Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Choisir la solution de cybersécurité qui convient le mieux à votre organisation

Série Gestionnaires

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

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

Le présent document entre en vigueur le 3 octobre 2022.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	3 octobre 2022

ISBN 978-0-660-45677-5
CAT D97-4/10-023-2022F-PDF

Vue d'ensemble

À mesure que les technologies évoluent et deviennent de plus en plus sophistiquées, les auteurs de menace cherchent de nouvelles façons d'exploiter les particuliers et les organisations. Être victime d'une cyberattaque peut entraîner des conséquences dévastatrices, voire irréversibles. En raison de ces menaces en évolution, les organisations de toutes tailles pourraient avoir des difficultés à trouver des solutions de sécurité adaptées à leur budget, à leurs cyberenvironnements et à leurs besoins opérationnels.

Le présent document traite des diverses options que les organisations de toutes tailles peuvent envisager lorsqu'elles cherchent à renforcer leur posture de cybersécurité. Il présente les pratiques exemplaires de base en matière de cybersécurité que les organisations peuvent mettre en œuvre avec leurs ressources en place, ainsi que les pratiques qui peuvent être mises en œuvre en faisant appel à un fournisseur de services de sécurité gérés (FSSG). Les FSSG offrent divers services de cybersécurité, notamment la sécurité des réseaux, la protection des terminaux et la surveillance connexe. Outre les services de sécurité de l'information, les FSSG peuvent héberger, déployer, surveiller et gérer les infrastructures de sécurité de leurs clients.

Les pratiques exemplaires et les contrôles de cybersécurité présentés dans ce document s'adressent aux organisations de toutes tailles. Nous présentons les cinq contrôles de sécurité de base que n'importe quelle organisation peut mettre en œuvre au moyen des ressources disponibles et qui lui permettront d'améliorer sa posture de cybersécurité. Plusieurs autres contrôles de sécurité à mettre en œuvre dans l'organisation sont définis en tenant compte de différents niveaux de ressources et de connaissances techniques nécessaires. Pour les organisations qui ne disposent pas d'un service technique, mais qui ont les moyens d'investir dans la cybersécurité, l'externalisation de certains ou de tous les besoins de l'organisation en matière de cybersécurité à des tiers, comme un FSSG, peut améliorer la résilience et la protection de l'organisation contre des cyberincidents.

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

contact@cyber.gc.ca

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

Table des matières

Liste des tableaux

1 Introduction

Compte tenu du contexte de cybermenace en constante évolution et du nombre sans cesse croissant de cyberattaques, les organisations de toutes tailles et de tous les secteurs d'activités font face à des menaces accrues et plus complexes. Les préjudices causés par les auteurs de menace peuvent s'avérer désastreux, coûteux et parfois irréversibles. Chaque organisation, indépendamment de sa taille, est exposée à des menaces liées à la cybersécurité. Parmi les cyberattaques courantes auxquelles font face les organisations, notons les suivantes :

- **Hameçonnage** : Procédé par lequel des auteurs de menace tentent de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les usurpant ou en imitant une marque commerciale connue dans le but de réaliser des gains financiers. Les hameçonneurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de carte de crédit, informations bancaires en ligne ou autres renseignements) afin de s'en servir pour commettre des actes frauduleux.
- **Maliciel :** Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement de son propriétaire. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
- **Menace interne :** Une menace interne provient de quiconque a une connaissance de l'infrastructure et des renseignements de votre organisation ou y a accès, et qui les utilise, sciemment ou par inadvertance, pour causer des préjudices.
- **Rançongiciel :** Type de maliciel qui empêche tout utilisateur légitime d'accéder à ses fichiers jusqu'à ce que l'utilisateur verse une somme d'argent.
- **Attaque par bourrage de justificatifs d'identité :** Cyberattaque au cours de laquelle des justificatifs de compte sont utilisés pour obtenir un accès non autorisé à des comptes d'utilisateur par l'entremise de demandes de connexion automatisées à grande échelle dirigées contre une application Web.

Les cybercriminels ciblent des organisations de toutes tailles; toutefois, un grand nombre de petites et moyennes organisations croient que leurs données et leurs biens ont peu de valeur ou présentent peu d'intérêt pour les cybercriminels. Les cybercriminels ciblent les petites et moyennes organisations parce qu'elles :

- manquent de ressources adéquates en cybersécurité pour protéger leurs renseignements, ce qui en fait des cibles faciles à pirater;
- ne font peut-être pas de sauvegardes de leurs données, ce qui les rend vulnérables face aux menaces de rançon;
- stockent des données importantes, comme des renseignements personnels et financiers;
- constituent une porte d'entrée aux plus grandes organisations qui offrent des services et des fournitures à partir de ces organisations de plus petites tailles.

Selon l'Évaluation des cybermenaces nationales 2020, la cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les organisations canadiennes [1]. Si vous avez été ciblé et que vos systèmes ont fait l'objet d'une intrusion, votre organisation pourrait subir les conséquences suivantes :

- atteinte à la réputation;
- perte de productivité;

- perturbations des opérations;
- vol de propriété intellectuelle et de données;
- frais de récupération;
- possibilité d'amendes et d'honoraires d'avocat.

En suivant les conseils décrits dans la présente publication, vous serez en mesure de renforcer la posture de cybersécurité de votre organisation. Nous présenterons des pratiques exemplaires de base en matière de cybersécurité que les organisations peuvent mettre en œuvre, en commençant par la plus facilement accessible pour les petites organisations et allant jusqu'à une gamme complète de contrôles de cybersécurité et de pratiques exemplaires s'adressant aux organisations plus grandes. Quelle que soit la taille de votre organisation, ce document vous aidera à renforcer votre posture de cybersécurité et il vous fournira des conseils sur des technologies et des services de sécurité plus complets que vous pouvez obtenir auprès de FSSG. Nous démontrerons les façons dont le recours à un FSSG peut améliorer la posture de cybersécurité de votre organisation, ainsi que votre capacité à détecter et à atténuer un cyberincident, et à vous en remettre.

2 Déterminer la posture de cybersécurité

Mettre en œuvre des mesures d'atténuation pour améliorer la sécurité de l'infrastructure, des réseaux, des systèmes et des données peut sembler presque impossible, plus particulièrement si votre organisation ne possède pas l'expertise nécessaire en interne. Certaines organisations choisissent de confier la cybersécurité à des fournisseurs tiers; toutefois, cette option pourrait ne pas être accessible à tous. L'information présentée dans cette section vous aidera à évaluer la posture de cybersécurité de votre organisation en examinant les principales pratiques exemplaires en matière de cybersécurité.

