Centre de la sécurité des télécommunications | Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Facteurs à considérer par les clients de services gérés en matière de cybersécurité

GESTION

ITSM.50.030

TLP:WHITE

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, envoyez un courriel ou téléphonez à notre Centre d'appel :

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

DATE D'ENTRÉE EN VIGUEUR

La présente publication entre en vigueur le 14 octobre 2020.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première diffusion.	14 octobre 2020

SURVOL

Ce document présente divers points qu'il convient de prendre en considération sur le plan de la sécurité avant et durant le processus d'acquisition de services gérés. Chaque section comprend une liste de vérification des mesures que vous devriez prendre et des questions que vous devriez poser à un fournisseur avant d'avoir recours à ces services.

Vous pouvez utiliser ce document comme point de départ lorsque vous discutez de la sécurité des services au sein de votre organisation. Nous avons inclus des facteurs à considérer pour vous aider à définir vos besoins opérationnels et vos exigences de sécurité, ainsi que les niveaux de service auxquels vous vous attendez dans le cadre des services gérés.

Pour obtenir de plus amples renseignements, communiquez avec notre Centre d'appel par téléphone ou par courriel :

Centre d'appel
contact@cyber.gc.ca
613-991-8700
Sans frais : 1-833-CYBER-88 (1-833-292-3788)

TABLE DES MATIÈRES

LISTE DES TABLEAUX

1 INTRODUCTION

Les petites et moyennes entreprises pourraient vouloir faire appel à des fournisseurs de services pour gérer à distance l'infrastructure de technologies de l'information (TI), la cybersécurité et d'autres activités opérationnelles connexes de leur organisation. Toutefois, les fournisseurs de services gérés (FSG) sont des cibles attrayantes aux yeux des cybercriminels, car ils ont accès à de nombreux systèmes client et à une grande quantité de données. Si un FSG subit une compromission, ses clients deviennent également vulnérables; une compromission peut entraîner le vol de renseignements exclusifs et la perturbation des activités de l'entreprise, et ainsi conduire à des pertes financières et porter atteinte à la réputation d'une organisation.

Votre organisation peut utiliser ce document pour l'aider à déterminer si un FSG dispose ou non des capacités nécessaires pour fournir des services de manière efficace et sécuritaire. Ce document présente différents points liés à la sécurité dont vous devriez tenir compte avant et durant le processus d'acquisition de services de TI gérés. Il s'agit notamment des points suivants :

- sécurité des données;
- conformité juridique;
- évaluations des fournisseurs de services;
- contrôle de l'accès;
- chiffrement;
- intervention en cas d'incident;
- continuité des activités et reprise après sinistre;
- intégrité de la chaîne d'approvisionnement;
- stratégies de sortie;
- destruction de données.

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

Pour en savoir plus sur certaines pratiques exemplaires en matière de passation de marchés avec un FSG, voir *Pratiques exemplaires en matière de cybersécurité : Passation de marché avec des fournisseurs de services gérés* [1][1].

[1] Un numéro entre crochets renvoie à une référence citée dans la section « Contenu complémentaire » du présent document.

1.1 SERVICES GÉRÉS

Un FSG est une entreprise qui gère à distance l'infrastructure de TI et les systèmes utilisateur au nom d'un client. Selon la MSP Alliance, les FSG présentent habituellement les caractéristiques distinctives suivantes :

- ils fournissent des services de centre d'exploitation du réseau (NOC pour *Network Operations Centre*) et de dépannage;
- ils surveillent et gèrent à distance la totalité ou la plupart des objets pour le compte du client;
- ils effectuent la maintenance proactive des objets qu'ils gèrent pour le compte du client; et
- ils emploient un modèle de facturation prévisible (qui donne au client le montant total exact pour les dépenses régulières liées à la gestion des TI).

Il convient de rappeler qu'il existe des différences entre les services infonuagiques et les services gérés. La principale différence concerne l'entité appelée à exercer un contrôle sur les données et les processus. Dans le cas des services gérés, le **client** (votre organisation) dicte la technologie et les procédures d'exploitation. Cependant, dans le cas des services infonuagiques, le **fournisseur de services** dicte à la fois la technologie et les procédures d'exploitation accessibles au client (votre organisation).

Dans le présent document, nous supposons que votre organisation aura recours au moins en partie à l'infrastructure infonuagique.

2 FACTEURS À CONSIDÉRER PAR LES CLIENTS

Pour chaque point abordé dans cette section, nous incluons une description vous donnant plus de contexte, une explication des raisons derrière l'importance du sujet, et une liste de vérification des activités et des questions qui vous aideront à déterminer si un FSG convient ou non à votre organisation. Selon les besoins opérationnels de votre organisation, certains points liés à la sécurité pourraient être plus pertinents que d'autres.

Veuillez noter que ce document ne vous aide pas à déterminer les besoins opérationnels de votre organisation; ils sont propres à votre environnement organisationnel et à vos circonstances.

2.1 SÉCURITÉ DES DONNÉES

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

On mesure la sensibilité des données par l'incidence qu'aurait une compromission sur la capacité de votre organisation à s'acquitter de son mandat. On classifie la sensibilité des données selon trois niveaux :

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

La sensibilité des données tient compte de l'incidence de la compromission sur la confidentialité, l'intégrité et la disponibilité des données, soit les trois piliers de la sécurité des TI. La confidentialité protège l'information contre la divulgation non autorisée. L'intégrité protège l'information contre les changements non autorisés. La disponibilité garantit que l'information est accessible lorsqu'on en a besoin. Vous devez appliquer des valeurs élevées, moyennes et faibles à chacun de ces trois volets afin de construire un *profil de sécurité des données* tripartite.

Prenons comme exemple un ensemble de données dont le profil de sécurité des données est E/M/F. Vous pouvez interpréter les trois caractéristiques du profil de sécurité des données de la façon suivante :

1. Une **compromission touchant la confidentialité des données** (E) aurait une incidence cruciale ou prohibitive sur la capacité de votre organisation à s'acquitter de son mandat.
2. Une **compromission touchant l'intégrité des données** (M) aurait une importante incidence sur la capacité de votre organisation à s'acquitter de son mandat.
3. Une **compromission touchant la disponibilité des données** (F) aurait une incidence modérée sur la capacité de votre organisation à s'acquitter de son mandat.

La classification des données peut changer selon le moment où elles sont produites. Par exemple, le degré de sensibilité des données sur les résultats d'une élection est beaucoup plus élevé le jour même de l'élection que le lendemain. Nous vous

recommandons de catégoriser vos données en fonction du degré de préjudice attendu le plus élevé qui pourrait résulter de la compromission de ces données. Voir l'annexe 1 du guide *ITSG-33, Gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2] pour obtenir de plus amples renseignements sur la classification et la catégorisation de vos données.

Tableau 1 : Activités des clients associées à la sécurité des données

Numéro	Activité des clients	Cocher
1	Définissez ce que les degrés de sensibilité *élevé, moyen* et *faible* signifient pour votre organisation. **Remarque :** Reportez-vous aux définitions génériques à la section 2.1.	
2	Indiquez l'information que votre organisation protège (c.-à-d. l'information sur la stratégie organisationnelle, les données personnelles sur les Canadiens, les transactions financières). **Remarque** : Vous pouvez regrouper les données comme suit : Données accessibles au public, données opérationnelles, secrets commerciaux. Déterminez qui (rôle) doit avoir accès à ces données.	
3	Déterminez où les données sont stockées (c.-à-d. à l'interne ou auprès du fournisseur de services).	
4	Relevez les données très sensibles. **Remarque :** Afin de protéger les données très sensibles, vous devez vous assurer de les stocker dans l'infrastructure de votre organisation, et non auprès d'un fournisseur de services. Nous recommandons à votre organisation d'analyser le risque lié au stockage de données très sensibles à l'extérieur de son infrastructure afin de déterminer s'il s'agit d'un risque acceptable. Consultez la section 2.3.1 pour obtenir des précisions.	
5	Déterminez si une compromission potentielle des données aurait des conséquences sur les intérêts en matière de sécurité nationale. **Remarque :** Nous vous recommandons de stocker les données qui présentent une importance pour la sécurité nationale uniquement dans l'infrastructure de confiance de votre organisation, et de vous assurer que les contrôles de sécurité appropriés sont en place pour protéger ces données.	
6	Consultez l'annexe 4a du guide ITSG-33 [2] afin d'y trouver un exemple de profil de sécurité M/M/M. **Remarque :** Votre organisation doit adapter les contrôles de ce profil en fonction des résultats de cette liste de vérification et des exigences particulières de votre organisation.	
7	Créez une grille qui énumère chaque groupe de données le long de l'axe des y. Le long de l'axe des x, énumérez la confidentialité, l'intégrité et la disponibilité. Appliquez la cote « élevé », « moyen » ou « faible ». Chaque cote tripartite représente la classification des données. **Remarque :** Voir la figure 1 pour un exemple simple de grille de données.	

