Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

PROCESSUS D'ÉVALUATION DE LA SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION S'APPLIQUANT AUX FOURNISSEURS DE SERVICES INFONUAGIQUES

ITSM.50.100

Octobre 2018

SÉRIE GESTIONNAIRES

Canada

AVANT PROPOS

La présente intitulée Processus d'évaluation de la sécurité des technologies de l'information (STI) s'appliquant aux fournisseurs de services infonuagiques (FSI) est un document NON CLASSIFIÉ publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST).

Les propositions de modifications doivent être envoyées à l'attention de votre représentant des Services à la clientèle, au Centre canadien pour la cybersécurité (CCC), par l'intermédiaire des services de sécurité des communications du ministère.

Pour obtenir de plus amples renseignements, prière de communiquer avec les Services à la clientèle en envoyant un courriel à contact@cyber.gc.ca ou en appelant le 613-949-7048 ou 1-833-CYBER-88.

DATE D'ENTRÉE EN VIGUEUR

La présente entre en vigueur Octobre 2018.

APERÇU

Le présent document a pour objet de décrire le Programme d'évaluation de la sécurité des technologies de l'information (STI) s'appliquant aux fournisseurs de services infonuagiques (FSI). En l'occurrence, l'objectif du Programme d'évaluation de la STI visant les FSI est d'assister les ministères et organismes du gouvernement du Canada (GC) qui doivent procéder à l'évaluation des services qui leur sont fournis par des FSI. Au reste, les conclusions de ces évaluations permettront d'établir si les processus et les contrôles de sécurité d'un FSI donné répondent aux exigences visant la sécurité des services d'infonuagique publique qui sont appelés à traiter de l'information et à prodiguer des services dont la catégorie peut aller jusqu'à Protégé B, intégrité moyenne, disponibilité moyenne (PBMM), et ce, conformément aux stipulations du Secrétariat du Conseil du Trésor [1].

Au reste, le programme a également pour objet de déterminer si les améliorations et les contrôles de sécurité que le GC a choisis depuis le Catalogue des contrôles de sécurité, que l'on retrouve en annexe 3 de l'ITSG 33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie, [2] sont en mesure de maintenir un degré de fiabilité acceptable. Ces évaluations peuvent être réalisées à l'aide des conseils, des normes et des rapports qui ont déjà été produits par le GC et par les organismes alliés ou encore par des intervenants de l'industrie (pratiques exemplaires) et du marché commercial (attestations). Cette mine d'information permettra d'accélérer les processus d'évaluation et incitera les FSI à travailler avec le GC et les vérificateurs indépendants ou avec d'autres organismes d'évaluation. L'objectif ultime du GC est de développer une compréhension approfondie des capacités STI et des risques inhérents aux services infonuagiques auxquels le GC a recours.

Les conseils et les avis formulés suivant les évaluations de la STI ont pour but d'alimenter le processus de gestion des risques engagé par les ministères du GC qui envisagent de faire appel à des services d'infonuagique publique.

Ainsi, les ministères qui se proposent de faire appel à des services d'infonuagique publique devraient répondre aux questions suivantes :

- Les risques relevés dans les rapports d'évaluation sont-ils tolérables?
- Des mesures de sécurité pourraient-elles être mises en œuvre pour atténuer les lacunes relevées?
- Devrait-on opter pour un autre service/fournisseur?

TABLE DES MATIÈRES

1 INTRODUCTION

Le présent document a pour objet de décrire le programme du CCC intitulé Programme d'évaluation de la sécurité des technologies de l'information (STI) s'appliquant aux fournisseurs de services infonuagiques (FSI). L'objectif du présent programme est d'assister les ministères et organismes du gouvernement du Canada (GC) qui doivent procéder à l'évaluation des services qui leur sont fournis par des FSI. Les conclusions d'une évaluation doivent indiquer si les processus et les contrôles de sécurité en vigueur chez le FSI visé répondent aux exigences de sécurité s'appliquer aux services d'infonuagique publique qui sont appelés à traiter de l'information ou à prodiguer des services dont la catégorie peut aller jusqu'à Protégé B, intégrité moyenne, disponibilité moyenne (PBMM), et ce, conformément aux stipulations du SCT [1].

