. **Aucune comptabilisation en double des composants :** L'organisation s'assure que tous les composants respectant la limite d'autorisation du système d'information ne sont pas reproduits dans d'autres inventaires de composants de système d'information. **Configurations évaluées et écarts approuvés :** L'organisation inclut dans l'inventaire des composants du système d'information les configurations de composants évaluées et les écarts approuvés en ce qui a trait aux configurations déjà déployées. Consultez également l'annexe 3A de l'ITSG-33 pour les contrôles connexes CM-2 et CM-6. **Dépôt centralisé :** L'organisation fournit un dépôt centralisé contenant l'inventaire des composants de système d'information. **Localisation automatisée :** L'organisation utilise des mécanismes automatisés pour géolocaliser les composants de système d'information. **Attribution de composants à des systèmes :** i. L'organisation attribue [*Affectation : composants de système d'information définis par l'organisation*] à un système d'information. ii. L'organisation reçoit un avis concernant cette attribution de la part du propriétaire du système d'information. Consultez également l'annexe 3A de l'ITSG-33 pour le contrôle connexe SA-4.	

A.2.2 Planification d'urgence

Le tableau 5 décrit le contrôle de sécurité de la planification d'urgence applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 5 : Contrôles de sécurité opérationnels de l'ITSG-33 : planification d'urgence

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
CP-9	Sauvegarde du système d'information	(A) L'organisation effectue des sauvegardes des données utilisateur contenues dans le système d'information [*fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*]. (B) L'organisation effectue des sauvegardes des données système contenues dans le système d'information [*fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*]. (C) L'organisation effectue des sauvegardes de la documentation liée au système d'information, y compris la documentation sur la sécurité [*fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise*]. (D) L'organisation protège la confidentialité, l'intégrité et l'accessibilité de l'information de sauvegarde aux sites de stockage. (E) L'organisation détermine les périodes de conservation de l'information opérationnelle essentielle et des sauvegardes archivées.	**Tests de fiabilité et d'intégrité :** L'organisation effectue des tests de l'information de sauvegarde [*fréquence définie par l'organisation*] pour vérifier la fiabilité des supports et l'intégrité de l'information. Voir le contrôle de sécurité connexe CP-4. **Essai de restauration au moyen de l'échantillonnage :** L'organisation utilise un échantillon de l'information de sauvegarde pour restaurer certaines fonctions du système d'information dans le cadre des tests du plan d'urgence. Voir le contrôle de sécurité connexe CP-4. **Stockage distinct pour l'information essentielle :** L'organisation conserve des copies de sauvegarde [*information liée à la sécurité et logiciels des systèmes d'information essentiels définis par l'organisation*], dans une installation distincte ou un conteneur résistant au feu situé hors de l'emplacement du système opérationnel. Voir les contrôles de sécurité connexes CM-2 et CM-8. **Transfert au site de stockage de secours :** L'organisation transfère l'information de sauvegarde du système d'information à un site de stockage de secours [*durée et débit de transfert définis par l'organisation et conformes aux objectifs de délai et de point de reprise*].	AC-3 CM-2 CM-8 CP-2 CP-4 CP-6 CP-7 CP-10 MP-2 MP-4 MP-5 SC-13

			Système secondaire redondant : L'organisation effectue la sauvegarde du système d'information 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. Voir les contrôles de sécurité connexes CP-7 et CP-10. **Double autorisation :** L'organisation applique l'exigence de double autorisation pour la suppression ou la destruction [*information de sauvegarde définie par l'organisation*]. Voir les contrôles de sécurité connexes AC-3 et MP-2.	

A.2.3 Protection des supports

Le tableau 6 décrit le contrôle de sécurité de protection des supports applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 6 : Contrôles de sécurité opérationnels de l'ITSG-33 : protection des supports

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
MP-6	Nettoyage des supports	(A) L'organisation nettoie les [*supports du système d'information définis par l'organisation*] avant leur élimination ou leur transfert hors de son contrôle ou à des fins de réutilisation. Elle utilise des [*techniques et procédures de nettoyage définies par l'organisation*], conformément à ses normes et politiques applicables ainsi que celles du GC. (B) L'organisation utilise des mécanismes de nettoyage dont la robustesse et l'intégrité correspondent à la catégorie de sécurité ou à la classification de l'information.	**Examen, approbation, suivi, documentation et vérification :** L'organisation examine, approuve, suit, documente et vérifie le nettoyage des supports et les activités d'élimination. Voir le contrôle de sécurité connexe SI-12. **Mise à l'essai du matériel :** L'organisation teste les procédures et l'équipement de nettoyage [*fréquence définie par l'organisation*] en vue de s'assurer que le nettoyage prévu a bien été réalisé. **Techniques non destructives :** L'organisation nettoie les dispositifs de stockage portatifs au moyen de techniques de nettoyage non destructives avant de les connecter au système d'information dans les situations suivantes : [*liste définie par l'organisation des circonstances où les dispositifs de stockage portatifs doivent être nettoyés*]. Voir le contrôle de sécurité connexe SI-3. **Double autorisation :** L'organisation fait appel à une double autorisation pour ce qui est du nettoyage des [*supports du système d'information définis par l'organisation*]. Voir les contrôles de sécurité connexes AC-3 et MP-2.	AC-3 MA-2 MA-4 MP-2 RA-3 SC-4 SI-3 SI-12

