Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les 10 mesures de sécurité des TI : Nº 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications

SÉRIE GESTIONNAIRES

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 TI 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 5 aout 2022.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	5 aout 2022

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

Vue d'ensemble

L'une des 10 mesures de sécurité des TI recommandées par le CST consiste à appliquer les correctifs aux systèmes d'exploitation et aux applications. Le présent document énonce plusieurs pratiques exemplaires en matière d'application des correctifs. Les conseils formulés dans la présente sont fondés sur les contrôles de sécurité mentionnés dans l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2].

Les fournisseurs de logiciels découvrent et signalent des vulnérabilités présentes dans leurs logiciels, puis ils publient de nouveaux correctifs pour remédier aux problèmes. Cependant, en signalant les vulnérabilités publiquement, ils fournissent également aux auteurs de menace des détails sur les vulnérabilités actuelles. Les auteurs de menace ciblent les organisations de toutes tailles. Si les organisations ne prennent pas les mesures nécessaires pour mettre à l'essai les correctifs logiciels, gérer les changements requis et les déployer le plus tôt possible après leur diffusion, les auteurs de menace peuvent se servir des vulnérabilités logicielles pour exploiter les réseaux, les systèmes et les actifs TI des organisations.

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]. 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 si la prise de plus amples mesures est nécessaire. Pour de plus amples renseignements sur la mise en œuvre 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

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Introduction

Le présent document offre des conseils sur les pratiques exemplaires relatives à l'application des correctifs à vos systèmes d'exploitation (SE) et à vos applications. L'application des correctifs, qui comprend les activités liées à la mise à l'essai des mises à jour et des correctifs, à la gestion des changements et à la mise en œuvre, réduit l'exposition de votre organisation aux menaces qui pourraient exploiter les vulnérabilités connues et compromettre vos réseaux, vos systèmes et vos actifs 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].

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. Les 10 mesures de sécurité comprennent les mesures prioritaires que votre organisation devrait adopter comme base de référence pour renforcer son infrastructure TI et protéger ses réseaux. Bien qu'il soit recommandé de suivre l'ordre numérique de ces mesures (en commençant par la mesure n°1) pour accroître vos efforts de protection contre les cybermenaces, vous pouvez changer la séquence des mesures de manière à répondre aux besoins et aux exigences de votre organisation. À mesure que vous ajoutez des mesures de sécurité dans votre environnement, votre exposition aux menaces (c.-à-d. tous les terminaux disponibles qu'un auteur de menace peut tenter d'exploiter) diminue, alors que votre posture de sécurité augmente.

Il convient de se rappeler que ces mesures ne sont qu'un point de départ et qu'aucune stratégie ne peut à elle seule prévenir tous les cyberincidents. Le contexte des cybermenaces est en constante évolution, et vous devriez veiller à réévaluer vos risques et à revoir les efforts en matière de sécurité de sorte à pouvoir tenir compte de toute lacune ou faiblesse.

Lorsque vous déterminez vos besoins liés à la sécurité, vous devriez également établir si votre organisation optera pour un modèle sur place ou un modèle d'externalisation à un fournisseur de services gérés (FSG) ou à un fournisseur de services infonuagiques (FSI). Si vous décidez de recourir à un FSG ou à un FSI, vous devriez évaluer les menaces, les vulnérabilités, les responsabilités partagées et les capacités de la plateforme infonuagique afin de pouvoir appliquer les contrôles de sécurité appropriés. La mise en œuvre des 10 mesures de sécurité peut varier selon les types de services utilisés. Par exemple, les rôles et les responsabilités de votre organisation et de votre FSG ou FSI dépendront des services que vous utilisez, ainsi que de vos modèles de services et de déploiement. En revanche, même si elle fait appel à des services infonuagiques ou gérés, votre organisation est toujours responsable sur le plan juridique d'assurer la sécurité de ses données et de rendre des comptes à cet égard. Pour de plus amples renseignements sur la sécurité et les services infonuagiques ou gérés, veuillez consulter l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique* [3], et l'ITSM.50.030, *Facteurs à considérer par les clients de services gérés en matière de cybersécurité* [4].