En somme, le programme devra établir si les améliorations et les contrôles que le GC a choisis à même l'*ITSG-33* sont en mesure de maintenir un degré de fiabilité acceptable et conforme aux exigences. Ces évaluations peuvent être réalisées à l'aide des conseils, des normes et des rapports qui ont déjà été produits par le GC et les organismes alliés encore ou par des intervenants de l'industrie (pratiques exemplaires) et du marché commercial (attestations)[1]. Cette mine d'information permettra d'accélérer les processus d'évaluation, et incitera les FSI à travailler avec le GC et les vérificateurs indépendants ou avec d'autres organismes d'évaluation. En définitive, le GC cherche à développer une compréhension approfondie des capacités STI et des risques inhérents aux services infonuagiques auxquels le GC a recours.

Les conseils et les avis découlant des évaluations de la STI ont pour but d'alimenter le processus de gestion des risques engagé par les ministères du GC qui envisagent de faire appel à des services d'infonuagique publique. Ainsi, les ministères qui se proposent de faire appel à des services d'infonuagique publique doivent être en mesure d'établir si les risques mis en évidence dans les rapports d'évaluation sont tolérables et s'il existe des mesures d'atténuation envisageables ou si, le cas échéant, il serait préférable de faire appel à un autre service.

Une connaissance approfondie de plusieurs domaines de sécurité est requise pour suffisamment comprendre la posture de sécurité d'un système de technologie de l'information. Au reste, parmi les aspects qui doivent être examinés avant de parfaitement comprendre les capacités et les lacunes qu'affiche un FSI sur le plan de la sécurité, citons, entre autres, la sécurité physique des centres de données des FSI, la sécurité du personnel doté de privilèges, ou l'observation des règlements sur la protection des renseignements personnels. Dans ce processus, le rôle du CCC est de fournir des conseils et des avis sur les capacités techniques, opérationnelles et procédurales des FSI en matière de STI. Les ministères qui envisagent le recours à un service d'infonuagique devront prendre en compte toutes les exigences de sécurité posées par la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI), du SCT du Canada [3] et par d'autres règlements et politiques applicables du GC.

1.1 OBJET

Le présent document décrit le processus grâce auquel le CCC sera en mesure de faire état des capacités STI et des risques résiduels inhérents aux services d'infonuagique publique, qui sont appelés à soutenir les services et l'information PBMM du GC.

1.2 CONTEXTE

Ces évaluations ne portent que sur les exigences en matière de confidentialité, d'intégrité et de disponibilité de l'information et des services de TI du GC. En l'occurrence, elles ne prennent pas en compte les exigences s'appliquant à la résidence des données électroniques qui, par ailleurs, font l'objet de la Politique sur la gestion des technologies de l'information du SCT [4].

[1] Dans le présent document, le terme attestation renvoie à toute évaluation ou certification du domaine de la STI, qui aurait pu être reçue par les services d'un FSI donné. Au nombre de ces certifications citons celles-ci en exemple : le Service Organization Control 2 (SOC2) ou encore les normes 27001 de la Commission électrotechnique internationale (CEI) ou de l'Organisation internationale de normalisation (ISO).

Le processus de gestion des risques liés aux (TI) décrit par le SCT dans le document Approche et procédures de gestion du risque en matière de sécurité de l'informatique en nuage [5] comprend les neuf activités suivantes :

- procéder à la catégorisation de la sécurité (sur le plan de la confidentialité, de l'intégrité et de la disponibilité) de chacun des services du GC qui feront appel à l'infonuagique;
- choisir les contrôles de sécurité appropriés en se fondant sur les catégories de sécurité des services du GC;
- choisir le modèle approprié de déploiement en nuage ainsi que le modèle approprié de service infonuagique pour le service du GC;
- évaluer la mise en œuvre des contrôles de sécurité destinés aux services infonuagiques;
- appliquer les contrôles de sécurité aux services du GC;
- évaluer la mise en œuvre desdits contrôles de sécurité au sein des services du GC;
- autoriser l'exploitation des services du GC fondés sur l'infonuagique;
- assurer une surveillance continue de la sécurité des services du GC fondés sur l'infonuagique pendant la durée de la phase opérationnelle;
- maintenir l'état d'autorisation des services fondés sur l'infonuagique.