Groupe de données	Confidentialité	Intégrité	Disponibilité	Qui a besoin d'accès	Emplacement de stockage
Groupe de données A	Élevée	Élevée	Élevée	Administrateur de système	Réseau interne
Groupe de données B	Moyenne	Élevée	Moyenne	Finances	Fournisseur de services
Groupe de données C	Moyenne	Faible	Faible	Utilisateurs Invité	Fournisseur du système

Figure 1: Exemple de grille de données

2.2 CONFORMITÉ JURIDIQUE ET RÉGLEMENTAIRE

Lorsque des données sont stockées à l'extérieur de l'infrastructure de votre organisation, vous devez savoir où elles sont stockées (c.-à-d. l'emplacement géographique). Les données stockées à l'extérieur du Canada sont assujetties à des lois et règlements différents en matière de protection des renseignements personnels, de sécurité et de propriété des données. Selon le domaine ou le secteur auquel appartient votre organisation, les données pourraient également être assujetties à des normes et règlements différents qui régissent la conservation, la divulgation à des tiers et la chaîne de possession.

Les lois canadiennes sur la protection des renseignements personnels (c.-à-d. la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* [LPRPDE]) correspondent aux les lois sur la protection des renseignements personnels de l'Union européenne (UE) (p. ex., le *Règlement général sur la protection des données* [RGPD]). Dans le cadre des lois canadiennes et européennes, les organisations doivent absolument demander aux particuliers la permission de recueillir leurs données personnelles. Au Canada et dans l'Union européenne, les particuliers ont aussi le droit d'être oubliés[2]. D'autres pays pourraient voir la protection des renseignements personnels différemment et ne pas se conformer au RGPD, ce qui pourrait nuire à la confidentialité des données de votre organisation[3].

Si les données sont stockées à l'extérieur du Canada, des lois différentes (p. ex., les priorités en matière de sécurité nationale) pourraient avoir préséance sur les lois canadiennes sur la protection des renseignements personnels. Si vous utilisez des services gérés qui stockent des données à l'extérieur du Canada, vous devez examiner les lois applicables et les répercussions possibles sur la protection des renseignements personnels. Cette préséance pourrait nuire à la disponibilité des données des clients en cas de menace à la sécurité ou de litige.

Dans l'*Avis de mise en œuvre de la politique sur la TI : Orientation relative à la résidence des données électroniques* [3], le Secrétariat du Conseil du Trésor du Canada (SCT) exige que les données de nature délicate[4] recueillies ou traitées par le gouvernement du Canada (GC) soient stockées dans les limites géographiques du Canada ou dans les locaux d'un ministère du GC situé à l'étranger (p. ex., consulat canadien). Cette exigence garantit que le GC puisse préserver un accès continu aux données afin d'assurer la continuité des activités.

Si votre organisation n'est pas un organisme du GC, nous vous recommandons de veiller à stocker toutes les données sensibles (M/M/M ou plus) uniquement dans des centres de données situés à l'intérieur des limites géographiques du Canada. De plus, divers secteurs ont des normes et directives de conformité particulières, telles que des règlements sur la vérification, qui exigent que les données soient conservées pendant des périodes normalisées. Il incombe à votre organisation de déterminer si un FSG potentiel se conforme ou non à ces exigences.

---

[2] Le droit à l'oubli oblige les organisations qui recueillent des renseignements personnels à supprimer les renseignements personnels d'une personne qui en fait la demande.

[3] Andorre, l'Argentine, le Canada, les îles Féroé, Guernesey, Israël, l'île de Man, Jersey, la Nouvelle-Zélande, la Suisse, l'Uruguay et les États-Unis sont tous des pays non membres de l'UE ayant des lois sur la protection des données que l'UE juge adéquates. Cependant, il convient de noter que les lois des États-Unis sur la protection des renseignements personnels sont propres au secteur et ne se conforment pas au RGPD, mais le bouclier de protection des données UE-États-Unis, qui a remplacé Safe Harbour, garantit que les entreprises américaines peuvent faire des affaires dans l'UE.

[4] Données dont le profil est établi au rang M/M/M ou à un rang supérieur et données qui ont trait à la sécurité nationale.

Si vos données sont stockées à l'extérieur des locaux ou de l'infrastructure de votre organisation (c.-à-d. dans une infrastructure en nuage), il est essentiel de veiller à ce que votre organisation conserve la propriété juridique de ses données. Votre organisation est légalement responsable de la confidentialité des données. Assurez-vous de maintenir le contrôle sur ces données en conservant la propriété de ces dernières lorsqu'elles sont stockées dans une infrastructure infonuagique. Demandez à votre fournisseur!

Tableau 2 : Activités des clients associées à la conformité juridique et organisationnelle

Numéro	Activité des clients	Cocher
1	Se reporter aux degrés de sensibilité des données (élevé, moyen, faible) à la section 2.1. Votre organisation détient-elle des données classifiées à un degré de sensibilité moyen ou élevé? Si oui, nous vous recommandons de stocker ces données dans les limites géographiques du Canada.	
2	Examinez la *Loi sur la protection des renseignements personnels* (organismes du GC) ou la LPRPDE (organismes non gouvernementaux) et tout règlement propre à votre secteur pour déterminer les exigences de votre organisation en matière de manipulation et de protection des renseignements personnels.	
3	Déterminez votre politique de conservation des données. **Remarque :** Les périodes de conservation dépendent des fonctions commerciales auxquelles les renseignements se rapportent (p. ex. rétention des dossiers fiscaux pendant une période de six ans à compter de la fin de la dernière année d'imposition à laquelle ils se rapportent) et suivant que l'on considère ces renseignements comme étant transitoires ou ayant une valeur opérationnelle. L'information transitoire sert uniquement de copie de commodité. L'information de valeur opérationnelle est requise pour contrôler, appuyer ou documenter l'exécution de programmes; effectuer des opérations; prendre des décisions; ou fournir des preuves.	
Questions à poser au fournisseur de services		
1	Le fournisseur de services peut-il prendre en charge le stockage de vos données sensibles dans les limites géographiques du Canada?	
2	Le fournisseur de services peut-il respecter les exigences découlant des lignes directrices et des directives en matière de sécurité propres à votre secteur (p. ex. : conservation des données, audits et destruction)?	
3	Votre organisation conserve-t-elle la propriété juridique des données stockées dans l'espace du fournisseur de services?	
4	Lorsque les données sont stockées à l'extérieur de l'infrastructure de votre organisation, le fournisseur de services peut-il répondre à vos besoins en matière de conservation des données?	

2.3 ÉVALUATION DES FOURNISSEURS DE SERVICES ET RAPPORTS D'AUDIT

Une fois que vous avez classifié les données de votre organisation, vous pouvez comparer les exigences en matière de contrôle de sécurité de votre organisation avec la capacité du fournisseur de services d'appliquer des mesures de protection adéquates à ces données.

2.3.1 ÉVALUATION DES FOURNISSEURS DE SERVICES

On peut évaluer les fournisseurs de services sur la base de normes et de cadres de sécurité reconnus afin de déterminer leurs capacités en matière de protection de données sensibles. Voici quelques exemples de normes et de cadres de sécurité :

- Organisation internationale de normalisation (ISO) – ISO270001/2 [4];
- Information Systems Audit and Control Association (ISACA) – Control Objectives for Information and related Technologies (COBIT) [5];
- Cloud Security Alliance (CSA) – Security Trust Assurance and Risk (STAR) [6];
- National Institute of Standards and Technology (NIST) – Risk Management Framework [7];
- Notre guide ITSG-33 [2].

Nous avons élaboré des programmes d'évaluation des fournisseurs de services, qui appuient le Programme de sécurité des contrats du SCT. Nous effectuons ces évaluations en utilisant des cadres de sécurité reconnus afin d'évaluer les capacités des fournisseurs de services sur le plan de la sécurité et leur capacité de protéger les données sensibles des Canadiens.

Tableau 3 : Activités des clients associées aux évaluations des fournisseurs de services

Numéro	Activité des clients	Cocher
1	Déterminez si vous faites l'acquisition de services d'un FSG, d'un fournisseur de services infonuagiques (FSI) ou des deux. Consultez les définitions de la section 1.1.	
2	Communiquez avec nous pour déterminer si le fournisseur de services a fait l'objet d'une évaluation dans le cadre de nos programmes d'évaluation des FSG ou des FSI. **Remarque :** Vous devrez comprendre la sensibilité de vos données pour demander des résultats d'évaluation. Si nous n'avons pas évalué le fournisseur de services, vous pourriez envisager les mesures suivantes : • Demander au fournisseur de services s'il a fait l'objet d'une évaluation par un tiers sur la base de normes de sécurité (p. ex. ISO270001/2, COBIT, ITSG-33, NIST, CSA). • Retenir les services d'un tiers afin d'évaluer le fournisseur de services par rapport à la norme ISO 27001/2, au STAR de la CSA ou à des normes semblables.	
Questions à poser au fournisseur de services		
1	Le FSG peut-il produire un certificat d'évaluation d'une tierce partie par rapport à des normes de sécurité (p. ex. ISO 270001/2 ou COBIT)?	

2	Qui sont les fournisseurs du FSG? **Remarque :** La réponse à la question vous permettra de mener une évaluation indépendante.	