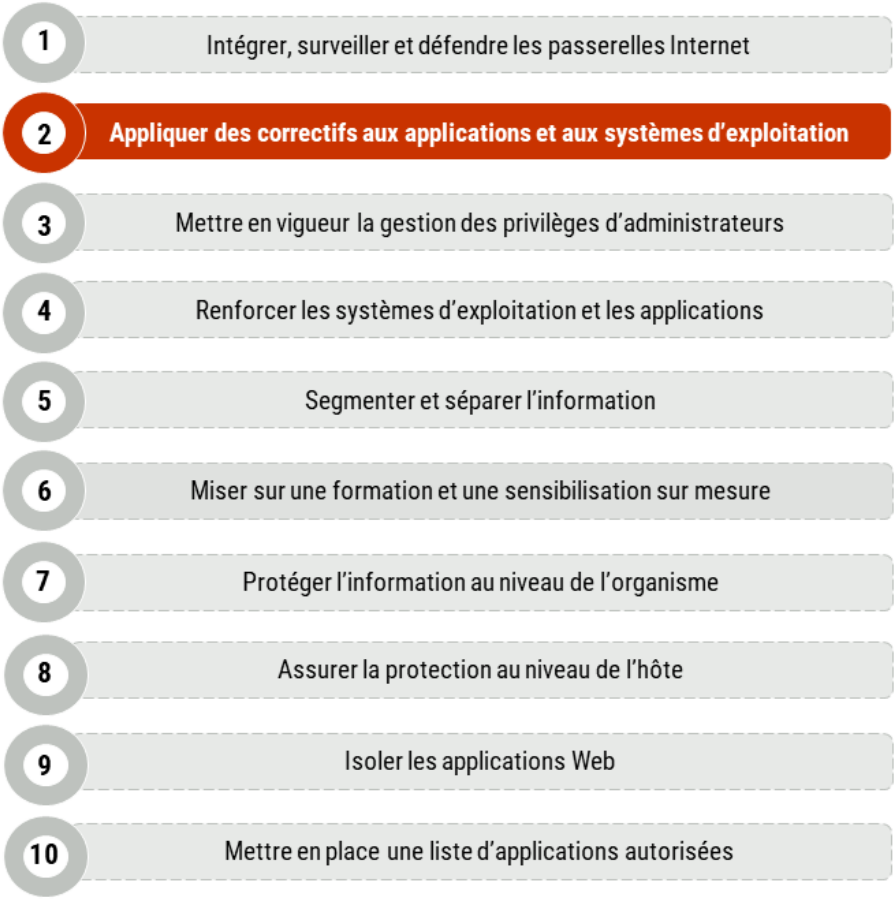

Figure 1 : Les 10 mesures de sécurité des TI – Nº 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications

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] est un cadre de gestion des risques qui 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 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 indiqué à la figure 2, les conseils formulés dans la présente concernent les contrôles de sécurité opérationnels associés aux familles Gestion des configurations (CM pour *Configuration Management*) et Intégrité de l'information et des systèmes (SI pour *System and Information Integrity*). Ils concernent également les contrôles de sécurité de gestion associés à la famille Acquisition des systèmes et des services (SA pour *System and Services Acquisition*). Ce document fait mention de mesures qui permettent de satisfaire les contrôles de sécurité suivants :

- **CM-2 Configuration de référence;**
- **SI-2 Correction des défauts;**
- **SA-22 Composants système non pris en charge.**

De plus amples renseignements sur les contrôles CM-2, SI-2 et SA-22 sont fournis à l'annexe A du présent document.

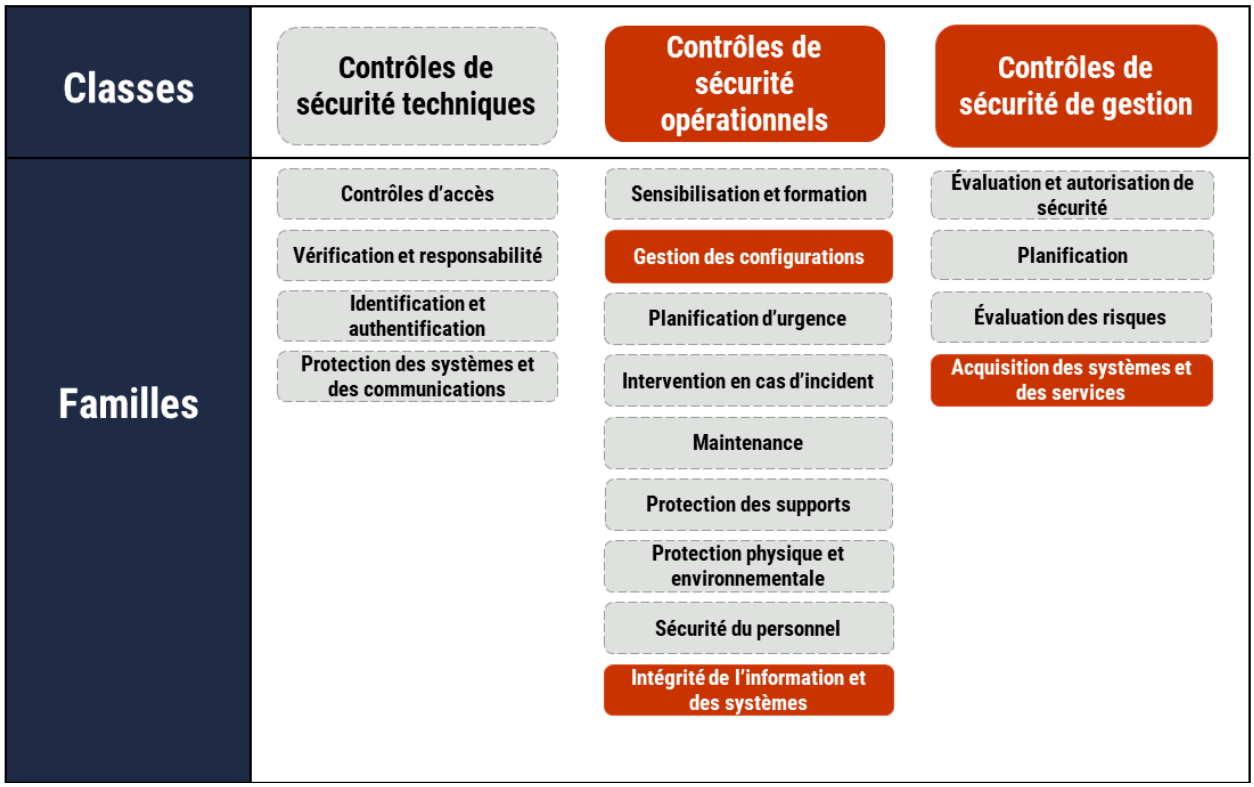

Figure 2 : Classes et familles de contrôles de sécurité applicables décrites dans l'ITSG-33

Vous pouvez utiliser les contrôles de sécurité mentionnés dans le présent document et à l'annexe 3A de l'ITSG-33 [2] pour déterminer la façon de gérer les risques liés à la cybersécurité de votre organisation et de protéger vos réseaux, vos systèmes et vos actifs TI. Il convient toutefois de garder à l'esprit que la mise en œuvre de ces contrôles ne constitue qu'une partie du processus de gestion des risques liés à la sécurité des TI.