La première étape pour comprendre les exigences liées à la cybersécurité de votre organisation est d'effectuer une évaluation des risques. Celle-ci permettra de déterminer toutes vulnérabilités et priorités en matière de sécurité connues ou potentielles au sein de l'infrastructure et des référentiels, notamment en ce qui concerne vos actifs informationnels les plus sensibles. L'évaluation des risques permet de définir la présence de menaces, la source potentielle de ces menaces ainsi que les incidents que pourraient entraîner ces vulnérabilités si elles étaient exploitées. L'évaluation permet également de cerner les répercussions de diverses menaces ou de divers incidents sur votre organisation, ainsi que la probabilité de chaque scénario possible.

Dans un deuxième temps, vous devez déterminer les exigences en matière de cybersécurité propres aux fonctions, aux rôles et aux responsabilités de l'organisation. Dans le cadre de ce processus, il est essentiel de comprendre la valeur de vos actifs informationnels. Par exemple, il est possible que votre organisation conserve de l'information sensible au sujet de clients et que celle-ci nécessite une protection supplémentaire. En tant que propriétaire d'entreprise, vous êtes légalement responsable, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) [2] ou de législations provinciales similaires, de protéger les renseignements personnels des clients et de signaler au Commissariat à la protection de la vie privée du Canada toutes atteintes à la vie privée ou à la protection des données qui posent un risque de préjudice à une personne. Protéger les renseignements exclusifs contre des cyberincidents est aussi important pour conserver votre avantage concurrentiel et assurer la continuité des activités. Votre organisation a la responsabilité de protéger la confidentialité, l'intégrité et la disponibilité de vos données et de vos actifs.

Le tableau 1 donne des exemples de questions préliminaires que les organisations de toutes tailles devraient aborder dans le cadre d'une évaluation des risques.

Tableau 1 : **Questions sur l'évaluation des risques**

Numéro	Questions sur l'évaluation des risques	Réponses
1	Avez-vous une liste d'actifs (p. ex. des systèmes, des dispositifs) qui sont connectés à votre réseau?	
2	Quels sont les différents niveaux de protection nécessaires pour vos actifs?	
3	Qui a accès à ces actifs?	
4	Où sont-ils conservés?	
5	Quels contrôles de sécurité sont en place pour les protéger?	
6	Quels sont les incidents les plus probables pouvant menacer ces actifs?	
7	Avez-vous mis en place un plan d'intervention en cas d'incident (PII) (p. ex. savez-vous qui appeler et quoi faire lorsqu'un incident se produit – communications, sécurité, service juridique, dirigeants)?	

2.1 Pratiques exemplaires de base en matière de cybersécurité

Des contrôles de sécurité de base et de bonnes pratiques de cybersécurité peuvent améliorer la résilience et la protection de l'organisation contre des cyberincidents. Ces contrôles ne font pas partie d'une approche universelle à l'égard de la cybersécurité. Ils sont des lignes directrices à utiliser pour créer le propre cadre de cybersécurité de votre organisation. Ces contrôles de sécurité de base visent à aider les petites et moyennes organisations, à savoir les organisations qui comptent moins de 500 employés, à protéger leurs actifs et leurs renseignements, ainsi qu'à améliorer la résilience par l'entremise d'investissements en cybersécurité. Les contrôles de sécurité de base ont été choisis en fonction de notre analyse des tendances des activités de cybermenace et de leur répercussion sur les réseaux connectés à Internet. Les organisations qui mettent en œuvre ces recommandations pourront mieux s'attaquer aux vulnérabilités et améliorer leur protection contre les cybermenaces.

De plus, les organisations doivent déterminer les éléments de leurs systèmes d'information et de leurs actifs dont elles doivent tenir compte pour les contrôles de base. Dans ce contexte, les systèmes d'information et les actifs font référence à tous les ordinateurs, serveurs, dispositifs réseau, appareils mobiles, systèmes d'information, applications, services, applications en nuage, etc. qu'utilise une organisation pour exercer ses activités. Nous recommandons fortement aux organisations de tenir compte de tous leurs systèmes d'information et actifs (qu'ils appartiennent à l'organisation, soient sous contrat ou utilisés d'une autre manière) dans le champ d'application pour les contrôles de base.

Vous devriez délimiter et adapter ces contrôles en fonction de l'évaluation des risques, des besoins opérationnels et des exigences de l'organisation. Bien que la meilleure approche soit pour les organisations de mettre en œuvre tous les contrôles de sécurité de base, cette approche n'est pas toujours possible. Les organisations qui ne disposent pas d'un soutien technique interne adéquat ou qui ne peuvent compter que sur des ressources limitées devraient commencer par les cinq contrôles suivants pour renforcer leur posture de cybersécurité et aider à minimiser le risque de cyberincidents :

1. **Mettre en œuvre une authentification robuste des utilisateurs :** Utilisez des politiques d'authentification qui assurent un équilibre entre la sécurité et l'utilisabilité. Il faut s'assurer que les dispositifs authentifient les utilisateurs avant qu'ils n'accèdent à vos systèmes. Dans la mesure du possible, utilisez l'authentification à deux facteurs (2FA pour *Two-Factor Authentication*) ou l'authentification multifacteur (MFA pour *Multi-Factor Authentication*).
2. **Appliquer les correctifs aux systèmes d'exploitation et aux applications :** Lorsque des problèmes ou des vulnérabilités sont repérés, les fournisseurs publient des correctifs pour corriger les bogues, résoudre les vulnérabilités et améliorer l'utilisabilité ou la performance. Dans la mesure du possible, activez l'application automatique de correctifs et de mises à jour pour tous les logiciels et tout le matériel afin de prévenir l'exposition à des vulnérabilités connues.
3. **Faire des sauvegardes et chiffrer les données :** Nous recommandons aux organisations de faire régulièrement des sauvegardes de toutes les applications et de tous les renseignements commerciaux essentiels vers au moins un emplacement sécurisé externe, comme le nuage ou un disque dur externe. Les sauvegardes de données sont un élément critique pour permettre d'assurer une reprise rapide non seulement après des incidents liés à la cybersécurité comme un rançongiciel ou un maliciel, mais aussi après des catastrophes naturelles, des pannes d'équipement ou des vols. Les sauvegardes peuvent se faire en ligne ou hors ligne, et elles peuvent également être réalisées en trois itérations différentes : complète, différentielle ou incrémentielle. Conservez les sauvegardes sous forme chiffrée et sécurisée afin de protéger la confidentialité des données. Les sauvegardes ne devraient être accessibles qu'aux personnes chargées de faire des tests et d'utiliser ces sauvegardes dans le cadre d'activités de restauration. Effectuez régulièrement des tests des sauvegardes pour vous assurer de pouvoir restaurer les données, le cas échéant.
4. **Former les employés :** Adaptez vos programmes de formation pour répondre aux protocoles, aux politiques et aux procédures de cybersécurité de l'organisation. Compter sur un personnel averti peut contribuer à réduire la possibilité que surviennent des cyberincidents.
5. **Élaborer un plan d'intervention en cas d'incident :** Lorsque vous disposez d'un plan, vous pouvez rapidement faire face aux incidents, restaurer les données et les systèmes essentiels, et limiter le plus possible les interruptions de services et la perte de données. Avant de mettre en œuvre votre plan, vous devez connaître les biens, les renseignements et les systèmes qui ont de la valeur pour votre organisation. Analysez le type d'incidents que vous pourriez rencontrer et déterminez les mesures d'intervention appropriées. Déterminez les personnes qui ont les qualifications requises pour faire partie de l'équipe d'intervention et la façon d'informer l'organisation de votre plan et des politiques et procédures connexes. Pour obtenir de plus amples renseignements sur la façon d'élaborer un plan d'intervention en cas d'incident, consultez la publication *Élaborer un plan d'intervention en cas d'incident* [3].