L'approche et les procédures décrites dans le présent document ont pour objet de faciliter la tâche des ministères et organismes du GC qui font appel à des services d'infonuagique publique et qui sont sur le point de s'engager dans la quatrième étape (voir plus haut) du processus de gestion des risques liés à la sécurité infonuagique : « évaluer la mise en œuvre des contrôles de sécurité destinés aux services infonuagiques ». Ainsi, la posture de sécurité et les risques résiduels relatifs à l'information et aux services du GC traités dans l'environnement d'un FSI varieront selon que les ministères et organismes concernés ont mené l'intégralité ou seulement une partie des activités de gestion des risques en matière de sécurité infonuagique.

1.3 L'AUDITOIRE CIBLE

Les évaluations fondées sur le présent processus correspondent aux scénarios faisant état des exigences opérationnelles et de l'acceptation des risques, comme il était indiqué précédemment. Il importe que le ministère ou l'organisme qui tient compte des résultats de ces évaluations aux fins du processus de gestion des risques liés à la sécurité infonuagique veille à ce que les exigences qu'il impose aux catégories de sécurité et à la sécurité de l'information correspondent aux exigences employées pour l'élaboration du profil de sécurité infonuagique du SCT.

1.4 DÉFINITIONS

Les notions abordées dans le présent document se fondent sur les définitions que la National Institute of Standards and Technology (NIST) propose en matière d'infonuagique dans le document Special Publication 800 145, The NIST Definition of Cloud Computing [6]. Certains de ces termes sont définis dans le glossaire se trouvant à la fin du présent document.

2 PROCESSUS D'ÉVALUATION

2.1 APERÇU

Une évaluation complète et indépendante de la sécurité des TI des FSI prend du temps, exige d'importantes ressources financières et sollicite plusieurs membres du personnel. Heureusement, la majorité des FSI obtiennent et conservent des attestations STI reconnues mondialement, ce qui leur permet d'offrir leurs services aux gouvernements et à certains secteurs de l'industrie. Parmi ces programmes d'attestation, on pense notamment au United States Federal Risk and Authorization Management Program (FedRAMP), aux Service Organization Controls (SOC) de l'American Institute of Certified Public Accountants (AICPA) ainsi qu'aux normes de l'Organisation internationale de normalisation (ISO) ou de la Commission électrotechnique internationale (CEI). Les services d'une tierce partie indépendante sont retenus pour vérifier si les FSI sont conformes à ces normes et, du même coup, aptes à répondre aux exigences de sécurité de la plupart de leurs clients. Pour prouver leur conformité, les FSI peuvent mettre leurs rapports d'attestation à la disposition de leur clientèle et ainsi confirmer la posture de sécurité de leurs services infonuagiques.

Le processus d'évaluation STI du CCC visant les FSI se fonde notamment sur les éléments constatés dans ces rapports d'attestation ou garantis par les attestations octroyées par d'autres tierces parties. Lorsqu'on ne peut pas garantir la conformité intégrale aux contrôles de sécurité des TI du GC et qu'aucune autre certification ne pourrait renforcer la posture de sécurité du FSI, il faut alors demander à celui-ci de fournir de nouveaux éléments de preuve. Si le FSI n'est pas en mesure de fournir ces éléments de preuve ou encore s'il est établi que ledit FSI ne répond pas aux exigences sur le plan des contrôles de sécurité des TI ou des améliorations des contrôles de sécurité, on recommandera des mesures d'atténuation ou une acceptation des risques.

2.2 PORTÉE

Ces évaluations ne porteront que sur les éléments suivants :

- services d'infonuagique publique auxquels les services du GC peuvent avoir recours;
- exigences du GC en matière de confidentialité, d'intégrité et de disponibilité, lesquelles sont définies dans le Profil de contrôle de sécurité infonuagique [1] visant le niveau PBMM ou aux niveaux inférieurs;
- mesures de sécurité dont le FSI estime qu'elles permettront à ses clients de répondre aux exigences PBMM du GC en matière de sécurité des TI.