L'ITSG-33 [2] décrit un processus fondé sur deux niveaux d'activités de gestion des risques liés à la sécurité des TI, à savoir 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 doit mettre en place et maintenir pour satisfaire un niveau de risque acceptable.

2 Vulnérabilités et correctifs de sécurité

Vous devriez toujours utiliser des versions de systèmes d'exploitation et de logiciels qui sont prises en charge, à jour et testées pour veiller à l'atténuation des vulnérabilités. Lorsque les fournisseurs de logiciels découvrent des vulnérabilités (c.-à-d. des lacunes ou des défauts) dans leurs logiciels, ils publient cette information ainsi que des correctifs visant à mettre à jour les logiciels et à pallier les vulnérabilités identifiées. Toutefois, comme ces vulnérabilités sont rendues publiques, les auteurs de menace peuvent se servir de cette information pour exploiter les failles réseau des systèmes non corrigés. Afin de limiter votre exposition aux cybermenaces, utilisez le processus de gestion des correctifs de votre organisation pour évaluer les correctifs, les mettre à l'essai, gérer les changements connexes et les appliquer aussitôt qu'ils sont diffusés. Il convient de noter que la simple application d'un correctif sans l'avoir mis à l'essai ou sans avoir évalué les répercussions qu'il peut avoir sur vos systèmes et vos logiciels peut causer des défauts ou des problèmes à la fois coûteux et chronophages. Vous devriez également avoir un inventaire permanent de vos actifs pour veiller à ce que les correctifs soient appliqués à tous les systèmes, serveurs et appareils qui utilisent les mêmes logiciels ou le même matériel informatique dès que les fournisseurs les publient.

Si votre organisation fonctionne dans un environnement infonuagique par l'entremise d'un FSI ou fait appel aux services d'un FSG, vous devriez vous assurer que vos ententes touchant la prestation des services énoncent les exigences relatives à la gestion des correctifs, ainsi que l'application des correctifs et des mises à jour d'urgence.

Il est fortement recommandé d'installer les correctifs et les mises à jour dès que possible pour garantir le bon fonctionnement et la sécurité de vos appareils et de vos systèmes. Il faut tout de même savoir que l'installation des correctifs et des mises à jour comporte certains risques. Voici les risques les plus couramment constatés :

- l'installation de correctifs peut perturber les fonctions d'autres applications ou de vos appareils (comme le redémarrage prévu à une certaine date/heure);
- le redémarrage des appareils qui viennent d'être mis à jour peut interrompre d'autres programmes, ce qui pourrait donner lieu à des pertes de données ou à des interruptions de service;
- l'installation de correctifs peut faire ressortir d'autres lacunes du programme, notamment des défauts de sécurité (c.-à-d. que l'application de correctifs devrait être considérée comme un processus continu en ce qui a trait aux opérations TI de votre organisation).

2.1 Notification de vulnérabilités et de correctifs

Les fournisseurs publient habituellement l'information suivante au sujet d'une vulnérabilité connue et du correctif connexe :

- les produits et les versions touchés;
- les détails techniques au sujet de la vulnérabilité, y compris les façons dont elle peut être exploitée;
- les conséquences d'une exploitation (p. ex. exécution de code, divulgation ou fuite d'information, déni de service);
- l'état actuel de l'exploitation (c.-à-d. si des auteurs de menace exploitent déjà la vulnérabilité);
- les solutions de contournement temporaires;
- la gravité de la vulnérabilité.

Les fournisseurs déterminent la gravité d'une vulnérabilité de différentes façons, par exemple selon une norme telle que le système de notation des vulnérabilités courantes (CVSS pour *Common Vulnerability Scoring System*) ou une catégorisation interne telle que « critique » ou « important ». Vous devriez employer les indices de gravité au départ pour évaluer la probabilité que la vulnérabilité soit exploitée dans l'environnement de votre organisation, de même que l'incidence d'une telle exploitation.

Un fournisseur peut également publier un bulletin consolidé qui comprend des instructions de déploiement recommandées pour un correctif.

2.2 Évaluation des risques liés aux vulnérabilités et aux correctifs

Après avoir analysé l'information fournie par le fournisseur, vous devriez évaluer les risques organisationnels en fonction de la vulnérabilité connue et du correctif. En réalisant une évaluation des risques, votre organisation peut déterminer le niveau de gravité en fonction de votre environnement particulier. Même si une menace pèse sur plusieurs organisations, votre organisation peut être touchée différemment que les autres.

Vous devriez dresser la liste des systèmes d'information qui sont touchés par la vulnérabilité connue. Lors de l'évaluation des risques, tenez compte du fait que les risques peuvent augmenter si un exploit s'attaque à des actifs de grande valeur ou à exposition élevée. De même, les risques peuvent être moindres si vous avez déjà des mesures d'atténuation en place. Les risques peuvent aussi être faibles si le risque d'exposition des actifs touchés est faible.

Le tableau 1 présente des exemples des divers niveaux de risque en fonction de la vulnérabilité.