2.2 Pratiques exemplaires avancées en matière de cybersécurité

Les contrôles de sécurité présentés dans cette section s'appuient sur les cinq contrôles de base mentionnés à la section 2.1. Ces contrôles exigences des ressources supplémentaires. Un FSSG ou d'autres services de cybersécurité tiers peuvent se charger de la gestion de ces contrôles pour votre organisation.

1. **Activer les logiciels de sécurité :** Activez des coupe-feux et installez un antivirus, un anti-maliciel et un logiciel de détection et d'intervention sur les terminaux (EDR pour *Endpoint Detection and Response*) pour contrecarrer les attaques malveillantes et assurer une protection contre les maliciels. Assurez-vous de télécharger les logiciels

auprès de fournisseurs reconnus. Installez un filtre de système d'adressage par domaines (DNS) sur vos appareils mobiles pour bloquer les sites Web malveillants et filtrer le contenu dangereux.

2. **Sécuriser les sites Web :** Protégez votre site Web et les renseignements sensibles qu'il recueille en chiffrant les données sensibles, en mettant à jour vos certificats au besoin, en utilisant des mots de passe ou des phrases passe robustes en arrière-plan et en utilisant le protocole HTTPS. Si vous avez externalisé votre site Web, assurez-vous que l'hôte a des mesures de sécurité en place qui correspondent à vos contrôles de sécurité, à vos politiques et à vos procédures internes.
3. **Sécuriser les appareils mobiles :** Choisissez un modèle de déploiement des appareils mobiles (p. ex. prenez vos appareils personnels, appareils fournis par l'entreprise) qui correspond à la posture de sécurité et aux politiques de l'organisation. Veillez à ce que les employés ne puissent utiliser que les applications approuvées par l'organisation et qu'ils ne puissent télécharger que des applications provenant de sources de confiance.
4. **Mettre en œuvre le contrôle et l'autorisation de l'accès :** Appliquez le principe du droit d'accès minimal. Ne donnez accès aux employés qu'aux fonctions et aux privilèges dont ils ont besoin pour leur travail pour ainsi éviter un accès non autorisé et des atteintes à la protection des données. Les employés ne devraient avoir accès qu'aux renseignements dont ils ont besoin pour exécuter leurs tâches. Chaque utilisateur doit détenir son propre ensemble de justificatifs de connexion, et les administrateurs doivent avoir des comptes d'administration distincts avec droits d'accès privilégiés connexes.
5. **Établir un périmètre de défense de base :** Protégez vos réseaux contre les cybermenaces en mettant en œuvre des périmètres de défense de base, comme l'utilisation d'un coupe-feu ou d'un réseau privé virtuel (RPV). Un coupe-feu peut être utilisé pour se protéger contre des intrusions extérieures en surveillant le trafic entrant et sortant, et en filtrant les sources malveillantes. Un RPV peut être utilisé lorsque les employés travaillent à distance pour sécuriser la connexion et protéger les renseignements sensibles.
6. **Configurer les dispositifs pour assurer leur sécurité :** Assurez-vous de passer en revue les paramètres par défaut des appareils et d'apporter toutes modifications nécessaires. Nous recommandons au moins de changer les mots de passe par défaut (plus particulièrement les mots de passe administratifs) et de désactiver les services de localisation ainsi que les fonctions inutiles.
7. **Sécuriser les supports amovibles :** Les supports amovibles, comme les clés USB, sont un moyen pratique et économique de stocker et de transférer des données, mais il est possible de les perdre ou de se les faire voler. Votre organisation devrait utiliser des dispositifs de stockage amovibles chiffrés, conserver un inventaire de tous les actifs et nettoyer correctement les dispositifs avant de les réutiliser ou de les mettre hors service.

Le dernier contrôle en est un que l'organisation doit bien comprendre et mettre en œuvre lors de l'externalisation d'une partie ou de la totalité de la cybersécurité.

8. **Sécuriser les services infonuagiques et externalisés :** Assurez-vous d'effectuer des recherches sur un fournisseur de services avant de conclure une entente avec celui-ci et de vous procurer ses produits ou services.
   Vos recherches doivent déterminer si le fournisseur de services a des mesures en place pouvant répondre à vos exigences en matière de sécurité pour soutenir les besoins de l'organisation. Lorsque vous travaillez avec un fournisseur de services infonuagiques (FSI), il est important de bien comprendre ses stratégies de gestion des données, notamment de savoir où se trouvent ses centres de données, car il existe différentes lois internationales en matière de protection de la vie privée et différentes exigences en matière de protection des données que vous ne connaissez peut-être pas.

Pour obtenir de plus amples renseignements sur ces contrôles de sécurité, veuillez consulter la publication *Contrôles de cybersécurité de base pour les petites et moyennes organisations* [4].

Outre ces contrôles de base, les organisations peuvent également engager des fournisseurs de services de sécurité gérés (FSSG) qui sauront leur offrir des avis et des conseils plus détaillés, ainsi que leur présenter des mesures de sécurité concrètes à mettre en œuvre pour améliorer la posture de cybersécurité de chaque organisation. La section 3 fournit des précisions sur les services qu'offrent ces fournisseurs et sur les facteurs que votre organisation doit prendre en compte avant de faire l'acquisition de leurs services.