Les éléments énumérés ci-dessous sont exclus de l'évaluation :

- vérifications permettant d'établir si les centres de données canadiens du FSI répondent aux exigences du GC en matière de sécurité physique;
- vérifications permettant d'établir si le personnel employé par le FSI pour la prestation des services au Canada a subi une enquête de sécurité permettant d'établir s'il répond aux exigences du GC en matière de sécurité du personnel ou à des exigences équivalentes;
- exigences du GC en matière de protection des renseignements personnels à l'exclusion de ce qui concerne la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information du GC;
- exigences concernant la résidence des données canadiennes.

2.3 PARAMÈTRES D'EXAMEN

Les évaluations de la sécurité des TI s'appliquant aux FSI procéderont notamment à une comparaison entre le Profil de contrôle de sécurité infonuagique [1] et les attestations internationales ou industrielles dont l'évaluation a été réalisée par de tierces parties reconnues par le GC. Les exigences de sécurité des TI sont définies dans le détail à l'annexe 3 Catalogue des contrôles de sécurité de l'ITSG-33 [2].

En matière de contrôles de sécurité et d'améliorations, des équivalences ont été établies entre les exigences de l'ITSG-33 et les normes de certification suivantes :

- System Security Plans (SSP) produits dans le cadre de FedRAMP;
- rapports SOC 2 Type II de l'AICPA;
- rapports 27001 de l'ISO et de la CEI;
- rapports 27018 de l'ISO et de la CEI.

À mesure qu'évolueront le Programme d'évaluation de la STI visant les FSI et les évaluations corollaires, des correspondances seront établies entre les exigences en matière de contrôles et d'améliorations énoncées dans l'ITSG-33 et un nombre croissant de normes de certification. En l'occurrence, il s'agit d'établir une base de connaissances commune à toutes les certifications couramment octroyées aux FSI. Cette base de connaissances permettra de vérifier si les FSI sont conformes aux exigences du GC en matière de sécurité des TI et d'assurance.

2.4 ATTRIBUT DE QUALITÉ

Des vérificateurs indépendants verront s'il y a lieu de confirmer l'exactitude des justificatifs sur lesquels se fondent les attestations fournies au CCC suivant l'entente de non-divulgation (END).

2.5 PROCESSUS

Les mesures préliminaires suivantes doivent être instaurées avant que l'évaluation STI visant les FSI ne soit réalisée par le CCC :

- Entériner ou conclure une END entre le CCC et le FSI faisant l'objet de l'évaluation. Les documents seront préparés et les discussions avec les FSI seront tenues selon les termes de l'END.
- Confirmer la catégorisation de la sécurité visée ainsi que le profil des contrôles de sécurité infonuagique.
- Obtenir des rapports actuels et pertinents de la part du FSI concernant le service à évaluer.

Le Programme d'évaluation de la STI s'appliquant aux FSI comporte les quatre phases suivantes :

<u>Phase 1 – Reconnaissance des documents d'attestation</u>

Un examen est d'abord réalisé pour établir si les documents d'attestation reçus de la part d'un FSI font état des améliorations et des contrôles de sécurité qui sont exigés conformément au profil qui fait état des contrôles de sécurité choisis. L'examen vise notamment à relever les éléments suivants :

- information manquante ou imprécise;
- problèmes nécessitant une discussion avec le FSI dans les plus brefs délais.

Dans la mesure du possible, l'examen des problèmes et l'attente des documents manquants ne devraient pas empêcher la réalisation des autres examens. Du reste, les discussions avec les représentants du FSI se poursuivent pendant le déroulement du processus d'évaluation.

<u>Phase 2 – Examen approfondi des preuves</u>

La documentation fournie par le FSI est analysée dans le but de relever les preuves d'application des améliorations et des contrôles de sécurité STI préalablement choisis. Cet examen permet d'établir si les conditions suivantes ont été respectées :

- Les exigences STI du GC (énoncées dans l'ITSG-33) ont été respectées.
- Les services et les procédures de sécurité du FSI correspondent aux contrôles de sécurité et aux améliorations définis par le GC.
- La documentation permet de conclure que les services de sécurité sont adéquatement mis en place, administrés et mis à jour par le FSI.