2.3.2 RAPPORTS DE VÉRIFICATION DES CONTRÔLES DE SÉCURITÉ

La Norme internationale de missions d'assurance (*International Standard on Assurance Engagements [ISAE] No. 3402, Assurance Reports on Controls at a Service Organization [ISAE 3402]*) [9][5] est une norme de vérification pour les contrôles qu'utilisent les organisations de services. Cette norme garantit que des contrôles de sécurité adéquats sont en place afin d'assurer l'exactitude des rapports financiers. Une tierce partie vérifie les contrôles du fournisseur de services afin de produire des rapports SOC (*System and Organization Controls*) et ainsi de démontrer la conformité du fournisseur de services à la norme ISAE-3402. Ces rapports peuvent servir à déterminer l'efficacité de la conception et de la mise en œuvre des contrôles de sécurité techniques et non techniques. Voir les descriptions des rapports SOC 2 et SOC 3 ci-dessous.

Tableau 4 : Types de rapports SOC pour la conformité ISAE-3402

Rapport	Description	Pertinence
SOC 2	Évalue les systèmes d'information d'une organisation qui sont pertinents pour la disponibilité de la sécurité, l'intégrité du traitement, ainsi que la confidentialité ou la protection des renseignements personnels. Il existe deux types de rapport SOC 2 : Type 1 : Conception des contrôles Type 2 : Efficacité de la mise en œuvre des contrôles	Le rapport SOC 2 de type 1 évalue la conception des contrôles de sécurité (c.-à-d. un moment unique dans le temps). Le rapport SOC 2 de type 2 évalue l'efficacité des contrôles de sécurité mis en œuvre au fil du temps (c.-à-d. durant une période de 6 mois et plus). Le rapport SOC 2 de type 2 tend à être le plus convoité, mais le fournisseur de services est moins susceptible de le publier, car il contient des renseignements sensibles sur la manière dont il protège les données. Cette information peut fournir des détails sur la posture de sécurité et des auteurs malveillants peuvent s'en servir pour compromettre un système. Si le FSG est disposé à partager le rapport, il le fera probablement en vertu d'une entente de non-divulgation (END).
SOC 3	Attestation du respect de la norme SSAE-16. Ne fournit aucun renseignement sur les contrôles mis à l'essai.	Un fournisseur de services est susceptible de fournir ce rapport. Ce dernier fait état de la conformité sans fournir de détails sur les contrôles utilisés.

[5] La norme internationale ISAE-3402 correspond à la norme américaine SSAE-16.

Tableau 5 : Questions relatives aux rapports de vérification de sécurité

Numéro	Questions à poser au fournisseur de services	Cocher
1	Le fournisseur de services a-t-il fait l'objet d'une vérification par un tiers indépendant à savoir s'il respecte la norme ISAE-3402? Peut-il fournir une attestation SOC 3?	
2	Le fournisseur de services est-il disposé à partager ses rapports SOC 2[6] (Type 2) si vous acceptez de signer une END?	

2.4 CONTRÔLE D'ACCÈS

Le contrôle d'accès (p. ex. une stratégie de contrôle d'accès) détermine qui peut accéder aux données, aux systèmes et aux réseaux de votre organisation. Dans ce contexte, le contrôle d'accès doit s'harmoniser avec les piliers de la confidentialité et de l'intégrité du profil de sensibilité des données décrit à la section 2.1.

La stratégie de contrôle d'accès de votre organisation doit être maintenue lorsque vous utilisez des services gérés, que les données soient stockées sur place ou dans le nuage. Lorsque vous utilisez des services gérés, votre organisation et le fournisseur de services doivent absolument s'entendre sur les rôles et les responsabilités liés au contrôle d'accès. Vous devez aussi définir les mécanismes d'authentification et d'autorisation, soit deux éléments du contrôle d'accès. L'authentification désigne tout processus ou toute mesure servant à vérifier l'identité d'un utilisateur, et l'autorisation désigne les privilèges d'accès accordés à un utilisateur, à un programme ou à un processus.

2.4.1 STRATÉGIE DE CONTRÔLE D'ACCÈS

Votre organisation est responsable de sa stratégie de contrôle d'accès. Vous devez clairement définir toutes les exigences en matière de contrôle d'accès et les communiquer au fournisseur de services afin de déterminer s'il peut répondre à ces exigences. Le contrôle d'accès doit reposer sur le **principe de droit d'accès minimal**, c'est-à-dire que les personnes ne doivent avoir que les privilèges dont elles ont réellement besoin pour s'acquitter de leurs fonctions. Les fournisseurs de services ne doivent avoir que l'accès leur permettant de gérer efficacement leurs services.

[6] Afin de protéger leur propre sécurité, certains fournisseurs de services ne fourniront pas les rapports SOC 2, même avec une END. Dans ce cas, votre organisation devra faire appel à d'autres moyens de vérification, comme nos programmes d'évaluation du FSG et du FSI.

Tableau 6 : Activités des clients associées au contrôle d'accès

Numéro	Activité des clients	Cocher
1	Si votre organisation n'a aucune stratégie de contrôle d'accès, vous devez définir vos exigences, y compris les suivantes : • Qui peut accéder aux données et à quels types de données peut-on accéder? (Voir la figure 1.) • Comment appliquera-t-on les privilèges (p. ex. rôles, accès discrétionnaire, étiquettes)? Comment les changements au contrôle d'accès seront-ils gérés?	
2	Déterminez toute autre exigence en matière de contrôle d'accès (sur la base du principe de droit d'accès minimal), comme l'examen des comptes lorsque des membres du personnel changent d'emploi ou quittent l'entreprise, et la séparation des tâches.	
3	Construisez une matrice de contrôle d'accès qui emploie des règles ou des rôles pour lier les ressources aux objets. Par exemple, créez un tableau qui distingue les rôles administratifs, tels que les administrateurs de système et les administrateurs d'applications. Veillez à tenir à jour les privilèges et à les modifier selon tout changement dans les rôles ou les fonctions du poste (p. ex. si quelqu'un n'a plus besoin de privilèges administratifs).	
Questions à poser au fournisseur de services		
1	Le FSG peut-il appuyer la stratégie de contrôle d'accès de votre organisation, notamment la façon dont les privilèges sont accordés et dont les changements sont contrôlés?	
2	De quels accès aux réseaux et aux systèmes le fournisseur de services a-t-il besoin pour exécuter ses services?	
3	De quelles données le fournisseur de services a-t-il besoin pour exécuter ses services?	
4	Votre organisation peut-elle gérer les contrôles d'accès (p. ex. attribution, révocation et maintenance de comptes) dans l'espace de service du FSG?	
5	Le fournisseur de services prend-il en charge la récupération des mots de passe en libre-service?	
6	Comment le fournisseur de services appuie-t-il le contrôle d'accès (p. ex. outils, ligne d'assistance)?	

2.4.2 ADMINISTRATEURS DE SYSTÈME ET ACCÈS PHYSIQUE AUX SERVEURS

Les administrateurs de système (AS) posent un risque de taille pour les données; en effet, les AS peuvent accéder à plusieurs clients et avoir un accès physique aux serveurs client. Parmi les autres membres du personnel qui peuvent avoir un accès physique aux serveurs, mentionnons le personnel d'entretien des installations et le personnel externe d'entretien du matériel et de maintenance des logiciels. Si des services gérés sont déployés à l'extérieur de l'infrastructure de votre organisation, il conviendra d'envisager d'autres normes qui abordent les façons dont vous pouvez limiter effectivement l'accès aux serveurs physiques par les administrateurs ou d'autres membres du personnel.

Tableau 7 : Activités des clients associées aux AS et à l'accès physique aux serveurs

Numéro	Activité des clients	Cocher
1	Consultez les rapports d'évaluation et de vérification des contrôles de sécurité du FSG; à l'aide de ces rapports, vous pouvez déterminer les contrôles des fournisseurs de services pour limiter ou contrôler l'accès des AS à vos données.	
Questions à poser au fournisseur de services		
1	Comment les données de votre organisation sont-elles protégées contre l'accès non autorisé (en lecture ou en mode modification) par les AS?	
2	Les AS sont-ils soumis à un filtrage de sécurité (p. ex. niveau d'habilitation approprié) avant qu'ils puissent accéder à votre espace en nuage?	
3	Où se trouvent les AS? Sont-ils situés au Canada, où ils sont assujettis aux lois canadiennes?	
4	Les AS sont-ils tenus de signer des END?	
5	Les AS ont-ils des droits d'accès en lecture seule aux fonctions d'audit?	
6	Le FSG peut-il fournir une piste de vérification de toutes les actions des administrateurs à des fins d'intervention en cas d'incident et de vérification générale?	
7	Les journaux d'audit permettent-ils de suivre les actions individuelles des AS?	
8	Les AS ont-ils des comptes d'utilisateur d'entreprise (servant aux tâches d'utilisateur général) et des comptes d'administrateur distincts (utilisés lorsqu'ils ont besoin de privilèges élevés pour effectuer une tâche au nom de votre organisation)?	
9	Comment le FSG gère-t-il l'accès physique aux serveurs et la responsabilisation connexe?	
10	Le FSG limite-t-il ou empêche-t-il l'accès des administrateurs locaux à un serveur physique individuel ?	
11	Quelles sont les exigences en matière d'accès physique au centre de données et aux cages de serveurs? Le centre de données est-il partagé?	
12	Le FSG fait-il appel à des fournisseurs externes pour effectuer la maintenance des systèmes ou des logiciels? Si oui, quels contrôles physiques le FSG emploie-t-il pour gérer l'accès de tiers (p. ex. escorter les personnes, les soumettre à un filtrage de sécurité pour qu'elles détiennent un certain niveau d'habilitation)?	
13	Le FSG exige-t-il que les administrateurs et le personnel de soutien suivent une formation sur la sécurité? Doivent-ils suivre cette formation de nouveau à intervalles réguliers (p. ex. une fois par année)?	