3 Externaliser la cybersécurité

Choisir des solutions efficaces de sécurité et de gestion des risques pour protéger l'organisation contre des attaques et pour sécuriser ses données est essentiel pour assurer la posture de cybersécurité de l'organisation. Certaines organisations préfèrent sous-traiter à un tiers une partie ou la totalité de leurs obligations en matière de cybersécurité. Il s'agit d'une pratique courante pour les organisations de toutes les tailles.

De nombreux services professionnels de cybersécurité sont offerts. Ils devraient tous être en mesure d'élaborer un plan de cybersécurité efficace qui saura profiter à votre organisation. La mise en œuvre de votre plan sera avantageuse pour votre organisation de bien des façons, notamment :

- réduire le risque et l'incidence potentielle de cyberattaques;
- protéger les systèmes, réseaux et technologies contre toute exploitation;
- empêcher des tiers indésirables d'accéder à de l'information sensible;
- se protéger contre des interruptions de services;
- maintenir la productivité tout en réduisant les temps d'arrêt causés par des maliciels;
- permettre une meilleure continuité des activités.

3.1 Fournisseur d'accès Internet (FAI)

Le niveau de protection ainsi que le coût associé à la mise en œuvre et au maintien des contrôles de cybersécurité varient selon la nature et les exigences de l'organisation. Bien que le recours à des services externalisés puisse s'avérer avantageux, les coûts peuvent être jugés trop onéreux pour certaines organisations. Si l'embauche d'une entreprise de sécurité comme un FSSG n'est pas une option envisageable pour l'organisation, vous devriez consulter votre FAI pour voir s'il offre des services de cybersécurité. Par exemple, beaucoup de FAI fournissent à leurs clients des antivirus, des anti-maliciels et des coupe-feux comme service complémentaire moyennant des frais supplémentaires.

La liste suivante énumère certaines des questions à poser à un FAI lorsque vous désirez ajouter des services de sécurité complémentaires au réseau de votre organisation.

- Offrez-vous des systèmes de prévention d'intrusion?

- Pouvez-vous détecter des cyberintrusions à mesure qu'elles se forment et avant qu'elles n'atteignent leurs cibles?
- Offrez-vous la détection de maliciel?
- Pouvez-vous détecter et bloquer la mystification d'adresses IP?
- Envoyez-vous aux utilisateurs des notifications concernant des infections ou des intrusions (p. ex. un réseau de zombies)?

3.2 Consultant en sécurité des TI ou en cybersécurité

Il n'est pas toujours évident de comprendre clairement les besoins en matière de cybersécurité de votre organisation. Il est tout aussi compliqué d'établir les répercussions potentielles pour votre organisation si elle devenait victime d'un cyberincident. Un consultant en sécurité des TI ou en cybersécurité peut vous aider à déterminer les domaines de la sécurité qui exigent une attention particulière et à savoir comment vous devriez prioriser la mise en œuvre de vos contrôles de sécurité et de vos mesures de suivi.

Souvent, un client embauche un consultant en sécurité des TI ou en cybersécurité pour :

- effectuer une évaluation exhaustive des risques de l'organisation;
- tester les mesures de sécurité actuelles;
- évaluer les vulnérabilités liées aux logiciels, aux systèmes informatiques et aux réseaux;
- aider à concevoir et à mettre en œuvre un modèle robuste de cyberdéfense;
- fournir des recommandations et des conseils techniques;
- concevoir, bâtir et déployer des solutions de cybersécurité.

Discuter de la posture de cybersécurité de l'organisation et déterminer les mesures nécessaires pour assurer la sécurité des réseaux, des systèmes et des données vous aidera à juger de la pertinence du recours aux services d'un FSSG. Beaucoup de FSSG réaliseront également une évaluation préliminaire de votre posture de cybersécurité pour vous aider à choisir le type et le niveau de service qui conviennent le mieux à vos besoins en matière de sécurité.

3.3 Fournisseur de services infonuagiques (FSI)

Un grand nombre d'organisations migrent leur infrastructure informatique, leur stockage, leurs applications, leurs bases de données et leurs données vers le nuage. Ce choix s'explique en partie parce qu'elles manquent de ressources informatiques à temps ou parce que l'infonuagique peut aider à réduire les coûts liés à la sécurité et aux services TI. L'infonuagique peut également réduire le coût des ressources TI internes, de l'équipement, des serveurs, du stockage et de la maintenance. Beaucoup d'organisations demandent l'aide de fournisseurs de services infonuagiques, car ceux-ci peuvent offrir des environnements informatiques sur demande et évolutifs, et une plus large gamme de capacités.

Bien que les services infonuagiques soient pratiques et économiques, ils ne garantissent pas automatiquement la protection des actifs de votre organisation dans le nuage ou qui sont gérés par un FSI. En ayant recours à un FSI, vous abandonnez le contrôle direct de plusieurs aspects de la sécurité et de la vie privée, et ce faisant, vous accordez un niveau de confiance au FSI. Malgré les services infonuagiques, votre organisation demeure responsable de la protection de la confidentialité, de l'intégrité et de la disponibilité des services TI et des renseignements hébergés par le FSI. Afin de bien tirer parti de l'infonuagique, votre organisation se doit de déterminer toutes les exigences opérationnelles et de sécurité, et elle doit s'assurer que les risques liés à la sécurité sont gérés adéquatement, que les facteurs liés à la sécurité propres à

l'infonuagique sont pris en compte et que les contrôles de sécurité des services dans le nuage sont correctement évalués avant que leur utilisation soit autorisée.

En règle générale, les FSI offrent aux clients trois modèles différents de services parmi lesquels ils doivent choisir :

- **Infrastructure à la demande (IaaS pour *Infrastructure as a Service*) :** Avec un modèle de service IaaS, le consommateur profite d'une disposition lui offrant le traitement, le stockage, les réseaux et d'autres ressources informatiques fondamentales lui permettant de déployer et d'exécuter les logiciels de son choix, ce qui comprend des systèmes d'exploitation et des applications.
- **Plateforme à la demande (PaaS pour *Platform as a Service*) :** Dans un modèle de service de type PaaS, le consommateur a la capacité de déployer dans son infrastructure infonuagique des applications qu'il a créées ou acquises au moyen d'outils de programmation, de bibliothèques, de services et d'autres outils pris en charge par le fournisseur.
- **Logiciel à la demande (SaaS pour Software as a Service) :** Dans le cadre du modèle SaaS, le service offert au consommateur lui permet d'utiliser les applications du fournisseur qui sont exécutées dans une infrastructure infonuagique. Il est possible d'accéder aux applications à partir de divers dispositifs clients au moyen d'une interface client léger comme un navigateur Web (p. ex. un courriel accessible sur le Web) ou une interface de programme (p. ex. une application locale).