De plus, l'équipe d'évaluation du CCC doit examiner la documentation fournie par le FSI pour établir s'il y a lieu de formuler des recommandations ou de soulever des points de préoccupation concernant ce qui suit :

- La structure infonuagique (cloud fabric) est-elle protégée?
- Le réseau central du FSI est-il séparé de la structure infonuagique que le GC envisage d'utiliser?
- Est-il prévu que les systèmes de gestion du FSI communiquent avec les réseaux et les systèmes de gestion des TI du GC?
- Les systèmes et l'information du GC sont-ils dans un environnement multilocataire où les systèmes et les informations sont dans des espaces protégés et distincts de ceux des autres locataires?
- Au moment de se connecter aux informations et aux services de TI hébergés par le FSI, les utilisateurs seront-ils authentifiés par ces mêmes services?
- Y a-t-il des politiques, des pratiques, des services ou des configurations que les clients du GC doivent mettre en place pour activer les configurations de sécurité du FSI?
- Y a-t-il des clauses contractuelles additionnelles qui devraient s'ajouter aux documents de soutien à l'approvisionnement?

Phase 3 – Rapport initial et documentation complémentaire

Un rapport initial doit être produit et mis à la disposition du FSI et des clients du GC. Suivant les conclusions dudit rapport initial, le FSI sera invité à apporter des éclaircissements, à fournir des éléments de preuve additionnels ou à proposer des mesures visant à corriger les lacunes relevées. Le client du GC peut se servir du rapport initial pour identifier des points de préoccupation, indiquer les services de sécurité relevant de sa responsabilité qu'il est apte à mettre en œuvre, envisager des modifications contractuelles ou tolérer certains risques.

Pendant cette phase, l'équipe d'évaluation du CCC s'adjoindra le FSI et les représentants des clients du GC de façon à maintenir un niveau de risque qui soit tolérable pour toutes les parties.

Phase 4 – Rapport final

Au terme de la phase 3, dès lors que les parties sont prêtes à entamer le processus de gestion des risques liés à la sécurité infonuagique, un rapport final doit être préparé. Ce rapport final comprendra un résumé des conclusions et des recommandations du CCC concernant la STI du FSI et sera mis à la disposition du FSI et des représentants des clients du GC.

Certains services d'infonuagique publique, y compris ceux qui soutiennent les TI d'entreprise du GC, devront se soumettre à une réévaluation périodique.

Le CCC soumettra ses recommandations aux clients du GC concernant la fréquence à laquelle les services infonuagiques devraient être réévalués et répondra aux demandes de réévaluation de la part ces mêmes clients du GC.

3 RAPPORTS ET COMMUNICATIONS

Il est attendu que les rapports et les produits de communication suivants devront circuler parmi les représentants du FSI, du client du GC et du CCC.

3.1 RAPPORTS

Phase 1 – L'équipe d'évaluation du CCC doit envoyer un bref rapport sommaire pour fournir d'emblée les indicateurs et les commentaires concernant la documentation fournie par le FSI et les problèmes de STI potentiels.

Phase 2 – Aucun rapport n'est produit à la présente étape. En l'occurrence, l'équipe d'évaluation du CCC communiquera périodiquement avec les représentants du FSI ou du client du GC lorsqu'il y aura lieu d'apporter des éclaircissements sur les exigences formulées, les questions posées ou les difficultés soulevées.

Phase 3 – Le rapport initial doit être envoyé aux représentants du FSI et des clients du GC. Des rencontres subséquentes seront tenues avec les représentants pour examiner les résultats et pour permettre aux parties de s'entendre sur les modalités de résolution des difficultés, d'application des recommandations ou de réponses aux questions présentées dans le rapport initial.

Phase 4 – Une fois approuvé par la gestion du CCC, le rapport final doit être envoyé aux représentants du FSI et des clients du GC. Les questions et les difficultés énoncées dans le rapport final peuvent être soumises à l'attention du chef de l'équipe d'évaluation du CCC. Il est attendu que l'organisme client du GC se servira des conclusions du rapport final pour alimenter le processus de gestion des risques liés à la sécurité infonuagique.

3.2 COMMUNICATIONS

Pour faciliter le suivi et pour assurer la protection des documents servant aux évaluations, une boîte de courrier sera créée pour recevoir les documents soumis à l'attention du CCC. Cette boîte sera gérée par le chef de l'équipe d'évaluation du CCC ou par une personne déléguée. L'intégralité de la documentation concernant les évaluations STI de FSI sera administrée et protégée conformément aux politiques du CCC en matière de gestion de l'information.