2.4.3 STRATÉGIE DE MOT DE PASSE

Si un FSG fournit des services au sein de l'infrastructure de votre organisation, le FSG doit respecter votre structure de contrôle d'accès (c.-à-d. authentification et autorisation). Toutefois, si un FSG fournit des services à l'extérieur de votre infrastructure, comme dans une infrastructure en nuage, vous devez vous assurer que le FSG prend en charge des mécanismes d'authentification correspondant au niveau de classification des données stockées.

Dans une infrastructure TI locale conventionnelle, c'est votre organisation qui établit la stratégie de mot de passe comportant les exigences minimales (p. ex. complexité, délai maximal entre les changements obligatoires de mot de passe, utilisation de phrases de passe). Les phrases de passe et les mots de passe doivent se conformer à cette stratégie. Dans le cadre de services gérés, votre organisation et le FSG doivent s'entendre sur une stratégie de mot de passe qui respecte ou dépasse les exigences de votre stratégie de mot de passe existante.

Vous avez besoin d'une stratégie de mot de passe efficace pour empêcher les auteurs de menace de deviner ou de casser facilement les mots de passe. Bien que les utilisateurs puissent trouver pénible de créer des phrases de passe et des mots de passe complexes, nous vous recommandons d'examiner les pratiques minimales définies dans la publication *Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032) [10]. Nous constatons que les normes suivantes produisent le meilleur effet dissuasif :

- Les phrases de passe doivent compter au moins 4 mots et 15 caractères;
- Les mots de passe doivent comporter au moins 12 caractères;
- Les codes de verrouillage et les NIP doivent servir uniquement si vous ne pouvez pas utiliser les phrases de passe ou les mots de passe;
    - Employez des NIP générés aléatoirement lorsqu'ils sont disponibles.

L'authentification à deux facteurs (2AF) utilise une combinaison de deux facteurs d'authentification différents lorsque vous accédez à un compte, ce qui le rend plus sécurisé. Les facteurs d'authentification doivent comprendre au moins deux types de facteurs distincts :

- **quelque chose que vous savez** (p. ex. un mot de passe ou un NIP);
- **quelque chose que vous avez** (p. ex. un jeton ou une carte à puce);
- **quelque chose que vous êtes** (p. ex. une donnée biométrique, comme une empreinte digitale).

Veuillez noter qu'un processus d'authentification qui exige un mot de passe et un NIP ne constitue pas une A2F véritable : les deux correspondent à un seul type de facteur (c.-à-d. quelque chose que vous connaissez).

En raison de la nature répandue des attaques par hameçonnage et du vol de mots de passe, de nombreux services, y compris la majorité des plateformes de médias sociaux, ont ajouté des options d'authentification à deux facteurs. Nous vous recommandons fortement d'utiliser l'authentification à deux facteurs pour l'accès à ces plateformes, surtout pour les comptes importants accessibles au public.

Tableau 8 : Activités des clients associées aux politiques sur les mots de passe

Numéro	Activité des clients	Cocher
1	Passez en revue et définissez la stratégie de votre organisation pour les mots de passe, en tenant compte de nos recommandations sur les phrases de passe et les mots de passe complexes.	
Questions à poser au fournisseur de services		
1	Le fournisseur de services peut-il appuyer la stratégie de mot de passe de votre organisation? Sinon, quelle est la stratégie du FSG et est-elle efficace?	
2	Le fournisseur peut-il prendre en charge l'A2F pour l'accès à vos données? Quelles méthodes d'authentification prend-il en charge?	

2.4.4 AUTHENTIFICATION FÉDÉRÉE

Dans une infrastructure de TI locale, l'utilisation et le stockage des mots de passe se font à l'interne seulement. Cependant, lorsque la vérification de l'identité se fait dans le nuage, la totalité des services d'authentification ou certains d'entre eux (y compris les noms d'utilisateur et les mots de passe) pourraient exister en dehors de l'infrastructure de TI interne de votre organisation. Les mots de passe représentent les « clés du royaume » parce qu'ils servent à contrôler l'accès aux données de votre organisation. Il faut protéger les mots de passe adéquatement. Comme pratique exemplaire, les mots de passe qui résident à l'extérieur de l'espace de confiance de votre organisation ne doivent jamais être stockés ou transmis en clair. De plus, aucune entité à l'extérieur de votre organisation ne doit détenir à la fois vos données et les justificatifs d'identité nécessaires pour y accéder.

Nous vous recommandons d'utiliser l'identité fédérée, qui fonctionne de la façon suivante :

1. Vous saisissez un mot de passe pour accéder aux ressources stockées à l'extérieur de l'infrastructure de votre organisation;
2. Un mécanisme d'authentification hache ce mot de passe et envoie le code haché à un service fédéré tiers qui tient les mots de passe (chiffrés) de votre organisation;
3. Le service fédéré exécute une fonction de hachage sur le mot de passe stocké et compare ce code haché à celui qu'il avait reçu afin de confirmer qu'ils se correspondent;
4. Le service fédéré génère un certificat (ou jeton) si les codes hachés se correspondent;
5. Ensuite, il envoie le certificat au fournisseur de services, ce qui vous authentifie et vous autorise à accéder aux ressources appropriées.

Un fournisseur de services infonuagiques pourra offrir des services d'authentification, mais il ne s'agit pas d'une véritable fédération, car il ne fait pas appel à un tiers. Ces services peuvent présenter un risque, car le fournisseur de services infonuagiques peut accéder à vos justificatifs d'identité et à vos données. Toutefois, il peut s'agir d'un risque raisonnable si le fournisseur de services infonuagiques dispose de processus internes qui isolent le processus d'authentification de vos données, ce qui protège ces dernières contre d'éventuels exploits. Vous devez vous assurer que si le fournisseur offre des services d'authentification, il peut attester que ceux-ci sont adéquatement isolés de vos données.

Tableau 9 : Activités des clients associées aux mécanismes d'authentification fédérée

Numéro	Activité des clients	Cocher
1	Passez en revue votre processus d'authentification actuel, s'il y a lieu.	
2	Déterminez vos exigences minimales en matière de chiffrement lorsque vous stockez des mots de passe auprès d'un tiers. Voir la section 2.5 pour connaître les lignes directrices du GC relatives au chiffrement.	
3	Demandez au fournisseur de services de vous présenter toutes les étapes de son processus d'authentification.	
Questions à poser au fournisseur de services		
1	Le fournisseur de services prend-il en charge l'authentification fédérée par l'entremise d'un tiers?	
2	Sinon, le fournisseur de services offre-t-il des services d'authentification?	
3	Si le fournisseur offre des services d'authentification, peut-il attester qu'il isole les services d'authentification (c.-à-d. les noms d'utilisateur et les mots de passe) de vos données?	
4	Le fournisseur de services respecte-t-il vos exigences minimales en matière de chiffrement des mots de passe?	
5	Quelles normes relatives au hachage et au salage le fournisseur de services infonuagiques prend-il en charge? **Remarque :** Le salage consiste à ajouter des caractères à un mot de passe pour obtenir une longueur standard, ce qui en obscurcit davantage la valeur réelle.	

2.5 CHIFFREMENT

Le chiffrement utilise une chaîne aléatoire de bits (c.-à-d. une clé de chiffrement) pour convertir des renseignements lisibles en texte chiffré illisible. Le chiffrement cache le contenu des données sensibles pour empêcher tout accès non autorisé. Le chiffrement est le mécanisme clé servant à protéger la confidentialité des données en transit dans Internet et des données inactives. Par conséquent, le chiffrement s'accorde avec le pilier de la confidentialité du profil de sensibilité des données (c.-à-d. M/M/M tel que le définit la section 2.1).

À titre de propriétaire des données, votre organisation est légalement responsable de la protection de la confidentialité de ses données sensibles. Vous devez décider du niveau de chiffrement à utiliser. Vous devez également vous assurer que le FSG peut prendre en charge le niveau de chiffrement que vous avez choisi et qu'il dispose des contrôles nécessaires pour empêcher qui que ce soit à l'extérieur de votre organisation d'accéder à vos données chiffrées ou aux clés de chiffrement permettant de déchiffrer les données.