Afin de permettre l'adoption de l'infonuagique, le gouvernement du Canada (GC) a élaboré une approche intégrée de gestion des risques pour établir des services fondés sur l'infonuagique. Cette approche est définie dans la publication *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)* [5]. La publication traite de cette approche qui peut être appliquée à tous les services fondés sur l'infonuagique, quels que soient le modèle de déploiement infonuagique et le modèle de services infonuagiques.

Il est à noter qu'il existe des différences entre les services infonuagiques et les services gérés. La principale différence est axée sur qui a le contrôle des données et des processus. Avec les services gérés, le consommateur (p. ex. votre organisation) impose la technologie et les procédures d'exploitation. Toutefois, avec des services infonuagiques, le fournisseur de services dicte à la fois la technologie et les procédures opérationnelles offertes au consommateur, en l'occurrence, votre organisation.

3.4 Fournisseur de services de sécurité gérés (FSSG)

Les auteurs de cybermenace continuent d'améliorer leurs tactiques, et ils sont parfois capables de contourner les mesures de sécurité les plus sophistiquées. Les environnements dans lesquels évoluent les organisations font face à des risques accrus et plus complexes; et même lorsqu'elles peuvent compter sur des professionnels compétents au sein de leur personnel, les organisations risquent quand même d'être victimes de cyberattaques. Plus que jamais, les organisations de toutes les tailles sous-traitent à des FSSG une partie ou la totalité de leur cybersécurité.

Un FSSG est une firme spécialisée dans la technologie qui offre des services de cybersécurité à des entreprises et à des organisations. Les FSSG peuvent héberger des services de sécurité, déployer des logiciels et du matériel de cybersécurité, et gérer votre infrastructure de sécurité en plus d'offrir des services de sécurité de l'information (SI). Leurs services comprennent une surveillance et une gestion externalisées des dispositifs et des systèmes de sécurité, et dans certains cas, ils prennent des mesures d'atténuation sur les systèmes TI pour aider à combattre et à prévenir les compromissions.

De nombreuses raisons expliquent pourquoi les organisations choisissent de collaborer avec un FSSG. Certaines organisations peuvent ne pas avoir suffisamment de ressources internes ou de compétences dans certains domaines de la sécurité. Elles peuvent aussi avoir besoin de surveillance et de gestion de la sécurité en dehors des heures opérationnelles normales. D'autres organisations cherchent plutôt à embaucher un FSSG pour effectuer des contrôles de sécurité ou intervenir en cas d'incidents et enquêter sur ceux-ci.

Parmi les raisons évoquées pour l'embauche d'un FSSG, notons les suivantes :

- augmenter la sécurité;
- miser sur la sécurité interne pour aider à combler certaines lacunes;
- mettre en œuvre ou intégrer des technologies et des solutions de sécurité de tiers qui ont été adaptées à l'infrastructure et à l'architecture des TI;
- accroître la visibilité des menaces tout en accélérant les interventions en matière de sécurité.

Les services que peut offrir un FSSG comprennent :

- la gestion des coupe-feux, des systèmes de détection des intrusions (SDI), des technologies de défense contre les menaces et des RPV;
- l'administration des outils de gestion des informations et des événements de sécurité (GIES);
- la surveillance continue de dispositifs et de systèmes;
- les services gérés de détection et d'intervention (MDR pour *Managed Detection and Response*) comprennent la surveillance, la détection, l'alerte et la gestion de l'intervention en cas d'attaque visant les systèmes;
- la supervision de la gestion des correctifs et des mises à niveau de l'équipement et des logiciels de sécurité;
- la réalisation d'évaluations de sécurité et de contrôles de sécurité;
- la réalisation de tests de vulnérabilité et de balayages de menace pour formuler des recommandations et des conseils concernant des solutions de cybersécurité;
- la sensibilisation à la sécurité;
- l'opérationnalisation des renseignements sur les menaces.

Il est à noter qu'il existe des différences entre un fournisseur de services gérés (FSG) et un FSSG. Un FSG offre un service d'administration des technologies de l'information (TI), tandis qu'un FSSG s'occupe de la cybersécurité. Toutefois, certains FSG offrent des services de sécurité des terminaux, de sécurité réseau et de sécurité infonuagique. Si vous avez un contrat avec un FSG, vérifiez les services de sécurité qu'il offre. Une comparaison plus approfondie est offerte dans la prochaine section.

3.4.1 Différences entre un FSSG et un FSG

Un FSSG met en place au moins un centre des opérations de sécurité (COS) chargé de surveiller et de protéger la sécurité de l'infrastructure d'un client (p. ex. réseaux, applications, bases de données, serveurs). Un FSG peut avoir son propre centre d'exploitation de réseau (NOC pour *Network Operation Center*) pour veiller à ce que les opérations TI du client se déroulent bien. Il s'occupe de tous les aspects relatifs aux TI d'une organisation par abonnement, mais il pourrait ne pas fournir de surveillance liée à la sécurité dans le cadre de ce service.

Le tableau 2 met en évidence les principales différences entre un FSG et un FSSG.

Tableau 2 : **Différences entre un FSSG et un FSG**

FSSG	FSG
Privilégie les opérations de sécurité des TI.	Privilégie les opérations TI de base comme l'assistance-client, la gestion des terminaux, la gestion des sauvegardes, les réseaux et la gestion des coupe-feux.
Assure la surveillance et la défense en matière de sécurité. S'assure que les systèmes informatiques sont toujours protégés. Peut inclure le balayage et l'analyse des menaces ainsi que les services gérés de détection et d'intervention (MDR).	Surveille les réseaux et l'infrastructure TI pour s'assurer qu'ils fonctionnent bien.
Fournit l'intégration et le soutien en matière d'outil de sécurité spécialisé.	Gère, met à jour et maintient les systèmes de réseau et propose des solutions et du soutien en matière de TI.
Fournit un soutien aux opérations de sécurité, ce qui comprend la détection, les alertes et les interventions possibles.	Fournit des services et un soutien aux opérations TI, y compris l'assistance-client.
Offre une gestion des incidents et assure la continuité des activités et la reprise après catastrophe.	Assure la maintenance, fournit les correctifs et les mises à jour après la détection d'une menace.