			Purge et nettoyage à distance de l'information : L'organisation fournit la capacité de purger et nettoyer l'information qui se trouve sur les [*systèmes d'information, composants système ou dispositifs définis par l'organisation*] à distance ou en vertu des conditions suivantes : [*conditions définies par l'organisation*].	
MP-7	Utilisation des supports	(A) L'organisation [*Sélection : limite, interdit*] l'utilisation de [*types de supports de support d'information définis par l'organisation*] sur les [*systèmes d'information ou composants système définis par l'organisation*] au moyen de [*mesures de protection définies par l'organisation*]. Remarque : Ce contrôle s'applique également aux dispositifs mobiles dotés d'une capacité de stockage d'information (p. ex. téléphones intelligents, tablettes, liseuses).	**Interdire l'utilisation sans propriétaire :** L'organisation interdit dans ses systèmes d'information l'utilisation de dispositifs de stockage portatifs dont le propriétaire est inconnu. Voir le contrôle connexe PL-4. **Interdire l'utilisation de supports résistant au nettoyage** L'organisation interdit l'utilisation de supports résistant au nettoyage dans ses systèmes d'information. Voir le contrôle connexe MP-6.	AC-19 MP-6 PL-4

A.2.4 Intégrité de l'information et des systèmes

Le tableau 7 décrit le contrôle de sécurité d'intégrité de l'information et des systèmes applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 7 : Contrôles de sécurité opérationnels de l'ITSG-33 : intégrité de l'information et des systèmes

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SI-12	Traitement et conservation des sorties d'information	(A) L'organisation traite et conserve l'information interne et celle produite par le système d'information conformément aux lois du GC, aux politiques, directives et normes applicables du SCT et aux exigences opérationnelles.	Aucune	AC-16 AU-5 AU-11 MP-2 MP-4

A.3 Contrôles de sécurité de gestion

A.3.1 Évaluation des risques

Le tableau 8 décrit le contrôle de sécurité d'évaluation des risques applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 8 : Contrôles de sécurité de gestion de l'ITSG-33 : évaluation des risques

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
RA-2	Catégorisation de sécurité	(A) L'organisation catégorise l'information et les systèmes d'information conformément aux lois du gouvernement du Canada et aux prescriptions du SCT. (B) L'organisation documente les résultats de la catégorisation (y compris les justifications) dans le plan de sécurité du système d'information. (C) L'organisation s'assure que la décision concernant la catégorisation de sécurité est examinée et approuvée par l'autorité responsable ou par son représentant désigné.	Aucune	CM-8 MP-4 RA-3 SC-7

A.3.2 Acquisition des systèmes et des services

Le tableau 9 décrit le contrôle de sécurité d'acquisition des systèmes et des services applicable mentionné à l'annexe 3A de l'ITSG-33 [2].

Tableau 9 : Contrôles de sécurité de gestion de l'ITSG-33 : acquisition des systèmes et des services

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SA-9	Services de système d'information externes	(D) L'organisation exige que les fournisseurs de services de système d'information externes respectent ses exigences en matière de contrôle de sécurité de l'information et utilisent les [*contrôles de sécurité définis par l'organisation*] conformément à la *Norme de sécurité et de gestion des marchés du SCT*. (E) L'organisation définit et documente la surveillance gouvernementale, de même que les rôles et responsabilités des utilisateurs en ce qui a trait aux services externes de système d'information. (F) L'organisme utilise des [*méthodes, techniques et processus définis par l'organisation*] dans le but de surveiller en tout temps la conformité des fournisseurs de services externes aux contrôles de sécurité.	**Évaluation des risques et approbations organisationnelles :** i. L'organisation effectue une évaluation des risques avant l'acquisition ou l'impartition des services spécialisés de sécurité de l'information. ii. L'organisation s'assure que l'acquisition ou l'impartition de ces services est approuvée par [*personnel ou rôles définis par l'organisation*]. Voir les contrôles de sécurité connexes CA-6 et RA-3. **Identification des fonctions, des ports, des protocoles et des services :** L'organisation exige que les fournisseurs de [*services de systèmes d'information externes désignés par l'organisation*] identifient les fonctions, les ports, les protocoles et les autres services qui sont requis pour l'utilisation des services en question. Voir le contrôle connexe CM-7. **Établir et maintenir une relation de confiance avec les fournisseurs de services :** L'organisation établit, documente et maintient une relation de confiance avec les fournisseurs de services externes en se fondant sur [*exigences de sécurité, propriétés, facteurs ou conditions définissant ce qui constitue une relation de confiance adéquate*].	CA-3 CA-6 CM-7 IR-7 PS-7 RA-3

			Concordance des intérêts des clients et des fournisseurs : L'organisation emploie [*mesures de protection définies par l'organisation*] pour veiller à ce que les intérêts de [*fournisseurs de services externes désignés par l'organisation*] répondent aux intérêts de l'organisation. **Lieux de traitement, de stockage et de service :** Les organisations circonscrivent les lieux de [*Sélection (un ou plusieurs) : services de traitement de l'information; de stockage d'information/de données; de systèmes d'information*] à [*lieux désignés par les organisations] en se fondant sur [exigences ou conditions définies par les organisations*].	