2.5.1 CHIFFREMENT DES DONNÉES EN TRANSIT ET DES DONNÉES INACTIVES

Dès que les données sont sensibles, vous devez vous assurer d'appliquer des mesures qui les protègent dans leurs différents états, par exemple lorsqu'elles sont en transit ou inactives. Les **données en transit** sont des données actives qui se déplacent d'un endroit à un autre, comme dans Internet ou sur un réseau privé. Les **données inactives** désignent les données qui ne sont pas en déplacement. Il pourrait s'agir des données résidant dans des bases de données, des entrepôts de données, des feuilles de calcul, des archives, des copies de sauvegarde et des appareils mobiles. Vous devez tenir compte des niveaux de chiffrement à utiliser pour les données en transit (p. ex. trafic Web HTTPS) et les données inactives (p. ex. le contenu chiffré stocké dans un centre de données).

Tableau 10 : Activités des clients associées au chiffrement des données en transit et des données inactives

Numéro	Activité des clients	Cocher
1	Consultez la publication intitulée *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSAP.40.111) [11]. Cette publication comprend des recommandations pour le chiffrement des données inactives classées jusqu'à un degré de sensibilité moyen (c.-à-d. M/M/M). Afin d'obtenir des recommandations sur le chiffrement de données très sensibles, envoyez un courriel ou téléphonez à notre Centre d'appel.	
2	Consultez la publication intitulée *Conseils sur la configuration sécurisée des protocoles de réseau* (ITSP.40.062) [12]. Cette publication fournit des recommandations sur le chiffrement des données en transit classées jusqu'à un degré de sensibilité moyen (c.-à-d. M/M/M). Afin d'obtenir des recommandations sur le chiffrement de données très sensibles, envoyez un courriel ou téléphonez à notre Centre d'appel.	
Questions à poser au fournisseur de services		
1	Le FSG prend-il en charge le chiffrement (en particulier AES ou 3DES) des données inactives, conformément aux exigences de chiffrement minimales recommandées dans l'ITSP.40.111 [11]?	
2	Le FSG prend-il en charge le chiffrement des données en transit (en particulier TLS 1.2 ou HTTPS), conformément aux exigences de chiffrement minimales recommandées dans l'ITSP.40.062 [12]? **Remarque :** On recommande le protocole HTTPS par opposition au protocole HTTP, qui n'englobe pas le chiffrement du trafic Web. Il faut utiliser le protocole TLS 1.2, car les protocoles TLS 1.1 et SSL ont été retirés en raison de vulnérabilités connues.	
3	Le FSG prend-il en charge un niveau de chiffrement suffisant pour le stockage des mots de passe (recommandations dans l'ITSP.40.111 [11])?	

2.5.2 GESTION DE CLÉS À L'EXTÉRIEUR DE L'INFRASTRUCTURE DU CLIENT

Le chiffrement est le principal contrôle de sécurité servant à protéger la confidentialité des données. Il convient toutefois de noter que si vous perdez le contrôle des clés de chiffrement (c.-à-d. la chaîne aléatoire de bits servant à chiffrer et déchiffrer les données), vous perdez le contrôle des données. À titre de pratique exemplaire, vous devriez stocker les clés uniquement dans l'infrastructure interne de confiance de votre organisation. Or, pour gérer les clés de chiffrement, votre organisation doit gérer une infrastructure qui peut s'avérer coûteuse et nécessiter du personnel spécialisé en gestion des clés. Pour les organisations de plus petite taille, c'est rarement faisable.

Les fournisseurs de services disposent souvent d'une solide infrastructure de gestion des clés et des stratégies appropriées pour verrouiller l'accès. Vous pouvez demander d'examiner les capacités de gestion de clés du FSG. Gardez à l'esprit les considérations suivantes :

- Les ressources à l'extérieur de votre organisation ne doivent jamais avoir accès à la fois à vos données et aux clés utilisées pour déchiffrer ces données. Des stratégies et mécanismes de contrôle d'accès devraient être en place pour veiller à ce que les clés de chiffrement soient isolées des données qu'elles protègent;
- Les clés de chiffrement ne doivent jamais être stockées en texte clair à l'extérieur de l'infrastructure de confiance de votre organisation. Les clés de chiffrement doivent être chiffrées au repos, au même niveau, ou à un niveau plus élevé, que les données qu'elles protègent.

N'oubliez pas que votre organisation dispose toujours d'autres options. Vous pouvez utiliser les services d'un tiers pour gérer les clés de chiffrement si la stratégie d'isolation des clés du FSG ne répond pas à vos besoins. Cette mesure pourrait ajouter à la complexité des négociations sur les niveaux de service, mais elle permettrait de mieux sécuriser vos données.

Tableau 11 : Activités des clients associées à la gestion des clés

Numéro	Activité des clients	Cocher
1	Déterminez vos exigences en matière de clés de chiffrement sécurisées (p. ex. les clés doivent être chiffrées au même niveau de sensibilité que celui des données que vous protégez, ou à un niveau supérieur).	
2	Déterminez la capacité de votre organisation à gérer les clés (p. ex. est-ce faisable et est-il préférable que votre organisation les gère?).	
3	Demandez à examiner les stratégies du FSG qui prennent en charge la gestion des clés et le contrôle d'accès.	
4	Demandez au fournisseur de services de vous présenter toutes les étapes du processus de gestion des clés afin de vérifier si le processus est sécurisé.	
5	Communiquez avec nous pour examiner l'évaluation du fournisseur de services du FSG, qui peut vous aider à déterminer si le FSG possède les capacités de gestion de clés appropriées.	
6	Déterminez s'il est faisable ou préférable d'utiliser un service de gestion des clés en tierce partie.	

Questions à poser au fournisseur de services		
1	Le fournisseur de services prend-il en charge la sauvegarde des clés de chiffrement?	
2	Qui a accès aux sauvegardes de vos clés de chiffrement?	
3	Quel niveau de chiffrement sert à protéger les clés de chiffrement stockées?	

2.6 INTERVENTION EN CAS D'INCIDENT

Des incidents peuvent se produire même si des contrôles de sécurité sont en place. Un incident de sécurité se définit comme tout dommage, vol ou accès non autorisé intentionnel ou non intentionnel qui a des répercussions directes ou indirectes sur la sécurité des systèmes ou des services de votre organisation. Les incidents peuvent avoir des conséquences sur la prestation ou la sécurité d'un service, entraînant l'interruption imprévue d'activités. En voici quelques exemples :

- atteinte à la sécurité des données;
- vol ou perte d'actifs;
- code malveillant;
- analyses de réseau;
- attaques par déni de service;
- fraude;
- défaillance du serveur.

Lorsqu'un incident se produit, votre organisation doit intervenir rapidement pour réduire au minimum les dommages qui en résultent. Un plan général d'intervention en cas d'incident comprend des étapes pour détecter, contenir, corriger et communiquer le problème. Un incident peut être détecté par votre organisation (p. ex. problèmes liés à l'utilisation d'un service) ou par le fournisseur de services (p. ex. un problème d'application dorsale). Pour cette raison, vous devez avoir établi des moyens de communication efficaces avec votre fournisseur afin de pouvoir vous soutenir l'un l'autre.

Lorsque vous faites appel à un fournisseur de services, votre organisation demeure responsable de l'intervention en cas d'incident, même si votre organisation ne s'occupe pas de la mise en œuvre de toutes les étapes du processus de gestion des incidents. Vous devez collaborer avec le fournisseur de services pour coordonner un plan d'intervention en cas d'incident. Dans le cadre de ce plan d'intervention, vous devriez séparer les rôles et les responsabilités de votre organisation et du fournisseur de services. Comme un fournisseur de services pourrait offrir des services semblables à de nombreux clients, ses priorités diffèrent de celles de votre organisation. Par exemple, si votre organisation est aux prises avec un problème catastrophique pour ses activités qui exige une intervention immédiate, votre demande d'intervention urgente risque de rester dans la file d'attente du fournisseur de services s'il est occupé à soutenir de nombreuses autres organisations qui sont elles aussi confrontées à de multiples problèmes critiques.

Vous devez donc établir des exigences claires en matière d'intervention en cas d'incident, et vous assurer que le fournisseur de services est en mesure d'y répondre. Nous vous recommandons de travailler avec le fournisseur de services afin de vous entendre sur les attentes liées au niveau de service dont votre organisation a besoin, et de les définir clairement. Votre entente sur les niveaux de service avec le fournisseur doit spécifier les délais d'exécution prévus, les moyens de communication, les processus de transmission à un palier supérieur, les paramètres d'évaluation du rendement, et les pénalités en cas de non-respect des délais d'exécution.

Si des incidents se produisent à répétition, il faut chercher la cause profonde. Dans le cadre de l'acquisition de services gérés, il est important de s'assurer que le fournisseur de services a la capacité de faire rapport sur les incidents au fil du temps afin de pouvoir cerner les problèmes sous-jacents. Prenons comme exemple les fuites de données sensibles. Si une

telle fuite se produit une seule fois ou rarement, on peut gérer les incidents au cas par cas, mais si des fuites se produisent à plusieurs reprises, il faudra déterminer si un problème plus profond est en cause. Il conviendrait peut-être d'investir les fonds nécessaires pour réviser la formation sur la sécurité afin qu'elle porte notamment sur les fuites de données ou pour mettre en œuvre des mesures comme la prévention de la perte de données (PPD) ou des solutions interdomaines (SID).