L'objectif prioritaire d'un FSG est l'administration des TI, alors qu'un FSSG se concentre principalement sur le soutien en matière de cybersécurité. Choisir un FSSG est une décision complexe pour une organisation, et elle nécessite une recherche et une analyse approfondies. La section suivante dresse une liste des critères à prendre en compte dans le cadre des échanges avec un FSSG.

3.4.2 Critères à prendre en compte

Après avoir pris la décision d'externaliser certaines fonctions de sécurité, vous devez bien comprendre les objectifs que votre organisation cherche à réaliser. Vos objectifs en matière de sécurité doivent être définis avant de prendre une décision. Les FSSG n'offrent pas tous les mêmes gammes de services ou de capacités; voilà pourquoi vous devez choisir un fournisseur qui répond aux exigences de sécurité de votre organisation.

Lors de l'évaluation de FSSG potentiels, tenez compte des critères énumérés au tableau 3. Ces critères vous aideront à choisir un fournisseur qui possède les capacités adéquates pour assurer la protection de vos biens et de vos données.

Tableau 3 : **Liste des critères d'évaluation d'un FSSG**

Numéro	Critère
1	Le FSSG offre-t-il des gammes bien établies et reconnues de normes, de processus et de procédures de sécurité qu'il peut mettre en œuvre et suivre dans le cadre des opérations?
2	Quels services le FSSG offre-t-il à ses clients en lien à la gestion, à la surveillance, à l'intervention et au signalement d'incidents liés à la sécurité? Ces services s'intègrent-ils bien aux activités de votre organisation?
3	Le FSSG peut-il compter sur une équipe de cybersécurité d'expérience ayant des compétences et des capacités reconnues en cybersécurité? Le personnel détient-il les accréditations ou autres certifications requises?
4	Le FSSG comprend-il les normes réglementaires et de conformité de l'organisation liées aux exigences de cybersécurité?
5	Quelle technologie et quelle infrastructure utilise le FSSG pour soutenir et assurer la détection et l'intervention en cas de menaces, pour faciliter la gestion des changements sur les systèmes et pour transmettre des alertes? Ces technologies et systèmes

Numéro	Critère
	semblent-ils convenir suffisamment pour être intégrés à vos systèmes d'exploitation? Le service est-il principalement dans le nuage? Est-il sur place avec surveillance à distance? Est-il hybride?
6	Le FSSG respecte-t-il le cadre de gestion des risques liés à la sécurité des TI (p. ex. ITSG-33 [6], NIST 800-53 [7], ISO27001 [8], COBIT, CIS Controls) pour sa propre planification de la sécurité?
7	Le FSSG peut-il confirmer qu'il a des clients qui font partie de votre secteur d'activités? Peut-il fournir des références de clients travaillant dans votre secteur d'activités?
8	Le FSSG a-t-il un accord sur les niveaux de service (ANS) de base ou a-t-il un ensemble d'objectifs de niveau de service (ONS) qui définit ses engagements à l'égard des délais d'intervention ou de résolution et d'autres facteurs importants? Demandez un exemple d'ANS et examinez-le pour voir s'il satisfait vos exigences sur le plan de la rapidité de détection, d'alerte et de résolution.
9	Quels mécanismes peut-il soutenir pour les alertes? Prend-il en charge les alertes par courriel, et fournit-il un portail administratif pour le signalement? Offre-t-il les alertes mobiles (service de messages courts [SMS], applications ou autre messagerie)?
10	Le FSSG est-il en mesure de s'adapter à vos outils et logiciels de sécurité sur place? Le FSSG peut-il facilement renvoyer l'information à un dispositif de gestion des informations et des événements de sécurité (GIES) sur place, ou exploiter des données basées sur les journaux des antivus et des terminaux?
11	Comment le FSSG protège-t-il vos systèmes et vos renseignements contre des compromissions et où conserve-t-il ses journaux? Comment protège-t-il les données inactives? En transit? Comment les systèmes et les employés du FSSG se connectent-ils à vos réseaux, systèmes ou données? Comment sont-ils surveillés, contrôlés ou vérifiés? Avez-vous accès aux données de vérification? Le FSSG peut-il satisfaire vos exigences relatives à la résidence de données (le cas échéant)?
12	Comment le FSSG peut-il apporter des mesures correctives dans le cas d'une compromission? Posez des questions relatives à la réalisation d'analyses judiciaires et leur prise en charge pour les données et les services qu'il gère pour vous. Offre-t-il un soutien à l'atténuation après une intrusion, comme l'intervention d'urgence en cas d'incident?
13	Le FSSG peut-il produire un certificat d'évaluation d'un tiers en fonction de normes de sécurité (p. ex. SSAE SOCII/TYPE II, ISO 270001)?
14	Le FSSG partage-t-il des renseignements sur les menaces avec ses clients?
15	Le client obtient-il l'accès aux systèmes et aux interfaces du FSSG (tableaux de bord, interfaces de programmation d'applications [API pour *Application Programming Interface*], comptes)?
16	Qui sont les fournisseurs du FSSG?
17	Combien coûtent les divers services?

3.4.3 Avantages et désavantages d'attribuer un contrat à un FSSG

Parmi les avantages à collaborer avec un FSSG, notons :

- l'amélioration des compétences et de la couverture de votre équipe de sécurité existante;
- la réduction des coûts liés à l'embauche en interne de spécialistes qualifiés de la sécurité des TI, à la mise à jour des technologies et à la mise en œuvre d'équipements de détection de maliciel et de nouveaux programmes;
- l'accès à des experts en sécurité informatique accrédités et qualifiés, et à leurs recherches et renseignements sur les menaces;
- l'accès à des technologies de pointe;

- l'atténuation des menaces et des vulnérabilités en utilisant des processus hautement efficaces et une automatisation du flux de travail pour améliorer considérablement les délais de remise en état liés aux problèmes de sécurité;
- l'accès à des COS en tout temps.

Il faut également tenir compte de certains inconvénients :

- Lorsque vous décidez de collaborer avec un FSSG pour protéger vos données de gestion, vous confiez votre sécurité à des étrangers, alors que vous êtes responsable des risques encourus.
- Les FSSG sont des cibles intéressantes pour des cyberattaques, car les répercussions d'une effraction à l'égard d'un fournisseur de services peuvent entraîner une atteinte à la protection des renseignements personnels de nombreux clients en même temps. Il est important de comprendre comment vos réseaux et données, qui sont pris en charge par le fournisseur, sont protégés contre une possible compromission du fournisseur de services.
- Contrairement à une équipe TI interne, un FSSG peut ne pas toujours être au courant des nouveaux services et des modifications apportées par l'organisation.