Tableau 1 : Exemples d'évaluation des risques liés aux vulnérabilités

Niveau de risque	Exemples
Risque extrême	• La vulnérabilité peut mener à l'exécution de code à distance. • Les systèmes et l'information essentiels aux activités sont touchés. • Des exploits existent et sont utilisés. • Le système est connecté à Internet et aucune mesure d'atténuation n'est en place.
Risque élevé	• La vulnérabilité peut mener à l'exécution de code à distance. • Les systèmes et l'information essentiels aux activités sont touchés. • Des exploits existent et sont utilisés. • Le système est dans une enclave protégée par des mesures d'accès robustes.
Risque moyen	• La vulnérabilité permet à l'attaquant de se faire passer pour un utilisateur légitime sur une solution d'accès distant. • Le système est exposé à des utilisateurs non authentifiés. • Le système exige une authentification à deux facteurs et l'ouverture de session à distance en tant qu'administrateur n'est pas autorisée.
Risque faible	• La vulnérabilité exige que les utilisateurs authentifiés mènent des activités malveillantes (p. ex. injection SQL). • Le système touché contient de l'information publique non sensible. • Les mesures d'atténuation en place rendent l'exploitation improbable ou très difficile.

Le tableau 2 présente des exemples simplifiés d'évaluation des risques liés à un correctif qui n'est pas installé. Dans cet exemple, trois organisations ayant mis en œuvre des mesures de sécurité différentes dans leur environnement évaluent une vulnérabilité courante (vulnérabilité critique d'exécution de code à distance touchant un logiciel).

Tableau 2 : Exemples d'évaluation des risques liés à un correctif visant une vulnérabilité critique d'exécution de code à distance touchant un logiciel

Organisation	Mesures de sécurité en place	Évaluation des risques liés au correctif
Organisation A	• Aucune	Extrême
Organisation B	• Filtrage efficace du contenu des courriels • Utilisateurs avec droits d'accès faibles	Élevé
Organisation C	• Filtrage efficace du contenu des courriels • Liste d'applications autorisées • Utilisateurs avec droits d'accès faibles	Moyen

3 Configuration de référence pour les systèmes (CM-2)

Les conseils énoncés dans cette section sont fondés sur le contrôle **CM-2, Configuration de référence**. Les sous-sections 3.1 à 3.4 présentent des mesures visant à renforcer votre configuration de référence. Ces mesures sont basées sur les améliorations du contrôle CM-2. Pour en savoir plus, consultez la section A.1 de l'annexe A.

Même si la mise à jour de vos systèmes et de vos logiciels réduira l'exposition de votre organisation aux menaces, vous devriez aussi élaborer, consigner et tenir à jour une configuration de référence pour vos systèmes. Les versions, les publications et les changements à venir concernant vos systèmes reposent sur votre configuration de référence. Les mises à jour, les retraits et les ajouts système pourraient modifier le comportement de vos systèmes, et une configuration de référence vous aidera à déterminer et à définir la cause de défauts ou de problèmes potentiels.

Votre configuration de référence devrait comprendre l'information sur les composants de systèmes d'information suivante :

- les logiciels standards installés sur les postes de travail, les serveurs, les composants réseau ou les appareils mobiles;
- les numéros de versions courantes et l'information liée aux correctifs qui sont appliqués aux systèmes d'exploitation et aux applications;
- les paramètres de configuration.

La configuration de référence devrait également fournir de l'information sur la topologie du réseau, l'emplacement logique des composants dans l'architecture du système et les mesures de sécurité mises en œuvre. De plus, vous devriez comparer la configuration des coupe-feux et des routeurs sur chaque appareil pour vous assurer qu'aucun changement non autorisé n'a été apporté.

Il est recommandé de stocker les diagrammes et documents relatifs à votre configuration de référence dans un environnement fiable qui est séparé du système d'exploitation standard.

3.1 Examens et mises à jour

Pour tenir à jour votre configuration de référence, vous devez évaluer les changements apportés aux systèmes et déterminer si la création d'une nouvelle configuration de référence s'impose. La tenue à jour de la configuration de référence devrait être intégrée à votre processus de gestion des changements. Votre organisation est responsable de définir la fréquence et les circonstances de l'examen et de la mise à jour de la configuration de référence, mais celle-ci devrait être examinée et mise à jour lorsque vous installez et mettez à niveau des composants de systèmes d'information.

Votre organisation peut utiliser un mécanisme automatisé pour l'aider à maintenir une configuration de référence à jour, complète, juste et facilement accessible. Les outils d'inventaire de logiciels et de matériel, les outils de gestion de configuration et les outils de gestion de réseau sont des exemples de mécanismes automatisés.

3.2 Configurations antérieures

Votre organisation devrait conserver les versions antérieures de configuration de référence (p. ex. matériel, logiciels, micrologiciels, et fichiers et données de configuration). La conservation des versions antérieures vous permettra de retourner à une version précédente dans l'éventualité où les mises à jour et les changements apportés donnent lieu à des défauts ou à des problèmes.

3.3 Environnements de test et de développement

Vous devriez tenir à jour une configuration de référence pour les environnements de test et de développement. Cette configuration de référence devrait être gérée séparément de votre configuration de référence opérationnelle.

En ayant une configuration de référence distincte pour les environnements de test et de développement, vous pouvez protéger vos systèmes opérationnels contre les événements imprévus qui peuvent découler des activités de test et de développement. Vous pouvez également utiliser les configurations de référence distinctes pour gérer les configurations de manière adéquate. Par exemple, bien que la gestion des configurations opérationnelles demande de la stabilité, il faut faire preuve d'une plus grande souplesse lors de la gestion des configurations dans les environnements de test et de développement.