Tableau 12 : Activités des clients associées à l'intervention en cas d'incident

Numéro	Activité des clients	Cocher
1	Passez en revue le processus de gestion des incidents de votre organisation et déterminez comment l'utilisation de services gérés influera sur ce processus.	
2	Examinez le processus de gestion des incidents de la bibliothèque d'infrastructure des TI (ITIL pour *IT Infrastructure Library*). La bibliothèque d'infrastructure des TI est un cadre qui définit et décrit les pratiques exemplaires en matière de prestation de services de TI. Cette bibliothèque établit les étapes, les définitions et la terminologie normalisées de la gestion des incidents. Il s'agit d'un bon point de départ pour déterminer les rôles et responsabilités en matière d'intervention en cas d'incident.	
3	Établissez les exigences en matière d'intervention en cas d'incident qui doivent être satisfaites afin que vous puissiez continuer à répondre à vos besoins commerciaux et opérationnels. Vous devriez définir vos exigences en matière de surveillance, de détection, d'analyse, de confinement, d'intervention, de rétablissement et de suivi des incidents. Considérez ce qui suit : • définir ce qui constitue un incident; • déterminer les types d'incidents; • établir les priorités quant aux types d'incidents; • désigner un chef d'équipe chargé de gérer le processus d'intervention en cas d'incident; • fixer les délais d'envoi des avis d'incident au personnel, au fournisseur de services et aux fournisseurs. **Remarque :** À titre de cliente de services gérés, votre organisation pourrait établir un processus défini de gestion des incidents ou utiliser le processus d'un fournisseur de services.	
4	Demandez au fournisseur de services de vous présenter toutes les étapes de son processus d'intervention en cas d'incident.	
5	Déterminez les temps d'arrêt acceptables de chaque unité opérationnelle.	
6	Déterminez la perte de données acceptable pour chaque unité opérationnelle (pour chaque type d'incident de sécurité) afin d'établir les méthodes et les calendriers de sauvegarde (p. ex. à quelle fréquence les sauvegardes doivent-elles avoir lieu?). Par exemple, si vous effectuez des sauvegardes quotidiennement et que le système tombe en panne 23 heures après la dernière sauvegarde, vous perdrez 23 heures de données. Est-ce un risque acceptable aux yeux de votre organisation?	

7	Déterminez la vision de votre organisation en ce qui a trait aux rôles et responsabilités en matière de gestion des incidents (pour chacun des types d'incidents relevés) lorsque vous utilisez un service géré.	
8	Déterminez les activités d'intervention en cas d'incident qui doivent demeurer sous le contrôle de votre organisation (p. ex. à des fins de conformité aux lois ou aux règlements).	
Questions à poser au fournisseur de services		
1	Le fournisseur de services prend-il en charge les types d'incidents et les rôles que votre organisation a définis?	
2	Le fournisseur de services souhaite-t-il travailler avec votre organisation pour simuler des scénarios d'intervention en cas d'incident relatifs aux types d'incidents déterminés?	
3	Quels sont les rôles et responsabilités du fournisseur de services pour ce qui est de l'intervention en cas d'incident? Quelles sont les attentes du fournisseur de services à l'égard des rôles et responsabilités de votre organisation?	
4	Quel est le délai de traitement garanti par le FSG pour les types d'incidents que vous avez déterminés?	
5	Quelles pénalités imposerez-vous si le FSG n'intervient pas dans les délais établis?	
6	Qui est la personne-ressource principale du FSG pour l'intervention en cas d'incident? **Remarque :** Fournissez également les coordonnées de la personne-ressource principale de votre organisation.	
7	Le FSG peut-il offrir une ligne d'assistance qui serait utilisée pour déclencher l'intervention en cas d'incident? Disponibilité?	
8	Lorsqu'un incident de sécurité touche les données de votre organisation, comment le FSG vous avise-t-il?	

2.6.1 PRISE EN CHARGE DE LA JOURNALISATION DES ÉVÉNEMENTS

Le fournisseur de services dispose d'un accès direct aux systèmes associés aux services qu'il fournit. À ce titre, il pourrait être en mesure de fournir des données de journaux ou d'exécuter des services de surveillance liés aux éléments suivants :

- analyse de virus;
- détection de codes, de fichiers ou de dossiers non standards ou suspects dans les hôtes (capteurs au niveau de l'hôte);
- vérification des signatures;
- utilisation de la bande passante;
- surveillance des événements;
- surveillance des activités de l'utilisateur.

Vous devez définir explicitement vos exigences et responsabilités en ce qui a trait à la prise en charge des journaux afin de détecter les incidents de sécurité potentiels. Vous n'avez peut-être pas besoin de consulter tous les journaux, mais vous devriez être au courant des événements qui ont une incidence sur vos données.

Tableau 13 : Activités des clients associées à la prise en charge de la journalisation des événements

Numéro	Activité des clients	Cocher
1	Déterminez vos capacités d'examen et d'analyse des journaux.	
2	Déterminez les données de journaux que vous devez examiner (p. ex. incidents de sécurité, procédures judiciaires, conformité juridique ou réglementaire).	
3	Examinez votre politique de conservation des données (c.-à-d. les exigences juridiques et la réglementation de l'industrie régissant la conservation des données) et demandez au FSG de vous présenter la sienne.	
Questions à poser au fournisseur de services		
1	Les données de journalisation sensibles sont-elles stockées au Canada?	
2	Le FSG peut-il prendre en charge et respecter votre politique de conservation des données en ce qui a trait aux journaux?	
3	Quels types de journaux le FSG peut-il fournir?	
4	À quelle fréquence le FSG fournit-il des journaux (p. ex. sur une base périodique, lorsque surviennent des incidents de sécurité, sur demande)?	
5	Le FSG peut-il fournir les journaux sur un support qui protège adéquatement les données sensibles?	
6	Le FSG offre-t-il des services de surveillance? Si oui, demandez des détails ou une présentation par étapes des services.	
7	À quelle fréquence le FSG examine-t-il les journaux?	
8	Comment le FSG vous informera-t-il d'un incident de sécurité qui porte atteinte à vos données? Combien de temps après l'incident le FSG vous informera-t-il?	
9	Le FSG surveille-t-il uniquement le code malveillant connu (p. ex. la détection de signature), ou utilise-t-il également la détection comportementale pour surveiller les attaques du jour zéro?	
10	Le FSG a-t-il la capacité de déceler les tendances des incidents au fil du temps? Vous en avisera-t-il?	

2.7 CONTINUITÉ DES ACTIVITÉS ET REPRISE APRÈS SINISTRE

La continuité des activités renvoie à la capacité de votre organisation de poursuivre ses activités à la suite d'un incident (p. ex. une interruption ou un sinistre). Si vous faites appel à un fournisseur de services, vous dépendez de lui pour assurer la disponibilité continue des services que vous utilisez. Vous devez connaître les mesures qu'applique le fournisseur de services afin de prévenir les défaillances et les moyens qu'il prendra afin de soutenir la reprise de ces services en cas de sinistre. La continuité des activités et la reprise après sinistre renvoient directement au pilier de la disponibilité du profil de sensibilité des données (voir la section 2.1).

2.7.1 REDONDANCE

Le temps de disponibilité désigne le pourcentage de temps garanti par le fournisseur de services pendant lequel il peut fournir des services. Veuillez noter que les fournisseurs de services, y compris les FSI, n'offrent pas tous le même temps de disponibilité garanti. Vous devriez vous assurer que vous pourrez accéder aux données de votre organisation au besoin.

Lorsque des défaillances matérielles se produisent, les systèmes peuvent continuer de tourner en fonction de la redondance et des mécanismes de basculement qu'on a mis en place. Dans le cadre de la planification de la continuité des activités de votre organisation, déterminez vos besoins en matière de temps de disponibilité, ainsi que la durée maximale de panne que vous pouvez tolérer sans mettre en péril vos activités commerciales (c.-à-d. le temps d'arrêt maximal tolérable). Veuillez noter que vos exigences en matière de temps de disponibilité et de temps d'arrêt maximal tolérable pourront varier selon vos fonctions et vos processus opérationnels. Par exemple, le temps d'arrêt acceptable pour un organisme d'administration des élections le jour d'une élection est beaucoup plus court et moins tolérable que le temps d'arrêt le lendemain de cette élection.

Tableau 14 : Activités des clients associées à la redondance

Numéro	Activité des clients	Cocher
1	Déterminez vos exigences en matière de temps de disponibilité (c.-à-d. le pourcentage de temps pendant lequel les fonctions et les processus de votre organisation doivent être opérationnels et en marche afin de vous permettre d'exercer efficacement vos activités).	
2	Déterminez le temps d'arrêt maximal tolérable que votre organisation peut accepter sans effet nuisible sur ses activités. Cela déterminera les exigences en matière de service que vous établissez avec le FSG (p. ex. la durée maximale pendant laquelle les services du FSG peuvent être en panne sans encourir de pénalité).	
3	Consultez les temps d'arrêt et pertes de données acceptables indiqués à la section 2.6.	
Questions à poser au fournisseur de services		
1	Quelles interruptions de service prévues surviendront?	