L'atténuation des risques associés à l'utilisation de services de sécurité contractuels est une responsabilité partagée par l'organisation et le FSSG. Toutefois, votre organisation est responsable sur le plan juridique de protéger ses données, y compris les renseignements personnels, et elle doit défendre ses réseaux et ses systèmes d'information. Si votre organisation choisit d'externaliser sa cybersécurité, il est important de maintenir un dialogue ouvert avec le FSSG et de comprendre les mesures qu'il prend pour assurer la sécurité de ses activités et services. Il est également important d'avoir des communications constantes avec le FSSG afin de s'assurer que les stratégies de sécurité font l'objet d'examens et de mises à jour en fonction de vos priorités et systèmes en constante évolution.

3.5 Catégories de services de sécurité gérés

Que vous cherchiez à externaliser certains des services de cybersécurité de l'organisation ou la totalité de ceux-ci, une consultation avec un FSSG de confiance peut offrir une perspective impartiale vous permettant d'harmoniser les objectifs de l'organisation pour obtenir les meilleures solutions possibles.

Les FSSG offrent généralement des conseils adaptés sur place à leurs clients pour les tâches suivantes :

- évaluer les risques;
- déterminer les principales exigences en matière de sécurité opérationnelle;
- élaborer des politiques et des processus de sécurité;
- intégrer des technologies de sécurité;
- fournir un soutien sur place à l'atténuation après une intrusion, comme l'intervention d'urgence en cas d'incident et l'analyse judiciaire.

3.5.1 Technologies de services de sécurité gérés

Les services TI les plus courants offerts par un FSSG comprennent le déploiement, la gestion et la configuration de ce qui suit :

- systèmes de détection et de prévention des intrusions (SDPI);
- détection et intervention sur les terminaux (EDR);
- filtrage du contenu Web et du trafic;
- gestion des informations et des événements de sécurité (GIES);
- détection et intervention étendues (XDR pour *Extended Detection and Response*);
- gestion de l'identité et de l'accès (GIA);
- gestion des accès privilégiés;
- analyse et évaluation des vulnérabilités;
- gestion des correctifs;
- antivirus, antipollupostage et anti-maliciel;
- coupe-feux;
- RPV;
- prévention de la perte de données (PPD);
- renseignements sur les menaces;
- surveillance des dispositifs et des systèmes.

3.5.2 Protection des données et surveillance de la sécurité

Les FSSG offrent des services pour protéger les données, s'assurent que les dispositifs et les systèmes fonctionnent comme prévu, et identifient des menaces existantes ou imminentes. Ces services comprennent, entre autres, les suivants :

- **Anti-maliciel :** Aider à identifier et à traiter le code malveillant dans les systèmes, l'infrastructure et les applications des clients.
- **Sauvegardes et reprise après catastrophe :** Protéger les données des clients contre le risque de perte due à des atteintes à la sécurité et à d'autres perturbations. Elles permettent d'avoir une copie des données à restaurer en cas de compromission des systèmes.
- **Criminalistique numérique :** Enquêter sur les incidents liés à la sécurité afin de déterminer ce qui s'est passé et d'empêcher qu'ils se reproduisent.
- **Liste d'applications autorisées et PPD** : Distinguer les ressources connues pour être sécuritaires de celles potentiellement malveillantes.
- **Sécurité des courriels :** Atténuer le risque d'hameçonnage et d'autres types d'attaques par courriel.

Les FSSG offrent une surveillance et une interprétation quotidiennes des événements système importants dans le réseau, ce qui comprend les comportements non autorisés, les piratages malveillants, les attaques par déni de service (DoS), les anomalies et l'analyse des tendances.

3.5.3 Évaluation et gestion des risques et des vulnérabilités

Un FSSG peut aider votre organisation à identifier les vulnérabilités connues que les cybercriminels peuvent exploiter pour avoir accès aux applications, aux systèmes et aux données, à établir la priorité de ces vulnérabilités et à y remédier. Les services de gestion des vulnérabilités comprennent les évaluations des vulnérabilités des réseaux, des systèmes et des applications du client (les mesures correctives sont la responsabilité du client), ainsi que la gestion complète des vulnérabilités (y compris la détection et la correction par l'application automatisée de correctifs et la reconfiguration système).

Les FSSG fournissent les types de services en matière de découverte des risques et d'intervention suivants :

- **Analyse et correction des vulnérabilités** : Aider à identifier les vulnérabilités connues dans des applications pour les résoudre.
- **Tests de pénétration :** Simuler des attaques que les cybercriminels pourraient mener en vue d'évaluer dans quelle mesure l'infrastructure d'un client peut résister aux attaques.
- **Évaluation et contrôles de sécurité :** Cerner les mauvaises configurations pouvant mener à des failles de sécurité, ainsi que des occasions de rendre les stratégies de sécurité encore plus rigoureuses.
- **Détection d'intrusion** : Surveiller les intrusions et les tentatives d'intrusion et intervenir lorsqu'elles se produisent.
- **Chasse aux cybermenaces :** Identifier et se débarrasser des menaces dans son environnement de façon proactive à l'aide de la criminalistique informatique, de renseignements sur les menaces et de l'analyse des maliciels.

Les offres de gestion des risques peuvent comprendre la surveillance, la gestion des règles de routage du trafic du coupe-feu et la production de rapports fréquents de trafic et de gestion pour les clients. La gestion de la détection d'intrusion, au niveau du réseau ou au niveau de l'hôte, comporte non seulement l'envoi aux clients d'alertes d'intrusion, mais aussi la connaissance des nouveaux moyens de défense contre les intrusions et la production fréquente de rapports sur les tentatives d'intrusion et les activités connexes. Des services de filtrage de contenu peuvent être fournis par filtrage de courriels et par d'autres types de filtrage de trafic des données.

3.5.4 Surveillance et gestion de la conformité

Si vous êtes tenu de prouver que l'état de la sécurité de votre organisation est conforme à la réglementation du gouvernement et du secteur, vous pouvez demander au FSSG d'évaluer, de vérifier et de documenter le respect de l'organisation à l'égard de mandats de conformité précis.

En outre, le contrôle de la conformité peut inclure le contrôle des journaux d'événements pour détecter les changements, que l'on appelle parfois la « gestion des changements ». Ce service permet de relever les modifications apportées à un système qui contreviennent à une politique de sécurité officielle. En bref, il mesure la conformité à l'égard d'un modèle de risque technique.