3.4 Configurations en voyage

Si des employés de votre organisation voyagent à l'étranger, vous devriez établir les répercussions de ces voyages sur la sécurité de vos systèmes et de vos appareils. Appliquez des mesures de sécurité supplémentaires à tous les appareils qui ont quitté le pays et élaborez un processus pour évaluer les appareils afin de déterminer quelles sont les prochaines étapes. Dans certains cas, il se peut que vous puissiez les réintégrer dans vos réseaux et systèmes organisationnels. Cependant, la réintégration de ces appareils peut exposer votre organisation à de graves risques. Ainsi, vous opterez peut-être pour le nettoyage et la réinitialisation des appareils, voire leur élimination, lorsque les employés sont de retour au pays.

4 Gestion des correctifs (SI-2)

Les conseils énoncés dans cette section sont fondés sur le contrôle **SI-2, Correction des défauts**. Pour en savoir sur ce contrôle, consultez la section A.2 de l'annexe A.

La réussite des activités de votre organisation repose sur sa capacité de maintenir des systèmes fiables. Votre organisation devrait détecter, signaler et corriger les défauts et les vulnérabilités des systèmes d'information dans les plus brefs délais. La gestion des correctifs est une stratégie et un processus organisationnels d'acquisition, de validation, de mise à l'essai et d'installation des correctifs et des mises à jour pour vos systèmes et vos appareils. Vous pouvez employer un logiciel de gestion des correctifs pour vous aider à recevoir, à valider, à mettre à l'essai et à installer les correctifs.

Afin d'assurer la fiabilité continue de vos systèmes, votre organisation devrait traiter la gestion des correctifs comme une mesure de sécurité prioritaire. Votre organisation protège ses réseaux, ses systèmes et ses actifs TI, et renforce sa posture de sécurité en s'assurant que tous les correctifs applicables ont été installés. Votre processus de gestion des correctifs devrait comprendre les mesures suivantes :

- surveiller la diffusion de nouveaux correctifs pour les appareils que vous utilisez;
- tester les correctifs (si possible) pour s'assurer qu'ils sont compatibles avec l'environnement et les logiciels visés;
- examiner les exigences additionnelles qui pourraient s'appliquer pour que les correctifs puissent être installés et fonctionner normalement;
- envoyer des avis lorsque des correctifs sont publiés;
- installer les correctifs;
- confirmer que les correctifs ont bien été appliqués.

Dans le cas des appareils personnels, il est recommandé de configurer la fonction de mise à jour automatique en guise de mesure de gestion des correctifs. Bien que la fonction de mise à jour automatique ne teste pas les correctifs, elle optimise sans délai le niveau de sécurisation des dispositifs en appliquant les mesures requises dès qu'elles sont accessibles.

Lorsque vous impartissez vos services TI à un FSI, le modèle de partage des responsabilités est un facteur essentiel à l'établissement des responsabilités et des mesures requises par votre organisation et par le FSI. Ce modèle définit la portée des responsabilités en matière de sécurité du FSI et celle de votre organisation. Généralement, le FSI est responsable de la sécurité du nuage, tandis que votre organisation est responsable des données stockées dans le nuage. Si vous avez externalisé vos services TI à un FSI ou à un FSG, n'oubliez pas d'inclure la gestion des correctifs à votre modèle de partage des responsabilités. Votre contrat de service devrait également comprendre votre modèle de partage des responsabilités afin d'établir les rôles et les responsabilités en matière de gestion des correctifs, lesquels varieront en fonction de votre modèle de services infonuagiques. Par exemple, dans le cas d'une infrastructure-service (IaaS pour *Infrastructure as a Service*) ou d'une plateforme-service (PaaS pour *Platform as a Service*), il vous incombe de mettre à jour vos systèmes et vos applications et d'appliquer les correctifs. Dans le cas d'un logiciel-service (SaaS pour *Software as a Service*), le FSI est responsable de l'application des mises à jour et des correctifs. Toutefois, même si vous utilisez un fournisseur de services, c'est à vous que revient la responsabilité d'appliquer les mises à jour et les correctifs aux applications, aux systèmes et aux appareils associés aux services qui ne font pas partie du contrat.

4.1 Délai d'application des correctifs

Après avoir évalué les niveaux de risque de votre organisation et l'applicabilité du correctif dans votre environnement, vous devriez déployer le correctif sans tarder. Vous devriez mettre en place une stratégie d'application opportune des correctifs. Cette stratégie devrait définir les délais pour l'application opportune des mesures correctives aux vulnérabilités, laquelle permet de réduire l'exposition de votre organisation aux menaces.

Le délai dans lequel vous déployez un correctif peut dépendre des niveaux de risque associés à la vulnérabilité et au correctif. Il est recommandé d'utiliser les délais suivants :

- **Niveau de risque extrême :** délai de 48 heures;
- **Niveau de risque élevé :** délai de deux semaines;
- **Niveau de risque moyen :** à la prochaine mise à jour importante ou dans un délai de trois mois;
- **Niveau de risque faible :** à la prochaine mise à jour importante ou dans un délai d'un an.

4.2 Mise à l'essai des correctifs

De nombreux fournisseurs de logiciels mettent à l'essai rigoureusement les correctifs avant de les diffuser publiquement. Normalement, ces essais sont réalisés dans une variété d'environnements, d'applications et de conditions. Il convient toutefois de noter que votre organisation est responsable d'effectuer les tests supplémentaires requis afin de déterminer les répercussions des correctifs sur votre environnement.

Vous devriez d'abord déployer un correctif à un groupe pilote d'utilisateurs qui proviennent de toutes les unités opérationnelles de l'organisation (p. ex. finances, ressources humaines et opérations). Si le groupe pilote ne signale aucune anomalie dans un délai de 48 heures, le déploiement du correctif dans l'ensemble de l'organisation peut aller de l'avant.