2	Comment le FSG vous informera-t-il des interruptions de service prévues et imprévues?	
3	Quels mécanismes de basculement le FSG emploie-t-il?	
4	Les données redondantes sont-elles stockées au Canada?	
5	Quelle est la garantie de temps de disponibilité du FSG?	
6	Comment ferez-vous respecter vos exigences en matière de temps de disponibilité?	

2.7.2 REPRISE APRÈS SINISTRE

Dans un monde idéal, il ne se produit aucun sinistre et il n'est jamais nécessaire de procéder au rétablissement. En réalité, votre organisation doit être prête à faire face à des scénarios où les choses tournent mal afin de pouvoir se rétablir rapidement et réduire les répercussions sur ses activités. Il revient à votre organisation d'établir et de mettre à l'essai un plan de reprise après sinistre. Vous pourriez impartir certains aspects de ce plan (p. ex. sauvegarde des données) à un fournisseur de services. Vous devez absolument travailler de concert avec le FSG pour vous assurer que les services impartis fonctionnent et que vos rôles et responsabilités sont clairs.

Tableau 15 : Activités des clients associées à la reprise après sinistre

Numéro	Activité des clients	Cocher
1	Définissez les exigences en matière de reprise après sinistre (p. ex. si un sinistre survient, que devez-vous faire pour reprendre les activités?).	
2	Déterminez la capacité de votre organisation à répondre aux exigences de reprise après sinistre (c.-à-d. que doit-on ou peut-on impartir?), et élaborez un plan de reprise après sinistre.	
3	Déterminez comment votre organisation mettra à l'essai le plan de reprise après sinistre, et les exigences relatives à la participation du fournisseur de services.	
4	Déterminez les exigences relatives à la fréquence et à la méthode de sauvegarde. **Remarque :** Cela dépend de facteurs comme la quantité de données que vous pouvez vous permettre de perdre. Par exemple, si une défaillance survenait 23 heures après la dernière sauvegarde quotidienne, vous risquez de perdre 23 heures de données. Les sauvegardes horaires peuvent cependant coûter cher.	
5	Déterminez votre politique de conservation des données quant aux sauvegardes (voir la section 2.2).	
6	Indiquez la personne-ressource principale de votre organisation en vue de la reprise après sinistre.	
Questions à poser au fournisseur de services		
1	Le fournisseur de services peut-il vous expliquer toutes les étapes des services de reprise après sinistre qu'il offre?	

2	Le FSG répond-il à vos exigences organisationnelles en matière de sauvegarde des données (p. ex. fréquence des sauvegardes, méthode, politique de conservation)?	
3	Le FSG offre-t-il un support de livraison pour les sauvegardes qui tient compte du degré de sensibilité de vos données (p. ex. canal sécurisé ou niveau de chiffrement approprié)?	
4	Les données de sauvegarde sensibles sont-elles stockées au Canada?	
5	Le FSG est-il disposé à participer activement à vos essais de reprise après sinistre?	
6	Le site de secours est-il une salle blanche, un centre de secours intermédiaire ou un centre de secours immédiat? **Remarque :** Un centre de secours immédiat désigne un site équipé de matériel, d'un système de CVC et de copies de données, ce qui en fait un site prêt à fonctionner en quelques heures. Un centre de secours intermédiaire dispose de matériel et d'un système de CVC, mais peut nécessiter jusqu'à une semaine pour être opérationnel avec les données de votre organisation. Une salle blanche est dotée d'un système de CVC, mais elle a besoin de matériel et il faut l'aménager avant de l'utiliser, ce qui prend habituellement un ou deux mois.	
7	Comment le FSG isole-t-il les données opérationnelles des sauvegardes? **Remarque :** La pratique exemplaire veut qu'on ne stocke jamais les sauvegardes au même endroit que les données opérationnelles. Autrement, le même sinistre (p. ex. incendie, inondation, lock-out du fournisseur) qui a causé la perte de données opérationnelles pourrait aussi porter atteinte aux sauvegardes.	
8	Le FSG dispose-t-il d'une ligne d'urgence sécurisée permettant de lancer le plan de reprise après sinistre?	

2.8 INTÉGRITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

Votre chaîne d'approvisionnement comporte votre réseau de fournisseurs, de fournisseurs de services (aussi appelés sous-traitants), d'organisations partenaires, et de ressources qui participent à la création et à la prestation de vos produits et services d'affaires. Votre chaîne d'approvisionnement est vitale pour vos activités, mais elle peut également constituer une cible de grande valeur aux yeux des auteurs de menace.

Comme l'indique l'*Évaluation des cybermenaces nationales 2018* [13] du Centre pour la cybersécurité, les auteurs de cybermenaces sophistiqués continuent d'exploiter les relations entre les entreprises et leurs fournisseurs et fournisseurs de services, y compris les chaînes d'approvisionnement des technologies de l'information et des communications (TIC). Des études de l'industrie confirment également que la moitié de toutes les cyberattaques observées font appel à la compromission de la chaîne d'approvisionnement.

Peu importe la taille de votre organisation, vous devriez tenir compte des risques associés à votre chaîne d'approvisionnement et à vos produits et services de TIC (p. ex. appareils d'utilisateur final, logiciels, solutions de réseautage, serveurs). Lorsque vous faites l'acquisition de services gérés, la responsabilité de protéger la sécurité de vos renseignements vous revient. Il importe donc de bien comprendre le niveau d'assurance que le fournisseur de services est en mesure d'offrir pour la technologie dont il est responsable.

Tableau 16 : Activités des clients associées à l'intégrité de la chaîne d'approvisionnement

Numéro	Activité des clients	Cocher
1	Examinez les services potentiels que vous souhaitez obtenir auprès du FSG. Qui est responsable de l'acquisition et de la gestion des technologies liées à ces services? La réponse à cette question orientera la portée de votre conversation avec le fournisseur de services.	
Questions à poser au fournisseur de services		
1	En ce qui concerne la technologie que le fournisseur de services est responsable de gérer, l'assurance de la chaîne d'approvisionnement du fournisseur de services s'accorde-t-elle avec les orientations établies pour le contrôle de sécurité SA-12 dans l'ITSG-33 [2]? L'assurance s'accorde-t-elle avec la publication spéciale 800-161 du NIST intitulée *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [14] ou avec la norme ISO/IEC 27036-1:2014 *(Sécurité d'information pour la relation avec le fournisseur)* [15]? Si oui, le fournisseur de services peut-il démontrer cette harmonisation dans ses documents de politique ou de planification?	
2	Lorsque le FSG passe un contrat avec un fournisseur de services (sous-traitant), comment examine-t-il les antécédents du fournisseur pour assurer l'intégrité de la chaîne d'approvisionnement? Comment le fournisseur démontre-t-il l'intégrité de la chaîne d'approvisionnement?	
3	Lorsque des changements surviennent, comment le fournisseur de services examine-t-il les risques liés à la chaîne d'approvisionnement? Le fournisseur de services avise-t-il votre organisation afin de discuter des paramètres d'adhésion ou de retrait?	

2.9 PORTABILITÉ DES DONNÉES ET DES SERVICES

Après avoir établi un contrat avec un fournisseur de services, votre organisation pourrait décider d'emprunter une autre voie si elle n'est pas satisfaite des services ou si ses besoins opérationnels évoluent. L'enfermement propriétaire se produit lorsqu'il n'est pas financièrement faisable de transférer des données d'un fournisseur à un autre (p. ex. pénalités d'envergure connexes, formats de données exclusifs, propriété des données).

La portabilité des données renvoie à la capacité de transférer des données d'un système ou serveur à un autre. Au moment de passer un contrat de service, votre organisation devrait envisager une stratégie de sortie, au cas où elle aurait besoin de changer de fournisseur plus tard.

Tableau 17 : Activités des clients associées à la portabilité des données et des services

Numéro	Activité des clients	Cocher
1	Discutez de la portabilité des données avec le fournisseur de services avant de signer un contrat de service (afin d'éviter l'enfermement propriétaire).	
2	Faites des recherches sur votre FSG potentiel. Sa réputation peut vous aider à déterminer si vous pouvez confier vos données à ce FSG.	