4 Résumé

Dans la présente publication, nous offrons aux organisations de toutes les tailles des solutions de cybersécurité pouvant aider à améliorer et à renforcer leur posture de cybersécurité et à améliorer leur résilience face aux cybermenaces. Nous présentons les pratiques exemplaires et les contrôles en matière de cybersécurité que toutes les organisations, quelle que soit leur taille, devraient mettre en œuvre. Les organisations doivent déterminer si elles ont les ressources et les connaissances techniques internes nécessaires pour fournir une protection adéquate contre les cybermenaces ou si elles devront confier à un tiers, comme un FSSG, une partie ou la totalité de leurs besoins en matière de cybersécurité.
L'objectif global est de créer et de maintenir une solide posture de cybersécurité en établissant une solution dynamique de cybersécurité.

5 Contenu complémentaire

5.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Expression au long
2FA	Authentification à deux facteurs
RPV	Réseaux privés virtuels
XDR	Détection et intervention étendues (*Extended Detection and Response*)
ANS	Accord sur les niveaux de service
ONS	Objectif de niveau de service
COS	Centre des opérations de sécurité
CIS	*Center for Internet Security*
PPD	Prévention de la perte de données
DNS	Système d'adressage par domaines (*Domain Name System*)
DoS	Déni de service (*Denial of Service*)
EDR	Détection et intervention sur les terminaux (*Endpoint Detection and Response*)
GIA	Gestion de l'identité et de l'accès
IaaS	Infrastructure à la demande (*Infrastructure as a Service*)
SDPI	Systèmes de détection et de prévention des intrusions
SDI	Systèmes de détection des intrusions
FSG	Fournisseur de services gérés
FSSG	Fournisseur de services de sécurité gérés
GIES	Gestion des informations et des événements de sécurité
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
PaaS	Plateforme à la demande (*Platform as a Service*)
SaaS	Logiciel à la demande (*Software as a Service*)
MDR	Services gérés de détection et d'intervention (*Managed Detection and Response*)
MFA	Authentification multifacteur (*Multifactor Authentication*)
NIST	*National Institute of Standards and Technology* (États-Unis)
COR	Centre des opérations de réseau
PII	Plan d'intervention en cas d'incident
FAI	Fournisseur d'accès Internet
SI	Sécurité de l'information
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
TI	Technologies de l'information

5.2 Glossaire

Terme	Définition
Application de correctifs	Acte d'appliquer des mises à jour aux logiciels et aux micrologiciels.
Atteinte à la protection des données	Incident de cybersécurité dans lequel une personne prend des renseignements sensibles sans l'autorisation du propriétaire.
Atteinte à la vie privée	Incident qui implique la collecte, l'utilisation ou la divulgation non autorisée de renseignements personnels. Une telle pratique est « non autorisée » si elle contrevient à la *Loi sur la protection des renseignements personnels*. Une atteinte peut découler d'erreurs accidentelles ou d'interventions malveillantes de la part d'employés, d'agents, d'entrepreneurs, de tiers, de partenaires ayant une entente de communication d'information en place ou d'intrus.
Cheval de Troie	Programme malveillant déguisé en logiciel légitime ou qui y est intégré.
Chiffrement	Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Contrôle d'accès basé sur les rôles	Ensemble d'autorisations d'accès que reçoit un utilisateur en fonction d'une hypothèse explicite ou implicite d'un rôle donné. Les autorisations de rôles peuvent être héritées au moyen d'une hiérarchie de rôles et reflètent en général les autorisations nécessaires pour exécuter des fonctions définies au sein de l'organisation. Un rôle donné peut s'appliquer à une seule ou à plusieurs personnes.
Contrôle de la 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 politiques, des pratiques et des procédures de sécurité.
Contrôles de sécurité de base	Mécanismes de protection qui sont définis dans les instruments de politique du Secrétariat du Conseil du Trésor du Canada (SCT) et qui constituent la norme minimale que les ministères doivent appliquer à leurs fonctions de sécurité des TI et à leurs systèmes d'information.
Coupe-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre.
Cybercrime	Crime perpétré au moyen d'ordinateurs ou de réseaux informatiques.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Droit d'accès minimal	Principe selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation accidentelle, incorrecte ou non autorisée d'un système d'information.

Terme	Définition
Évaluation des risques	Processus d'identification, d'analyse et de priorisation des risques liés aux opérations de l'organisation. Ce processus aide à déterminer les contrôles de cybersécurité nécessaires en fonction du niveau de risque de l'organisation.
Information sensible	Information qui doit être protégée contre toute divulgation non autorisée.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Logiciel espion	Logiciel indésirable qui s'installe dans un dispositif informatique dans le but de voler des données relatives à l'utilisation d'Internet et de l'information sensible.
Logiciel publicitaire	Logiciel soutenu par la publicité qui affiche à l'écran d'un utilisateur des publicités non sollicitées.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice à l'information et aux actifs TI.
Préjudice	Dommages que subissent les organisations à la suite d'une compromission de leurs systèmes d'information et de leurs actifs TI.
Propriété intellectuelle	Droits légaux qui découlent de l'activité intellectuelle dans les domaines industriel, scientifique, littéraire et artistique. Des exemples incluent les droits d'auteur, les marques de commerce et les brevets.
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.
Renseignements personnels	Renseignements concernant une personne identifiable, quelle que soit leur forme, au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*.
Réseau de zombies	Plusieurs dispositifs connectés à Internet et infectés par un maliciel contrôlés par des utilisateurs malveillants.
Réseau privé virtuel	Réseau de communication privé généralement utilisé au sein d'une organisation ou entre plusieurs entreprises ou organisations diverses pour communiquer sur un réseau élargi. Les communications sur le RPV sont habituellement chiffrées ou codées pour protéger le trafic provenant des autres utilisateurs, qui est transmis sur le réseau public ayant recours au RPV.
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, et causent des dommages de toutes sortes. Ils peuvent faire afficher des messages irritants, voler des données ou même permettre à d'autres utilisateurs de prendre le contrôle de l'ordinateur infecté.
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.

5.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. *Évaluation des cybermenaces nationales 2020*, 16 novembre 2020.
2	Commissariat à la protection de la vie privée du Canada. *La Loi sur la protection des renseignements personnels et les documents électroniques*, février 2021.
3	Centre canadien pour la cybersécurité. *Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)*, février 2022.
4	Centre canadien pour la cybersécurité. *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, février 2020.
5	Centre canadien pour la cybersécurité. *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)*, mars 2019.
6	Centre canadien pour la cybersécurité. *Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*, décembre 2014.
7	National Institute of Standards and Technology. *NIST Risk Management Framework*, décembre 2020.
8	Organisation internationale de normalisation. *ISO 27001: Information Security Management*, 2018.