4.3 Déploiement des correctifs

Avant d'installer un nouveau correctif, les administrateurs de système devraient lire toute l'information contextuelle pertinente liée au correctif, notamment les détails et les exigences relatifs à l'installation. Il pourrait également s'avérer utile de réaliser de plus amples recherches. À titre d'exemple, une recherche externe peut révéler que l'installation du correctif occasionne certains problèmes.

Les mises à jour automatiques de logiciels et de micrologiciels assurent l'installation opportune des correctifs. Vous devriez toutefois tenir compte des besoins de votre organisation concernant la gestion et le maintien des configurations système, de même que des répercussions possibles des mises à jour automatiques sur vos activités opérationnelles.

L'application des correctifs aux systèmes d'exploitation d'appareils mobiles n'est généralement pas automatique et demande une interaction avec l'utilisateur. Votre organisation devrait mettre en œuvre une stratégie pour veiller à ce que les utilisateurs appliquent les correctifs au système d'exploitation de leurs appareils mobiles lorsqu'ils reçoivent un avis du fournisseur de télécommunications sans fil. Il se peut que certains fournisseurs prennent en charge les mises à jour automatiques du système d'exploitation pour les appareils mobiles de l'organisation moyennant des frais de service supplémentaires.

N'oubliez pas de retirer toute version antérieure de composants logiciels ou micrologiciels après l'installation des versions mises à jour.

4.4 Solutions de contournement

Si le fournisseur n'a pas encore diffusé de correctif pour une vulnérabilité, il se peut qu'il publie des solutions de contournement ou des mesures de correction temporaires. Ces solutions de contournement peuvent comprendre, à titre d'exemple, la désactivation de la fonctionnalité vulnérable dans le logiciel ou dans l'appareil, ou encore l'utilisation de coupe-feux et d'autres contrôles d'accès visant à restreindre ou à bloquer l'accès au service vulnérable. En ce qui a trait aux appareils mobiles, les solutions de contournement peuvent comprendre la restriction de la fonctionnalité ou la mise en œuvre d'une liste d'applications interdites, généralement par l'entremise d'un logiciel de gestion des appareils mobiles (MDM pour *Mobile Device Management)* ou d'un logiciel de gestion unifiée des terminaux (UEM pour *Unified Endpoint Management*).

Tout comme l'application des correctifs, la décision relative à la mise en œuvre d'une solution de contournement temporaire est fondée sur les risques. Vous devriez faire appel à des solutions de contournement temporaires uniquement dans les cas où il n'existe pas encore de correctifs permettant de résoudre des vulnérabilités ou des problèmes touchant les logiciels et les systèmes d'exploitation. Il est recommandé de faire un suivi de toutes les solutions de contournement temporaires afin de veiller à ce que les correctifs soient téléchargés de manière à se compléter et à se prendre en charge mutuellement (plutôt qu'à se chevaucher). La gestion des solutions de contournement peut s'avérer difficile si ces solutions ne sont pas toutes suivies et documentées adéquatement. Si une solution de contournement nécessaire était retirée, votre organisation risquerait d'exposer les systèmes et les logiciels vulnérables à des menaces.

Il faut donc se rappeler que les solutions de contournement ne sont pas permanentes. Vous devriez appliquer le correctif dès qu'il est publié et supprimer ensuite la solution de contournement. Votre organisation devrait aussi déployer d'autres mesures d'atténuation, comme un système de prévention d'intrusion et un coupe-feu d'applications Web, dans le but d'ajouter des couches de défense en l'absence d'un correctif ou en cas de retard.

4.5 Surveillance et évaluation continues

Après l'installation d'un correctif, les administrateurs de système devraient réaliser des audits afin de mesurer le taux de réussite et s'assurer qu'il est efficace. À titre de mesure d'atténuation supplémentaire, vous devriez également vous abonner aux alertes de sécurité de votre fournisseur et à ses fils de renseignement sur les menaces. Par ailleurs, les administrateurs de système de votre organisation devraient rester au fait des mises à jour de correctifs pour les applications, les systèmes d'exploitation et les réseaux afin qu'ils puissent savoir quand de nouvelles vulnérabilités sont découvertes et quand appliquer les correctifs. Il est également recommandé de réaliser une surveillance externe des vulnérabilités connues que le correctif est censé résoudre et de veiller à ce que les systèmes de votre organisation n'aient pas fait l'objet de tentatives d'exploitation.

Afin de corriger les vulnérabilités et les défauts découverts dans vos systèmes d'exploitation, vous devriez tirer parti des ressources de source ouverte, notamment les bases de données Common Weakness Enumeration (CWE) ou Common Vulnerabilities and Exposures (CVE).

4.6 Gestion des correctifs pour les systèmes essentiels

L'application de correctifs peut entraîner une période d'indisponibilité et ainsi des conséquences opérationnelles graves sur les systèmes essentiels devant être fonctionnels en tout temps, comme c'est le cas pour certains systèmes de contrôle industriels (SCI) et certaines technologies opérationnelles (TO). Compte tenu de cette exigence, vous devez établir un plan de gestion des correctifs cohérent qui comprend la participation du personnel des TI, de la sécurité des TI, de la conception des processus, des opérations et de la haute direction.

Si un système doit fonctionner continuellement, il est possible que vous ne soyez pas en mesure de retirer un appareil pour y apporter des mises à jour micrologicielles. Si c'est le cas, votre organisation doit évaluer et approuver le niveau de tolérance au risque et mettre en place d'autres mesures de sécurité pour améliorer la sécurité du système.