Questions à poser au fournisseur de services		
1	Qui conserve la propriété juridique des données dans les circonstances suivantes? • Le contrat d'un fournisseur de services est résilié. • Un fournisseur de services déplace des serveurs, des données ou des sauvegardes vers un emplacement non convenu au moment de la négociation du contrat. • Des changements importants apportés aux pratiques de sécurité minent la confiance de votre organisation dans la capacité du fournisseur de services de protéger les données. • Le fournisseur de services fait l'objet d'acquisition par une organisation qui n'évalue pas la sécurité ou qui soulève des préoccupations quant à l'intégrité de la chaîne d'approvisionnement.	
2	Quelles sont les pénalités si votre organisation souhaite changer de FSG (c.-à-d. les coûts de déménagement)?	
3	Y a-t-il des formats de données qui ne répondent pas aux normes de l'industrie (c.-à-d. des normes exclusives au fournisseur)?	
4	Quels sont les coûts liés au transfert des systèmes hérités à l'infrastructure de stockage du FSG?	
5	Que se passe-t-il si le fournisseur de services déclare faillite? Comment pourrez-vous récupérer les données de votre organisation?	

2.10 DESTRUCTION DES DONNÉES

Une fois que les données ne sont plus nécessaires à des fins opérationnelles et qu'elles ont été conservées pendant la période de conservation désignée, il convient de les détruire. La destruction des données consiste à détruire les données stockées sur des bandes, des disques durs et d'autres supports électroniques ou physiques afin de les rendre complètement illisibles, inaccessibles et inutilisables à des fins non autorisées. La destruction appropriée des données garantit que votre organisation se conforme aux exigences juridiques et réglementaires. Elle réduit également le risque de fuite de données et d'atteinte à leur protection. Les fuites de données peuvent entraîner la non-conformité aux exigences législatives et de politiques, la perte de réputation, une couverture médiatique négative, la perte de revenus, des amendes réglementaires, des poursuites et des frais juridiques.

Lorsque vous faites appel à des services infonuagiques, vous devez vous assurer que le FSI protège vos données et qu'il les détruira en conformité avec les exigences de votre organisation (p. ex. politique de gestion de l'information, calendrier de conservation). Dans le nuage, la destruction physique du matériel est extrêmement difficile, car le FSI est propriétaire du matériel et que celui-ci peut héberger les données de plusieurs clients. Le crypto-déchiquetage constitue alors le moyen le plus efficace de détruire les données. Le crypto-déchiquetage consiste à chiffrer les données qui ne sont plus nécessaires, puis à supprimer ou écraser délibérément les clés de chiffrement pour ainsi rendre les données inaccessibles.

Il convient de noter que l'infrastructure en nuage se fonde sur le principe de la redondance (c.-à-d. qu'il existe de nombreuses instances des données). Pour détruire complètement les données, il faut d'abord localiser toutes les instances des données. Il importe de savoir s'il existe des copies hors ligne, telles que les sauvegardes ou d'autres téléchargements, afin de vous assurer qu'elles sont visées par le processus de destruction.

Tableau 18 : Activités des clients associées à la destruction des données

Numéro	Activité des clients	Cocher
1	Déterminez les exigences de votre organisation en matière de destruction de données, en tenant compte de la sensibilité des données. **Remarque :** Si les données résident dans le nuage, il faudra avoir recours au crypto-déchiquetage pour les détruire.	
2	Communiquez avec notre Centre d'appel et consultez l'ITSP.40.006 (*Nettoyage des supports de TI*) [16] pour en savoir plus sur la destruction des données.	
Questions à poser au fournisseur de services		
1	Quelle approche le FSG adoptera-t-il pour assurer la suppression complète et sécurisée des données?	
2	Le FSG sera-t-il en mesure de repérer toutes les instances de données aux fins de destruction?	
3	Lorsque le matériel fait l'objet de la gestion du cycle de vie, comment le nettoie-t-on?	

3 CONTENU COMPLÉMENTAIRE

3.1 LISTE D'ABRÉVIATIONS

Terme	Définition
A2F	Authentification à deux facteurs
ADFS	Services de fédération Active Directory (*Active Directory Federation Services*)
AS	Administrateur de système
COBIT	Objectifs de contrôle de l'information et des technologies connexes *(Control Objectives for Information and related Technologies*)
CSA	Cloud Security Alliance
FSG	Fournisseur de services gérés
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
ICA	Intégrité de la chaîne d'approvisionnement
ISACA	Information Systems Audit and Control Association
ISAE	Norme internationale de missions d'assurance *(International Standard on Assurance Engagements)*
ISO	Organisation internationale de normalisation
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
NIP	Numéro d'identification personnel
NIST	National Institute for Standards and Technology
NOC	Centre d'exploitation du réseau (*Network Operation Centre*)
PPD	Prévention de la perte de données
RGPD	*Règlement général sur la protection des données*
SCT	Secrétariat du Conseil du Trésor du Canada
SID	Solution interdomaines
SOC	Contrôles au niveau du système et au niveau organisationnel (rapport SOC) (*System and Organization Controls*)
STAR	Programme Security Trust Assurance and Risk
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
UE	Union européenne

3.2 GLOSSAIRE

Terme	Définition
Authentification	Processus permettant de confirmer l'identité d'un utilisateur ou d'une autre entité (p. ex. une application) comme étant valide et authentique.
Authentification à deux facteurs	Méthode d'authentification selon laquelle deux facteurs d'authentification distincts (p. ex. quelque chose que vous savez, quelque chose que vous êtes, quelque chose que vous avez) sont requis pour obtenir l'accès à un système.
Autorisation	Utilisation de renseignements d'authentification pour déterminer si une entité (c.-à-d. une personne ou une application) peut ou non accéder à des données ou exécuter une fonction.
Centre de secours immédiat	Site de secours équipé de matériel, d'un système de CVC et de copies de données, ce qui en fait un site pleinement opérationnel en quelques heures.
Centre de secours intermédiaire	Site doté de matériel et d'un système de CVC.
Clé de chiffrement	Chaîne aléatoire de bits générée par un algorithme et servant à chiffrer et déchiffrer les données.
Confidentialité	Valeur qui est accordée à une information pour indiquer son niveau de sensibilité et les restrictions d'accès mises en place pour empêcher les utilisateurs non autorisés de les consulter.
Crypto-déchiquetage	Procédé consistant à chiffrer les données qui ne sont plus nécessaires, puis à supprimer ou à écraser de façon délibérée les clés de chiffrement pour rendre les données inaccessibles.
Disponibilité	Valeur qui est accordée aux actifs informationnels, logiciels et matériels (l'infrastructure et ses composantes). Les données ayant la valeur 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 ou les compromissions.
Données en transit	Données actives qui se déplacent d'un endroit à un autre, comme dans Internet ou un réseau privé.
Données inactives	Données au repos (p. ex. résidant dans une base de données, un entrepôt de données, une feuille de calcul, des archives, des sauvegardes, des appareils mobiles).
Droit d'accès minimal	Principe de contrôle d'accès selon lequel on n'accorde aux utilisateurs que les privilèges dont ils ont besoin pour exécuter leurs fonctions.
Hachage	Fonction mathématique servant à convertir un bloc ou groupe de données en une valeur de longueur fixe, habituellement plus courte que les données d'origine. Le hachage masque les données d'origine par une autre valeur qu'on ne peut décoder qu'en recherchant la valeur dans un tableau de hachage.
Identité fédérée	Moyen de relier l'identité électronique et les attributs d'une personne, stockés dans plusieurs systèmes d'identité.
Intégrité	Valeur qui est accordée à l'information pour indiquer dans quelle mesure elle est sensible 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. Le concept d'intégrité s'applique également aux processus opérationnels, à la logique des logiciels d'application, au matériel et au personnel.

Terme	Définition
Salage	Ajout de caractères à un mot de passe pour obtenir une longueur standard, obscurcissant davantage sa valeur réelle.
Salle blanche	Emplacement doté d'un système de CVC, mais qui a besoin de matériel et qu'il faut aménager avant de l'utiliser.

3.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité. *Pratiques exemplaires en matière de cybersécurité : Passation de marché avec des fournisseurs de services gérés,* 3 avril 2017.
2	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33), décembre 2014.
3	Secrétariat du Conseil du Trésor du Canada. *Directive sur la résidence des données électroniques : Avis de mise en œuvre de la politique sur les TI,* 1er novembre 2017.
4	Organisation internationale de normalisation. *ISO27001/2 Gestion de la sécurité de l'information.*
5	Information Systems Audit and Control Association. *Control Objective for Information and related Technologies (COBIT).*
6	Cloud Security Alliance. *Security Trust Assurance and Risk (STAR).*
7	National Institute of Standards and Technologies. *Risk Management Framework*.
8	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.189),* octobre 2018.
9	Conseil des normes internationales d'audit et d'assurance. Norme internationale de missions d'assurance (ISAE) nº 3402*, Assurance Reports on Controls at a Service Organization*, juin 2011.
10	Centre canadien pour la cybersécurité. *Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032), septembre 2019.
11	Centre canadien pour la cybersécurité. *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111), août 2016.
12	Centre canadien pour la cybersécurité. *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062), octobre 2020.
13	Centre canadien pour la cybersécurité. *Évaluation des cybermenaces nationales 2018.*
14	National Institute of Standards and Technology. *Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, avril 2015.
15	Organisation internationale de normalisation. *ISO/IEC 27036-1:2014 Sécurité d'information pour la relation avec le fournisseur*, avril 2014.
16	Centre canadien pour la cybersécurité. *Nettoyage des supports de TI* (ITSP.40.006), juillet 2017.