4 CONTENU COMPLÉMENTAIRE

4.1 LISTE DE D'ABBRÉVIATIONS, D'ACRONYMS ET DE SIGLES

Forme abrégée	Expression au long
AICPA	American Institute of Certified Public Accountants
AMPTI	Avis de mise en œuvre de la Politique sur la technologie de l'information
CCC	Centre canadien pour la cybersécurité
CEI	Commission électrotechnique internationale
CST	Centre de la sécurité des télécommunications
END	Entente de non-divulgation
FedRAMP	Federal Risk and Authorization Management Program
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
GSTI	Gestion de la sécurité des technologies de l'information
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
MCI	Matrice des contrôles infonuagiques
PBMM	Protégé B, intégrité moyenne, disponibilité moyenne
PSS	Plan de sécurité des systèmes
SCT	Secrétariat du Conseil du Trésor
SOC	Service Organization Controls (AICPA)
STI	Sécurité des technologies de l'information
TI	Technologie de l'information

4.2 GLOSSAIRE

Terme	Définition
Attestation	Toute certification du domaine de la STI, qui aurait pu être reçue par les services d'un FSI donné.
Catégorie de sécurité	Caractérisation d'une activité opérationnelle selon la gravité des préjudices possibles (niveau de préjudice) résultant de la compromission de l'un des objectifs de sécurité (confidentialité, intégrité et disponibilité). [1]
Confidentialité	Fait d'être divulgué uniquement aux mandants autorisés. [1]
Contrôle de sécurité	Exigence technique, opérationnelle ou gestionnelle de haut niveau relative à la sécurité et prescrite pour un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité de ses biens de TI. [1]
Disponibilité	Fait d'être accessible et utilisable intégralement et en temps opportun. [1]
Environnement multilocataire	Environnement de systèmes d'information où les ressources physiques et virtuelles sont dynamiquement attribuées ou réattribuées de façon à servir une pluralité de clients.

Terme	Définition
Gestion des risques	Démarche systématique visant à établir la meilleure façon de procéder dans des circonstances incertaines par la détermination, l'évaluation, la compréhension et la communication des questions liées aux risques, de même que par la prise de décisions conséquentes.
Infonuagique	L'informatique en nuage (ou l'infonuagique) est un modèle convivial d'accès Web sur demande à un répertoire partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services). Mis en œuvre en un tournemain, ce modèle exige une gestion minimale et peu d'interaction avec le fournisseur du service. [5]
Intégrité	État de ce qui est précis, complet, authentique et intact. [1]
Modèle de déploiement	Motifs invoqués par les utilisateurs concernés, pour lesquels l'infrastructure infonuagique est mise en place. Pour obtenir de plus amples informations, voir le document *Special Publication 800-145, The NIST Definition of Cloud Computing* [5].
Modèle de service	Capacités offertes aux clients qui utilisent un nuage informatique. Pour obtenir de plus amples informations, voir le document *Special Publication 800-145, The NIST Definition of Cloud Computing* [5].
Profil de contrôle	Ensemble d'améliorations et de contrôles de sécurité qui constitue le minimum à réaliser pour assurer le bon fonctionnement des technologies de l'information et soutenir les systèmes d'information. [1]
Structure infonuagique	Les serveurs, les connexions haute vitesse et les commutateurs qui constituent une plateforme ou un cadre d'infonuagique.

4.3 DOCUMENTS DE RÉFÉRENCES

Numéro	Référence
1	Secrétariat du Conseil du Trésor du Canada. *Profil de contrôles de sécurité pour les services de la TI du GC fondées sur l'informatique en nuage (Protégé B, intégrité moyenne, disponibilité moyenne), version 1.1*, 28 mars 2018.
2	Centre canadien pour la cybersécurité. *ITSG-33 – La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
3	Secrétariat du Conseil du Trésor du Canada. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)*, 31 mai 2004.
4	Secrétariat du Conseil du Trésor du Canada. *Politique sur la gestion des technologies de l'information*, 29 mars 2018
5	Secrétariat du Conseil du Trésor du Canada. *Approche et procédures de gestion du risque en matière de sécurité de l'informatique en nuage, 25* juin 2018.
6	National Institute of Standards and Technology *Special Publication 800-145, The NIST Definition of Cloud Computing,* septembre 2011