5 Systèmes et logiciels non pris en charge (SA-22)

Cette section repose sur le contrôle **SA-22, Composants système non pris en charge**. La sous-section 5.1 offre des conseils sur les autres sources possibles de soutien, lesquels sont abordés dans l'amélioration du contrôle SA-22. Pour en savoir plus, consultez la section A.3 de l'annexe A.

Les appareils, les systèmes d'exploitation et les logiciels qui ne sont pas pris en charge sont ceux pour lesquels le fabricant ne diffuse plus de correctifs ni de mises à jour. Les appareils patrimoniaux et non pris en charge sont susceptibles de présenter des vulnérabilités qui ne seront vraisemblablement jamais corrigées, ce qui accroît le niveau de risque encouru par votre organisation. S'il est impossible de mettre à jour les systèmes et les logiciels, les auteurs de menace peuvent continuer à exploiter les vulnérabilités présentes.

Vous devriez remplacer les composants système et les logiciels pour lesquels le développeur, le fournisseur ou le fabricant n'offre plus de soutien (p. ex. correctifs de logiciels, mises à jour de micrologiciels, contrats de maintenance). Certaines exceptions pourraient toutefois empêcher votre organisation de remplacer les composants système et les logiciels non pris en charge. À titre d'exemple, vous utilisez peut-être des systèmes non pris en charge qui fournissent des capacités essentielles aux activités, mais il est impossible de se procurer des technologies plus récentes pour les remplacer.

Il est important que votre organisation dispose d'un cycle de vie des systèmes TI. Le recours à un cycle de vie permet à votre organisation de gérer efficacement l'élimination de ses vieux systèmes et logiciels qui ne sont plus pris en charge, de même que la mise en œuvre de logiciels modernes. L'utilisation de logiciels non pris en charge expose votre organisation à des risques importants et n'est pas recommandée. Si votre organisation accepte ces risques, vous devriez consigner la justification et l'approbation de leur utilisation continue.

5.1 Autres sources de soutien

Lorsque le développeur, fournisseur ou fabricant d'origine ne fournit plus de soutien, votre organisation peut choisir d'établir un soutien en interne. Votre organisation peut, par exemple, développer des correctifs personnalisés pour les principaux composants logiciels ou faire appel aux services d'un fournisseur externe (p. ex. fournisseur de logiciels de source ouverte) qui fournira un soutien continu pour les systèmes et logiciels non pris en charge.

Il est recommandé de réaliser une évaluation des risques relatifs à l'utilisation continue des logiciels non pris en charge en ce qui a trait aux vulnérabilités de sécurité possibles. Au bout du compte, votre organisation devrait entamer un processus visant à abandonner les systèmes et les logiciels qui ne sont plus pris en charge et à migrer vers des produits pris en charge.

Vous devriez également prendre en compte les appareils mobiles qui sont utilisés par votre organisation et sur lesquels des applications ont été installées à des fins personnelles. Même si vous n'êtes pas responsable du soutien de ces applications, puisqu'elles n'ont pas été conçues à des fins opérationnelles, leur présence sur les appareils mobiles organisationnels peut augmenter les risques pour votre organisation. Si vous avez autorisé les applications installées à des fins personnelles (p. ex. vous avez adopté un modèle Prenez vos appareils personnels [PAP]), l'utilisateur devrait être tenu responsable du suivi des vulnérabilités et de l'installation des mises à jour pour ces applications dès qu'elles sont offertes. Si les risques associés à ces applications sont trop élevés pour votre organisation, envisagez de déployer un modèle différent ou des contrôles tels que des stratégies et des procédures permettant de veiller à ce que les utilisateurs appliquent les correctifs appropriés et retirent les applications lorsqu'elles ne sont plus prises en charge par le développeur.

6 Sommaire

L'une de nos 10 mesures de sécurité des TI recommandées consiste à appliquer les correctifs aux systèmes d'exploitation et aux applications. Le présent document énonce nos pratiques exemplaires en matière d'application des correctifs. Ces pratiques exemplaires sont fondées sur les contrôles de sécurité CM-2, SI-2 et SA-22, lesquels sont décrits à l'annexe A du présent document. L'application des correctifs réduit l'exposition de votre organisation aux menaces qui pourraient exploiter des vulnérabilités publiques et compromettre vos réseaux, vos systèmes et vos actifs TI.

Elle n'est cependant 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].

6.1 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, veuillez communiquer par téléphone ou par courriel avec le :

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

7 Contenu complémentaire

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

Acronyme ou sigle	Expression au long
CM	Gestion des configurations (code de la famille de contrôles de sécurité)
CVE	Vulnérabilités et expositions courantes (*Common Vulnerabilities and Exposures*)
CVSS	Système de notation des vulnérabilités courantes (*Common Vulnerability Scoring System*)
CWE	*Common Weakness Enumeration*
SA	Acquisition des systèmes et des services (code de la famille de contrôles de sécurité)
SI	Intégrité de l'information et des systèmes (code de la famille de contrôles de sécurité)
TI	Technologies de l'information

7.2 Glossaire

Terme ou expression	Définition
Actif TI	Composants d'un système d'information, ce qui comprend les applications opérationnelles, les données, le matériel et les logiciels.
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.
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.
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 technique	Classe de contrôles de sécurité 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.
Contrôle de sécurité opérationnel	Classe de contrôles de sécurité qui sont principalement mis en œuvre et exécutés par des personnes, mais habituellement fondés sur l'utilisation de la technologie, par exemple, un logiciel de soutien.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un appareil.
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.

Terme ou expression	Définition
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.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs et à l'information TI.
Risque	Degré de probabilité qu'un auteur de menace exploite une vulnérabilité pour accéder à des actifs TI ou pour les compromettre, 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 actifs ou les activités d'une organisation.

7.3 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*, octobre 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*, décembre 2014.
3	Centre canadien pour la cybersécurité. *ITSM.50.062, Gestion des risques liés à la sécurité infonuagique*.
4	Centre canadien pour la cybersécurité. *ITSM.50.030, Facteurs à considérer par les clients de services gérés en matière de cybersécurité*.

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

A.1 Contrôles de sécurité opérationnels : Gestion des configurations

Le tableau 3 décrit les contrôles de gestion des configurations (CM) mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 3 : Contrôles de sécurité opérationnels de l'ITSG-33 : Gestion des configurations (CM)

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
CM-2	Configuration de référence	(A) L'organisation élabore et consigne la configuration de référence à jour du système d'information. Cette configuration de référence est tenue à jour dans le cadre du contrôle des configurations.	**Examens et mises à jour :** L'organisation examine et met à jour la configuration de référence du système d'information : i. [*fréquence définie par l'organisation*]; ii. au besoin, selon [*circonstances définies par l'organisation*]; iii. lors des installations et des mises à niveau des composants du système d'information. Voir le contrôle connexe CM-5.	CM-3 CM-6 CM-8 CM-9 SA-10
			Automatisation du soutien aux fins d'exactitude et d'actualité : L'organisation utilise des mécanismes automatisés pour assurer le maintien d'une configuration de référence à jour, complète, exacte et facilement accessible. Voir les contrôles connexes CM-7 et RA-5.	
			Conservation des configurations antérieures : L'organisation conserve [*versions de configuration de référence antérieures définies par l'organisation*] pour permettre le retour à la version précédente.	
			Environnements de test et de développement : L'organisation conserve pour les environnements de développement et de tests des systèmes d'information une configuration de référence gérée séparément de la configuration de référence opérationnelle. Voir les contrôles connexes CM-4, SC-3 et SC-7.	

			Configuration de systèmes, de composants ou de dispositifs pour des secteurs à risques élevés : i. L'organisation remet [*systèmes d'information, composants de système ou dispositifs définis par l'organisation*] dotés de [*configurations définies par l'organisation*] aux personnes qui se rendent dans des endroits que l'organisation juge très risqués. ii. L'organisation applique [*mesures de protection de sécurité définies par l'organisation*] aux dispositifs lors du retour de ces personnes.	

A.2 Contrôles de sécurité opérationnels : Intégrité de l'information et des systèmes

Le tableau 4 décrit les contrôles d'intégrité de l'information et des systèmes (SI) mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 4 : Contrôles de sécurité de gestion de l'ITSG-33 : Intégrité de l'information et des systèmes (SI)

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SI-2	Correction des défauts	(A) L'organisation identifie, signale et corrige les défauts du système d'information. (B) L'organisation, avant leur installation, teste les mises à jour logicielles visant la correction des défauts pour en vérifier l'efficacité et les répercussions potentielles sur ses systèmes d'information. (C) L'organisation installe les mises à jour de sécurité appropriées des logiciels et des micrologiciels dans un délai de [*délai défini par l'organisation*] après la diffusion des mises à jour. (D) L'organisation intègre la correction des défauts à son processus de gestion des configurations.	**Gestion centrale :** L'organisation centralise la gestion du processus de correction des anomalies. **Automatisation des correctifs d'anomalies :** L'organisation utilise des mécanismes automatisés [*fréquence définie par l'organisation*] pour déterminer l'état des composants du système d'information en ce qui concerne la correction des défauts. Contrôles connexes : CM-6 et SI-4. **Délais de correction des anomalies et repères liés aux mesures correctives :** L'organisation : i. mesure le temps écoulé entre la détection de l'anomalie et la correction de l'anomalie; ii. fixe [*repères définis par l'organisation*] pour la prise de mesures correctives. **Mises à jour logicielles ou micrologicielles automatiques :** L'organisation installe [*mises à jour logicielles et micrologicielles pertinentes en matière de sécurité définies par l'organisation*] automatiquement à [*composants du système d'information définis par l'organisation*]. **Suppression des versions antérieures des logiciels ou des micrologiciels :** L'organisation doit supprimer [*éléments logiciels et micrologiciels définis par l'organisation*] une fois qu'une version mise à jour a été installée.	CA-2 CA-7 CM-3 CM-5 CM-8 MA-2 IR-4 RA-5 SA-10 SA-11 SI-11

A.3 Contrôles de sécurité de gestion : Acquisition des systèmes et des services

Le tableau 5 décrit les contrôles d'acquisition des systèmes et des services (SA) mentionnés à l'annexe 3A de l'ITSG-33 [2].

Tableau 5 : Contrôles de sécurité opérationnels de l'ITSG-33 : Acquisition des systèmes et des services (SA)

Numéro	Contrôle	Exigence	Améliorations du contrôle	Contrôles de l'ITSG-33 connexes
SA-22	Composants système non pris en charge	(A) L'organisation remplace les composants des systèmes d'information, lorsque la prise en charge de ces mêmes composants n'est plus offerte par le développeur, le fournisseur ou le fabricant. (B) L'organisation justifie et documente l'approbation relative à la continuation de l'usage de composants de systèmes qui ne sont plus pris en charge, mais qui continuent de répondre aux besoins des missions ou des opérations.	**Solution de rechange visant à assurer la continuité du soutien :** L'organisation fournit [*Sélection (un ou plusieurs) : soutien en interne; [Affectation : soutien de fournisseurs externes défini par l'organisation*]] pour les composants de systèmes d'information non pris en charge.	PL-2 SA-3