Procédure d'évaluation des risques liés à la cybersécurité

ID du document : **SECSD-01**
À l'attention de: Fédération de l'Alliance
Approuvé le 2022-02-15
Approuvé par le Conseil national de la sécurité (CNS)

1. Introduction

L'évaluation des risques liés à la cybersécurité est un élément clé du cycle de vie de la gestion des risques. Le but de la présente procédure est donc de délimiter les étapes pour :

- préparer les évaluations des risques;
- procéder aux évaluations des risques;
- communiquer les résultats des évaluations des risques au personnel clé de l'organisation;
- maintenir les évaluations des risques dans le temps.

2. Définitions

Reportez-vous au document *SEC-00 Glossaire de la sécurité de l'information* pour la définition des termes utilisés dans la présente procédure.

3. Applicabilité

La présente procédure s'applique à tous les risques liés à la cybersécurité entrant dans le champ d'application de la *SEC-05 Politique de gestion des risques liés à la cybersécurité*. Les sites hôtes nationaux sont encouragés – sans y être tenus – à utiliser la même procédure pour leurs évaluations des risques liés à la cybersécurité.

3.2 Rôles et responsabilités
Reportez-vous à *SEC-05 Politique de gestion des risques liés à la cybersécurité* (paragraphe 3.2) pour les rôles et responsabilités associés à l'évaluation des risques.

4. Procédure d'évaluation des risques

4.1 Préparation

4.1.1. Les catégories nous permettent de regrouper les risques dans des domaines similaires pour la préparation de rapports. Avant de commencer une évaluation des risques, consultez l'annexe A (Catégories de risques). Les risques doivent toujours être présentés dans les rapports sous une seule catégorie. Veuillez sélectionner la catégorie qui correspond le mieux au risque à l'étude au moment de l'évaluation.

4.1.2. Assurez-vous que la portée est bien définie, documentée et comprise. Consultez la matrice d'évaluation des risques pour savoir comment déterminer le score de probabilité et d'impact.

4.1.3. Consultez *SEC-05 Politique de gestion des risques liés à la cybersécurité* (paragraphe 4.3, Réponse au risque) pour envisager les approches de traitement.

4.2 Identification

4.2.1. Identifiez l'actif, le service ou le composant qui sera évalué. Plus l'évaluation est détaillée, plus il sera facile de relever les risques distincts ou ceux qui requièrent une intervention. Gardez à l'esprit que de nombreux services comportent des dépendances et que les risques pour les dépendances doivent être évalués séparément. Reportez-vous aux exemples fournis dans l'annexe B pour plus d'information.

4.2.2. Passez en revue les menaces identifiées dans le registre des risques et répertoriez celles qui s'appliquent directement à l'actif, au service ou au composant. Si vous relevez une menace qui ne figure pas déjà dans le registre des risques, celle-ci peut être suggérée au CNS, qui envisagera de l'inclure comme une nouvelle menace. Pour ce faire, veuillez écrire à security@tech.alliancecan.ca. Enfin, il faut éviter de répertorier les menaces à l'égard des dépendances.

4.2.3. Examinez les contrôles existants liés aux menaces relevées en 4.2.2, assurez-vous qu'ils soient bien connus et préparez un résumé. Reportez-vous aux exemples fournis dans l'annexe C pour plus d'information.

4.2.4. En suivant les options de traitement des risques comme indiqué dans *SEC-05 Politique de gestion des risques de cybersécurité* (paragraphe 4.3), déterminez et consignez le plan de traitement des risques.

4.2.5. Relevez les contrôles d'atténuation dans le plan de traitement des risques et les vulnérabilités en présence, compte tenu de la manière dont le contrôle de sécurité est mis en œuvre.

4.2.6. Déterminez la probabilité résiduelle par rapport à la menace, à savoir si celle-ci pourrait compromettre l'actif ou le service, ainsi que l'impact éventuel sur l'actif ou le service.

4.3 Analyse

4.3.1. Évaluez et consignez dans le registre des risques la probabilité inhérente de ce risque en lui accordant un score de 1 à 5, tel que défini dans la matrice des risques; voir l'annexe D pour des exemples.

4.3.2. Évaluez et consignez dans le registre l'impact de ce risque en lui accordant un score de 1 à 5, tel que défini dans la matrice des risques; voir l'annexe D pour des exemples.

4.3.3. Assurez-vous que le score de risque calculé, basé sur la probabilité et l'impact, soit consigné dans le registre des risques.

4.4 Évaluation

4.4.1. Évaluez le risque en fonction de *SEC-05 Politique de gestion des risques liés à la cybersécurité* (paragraphe 4.3) et suivez les procédures de gestion des risques, au besoin.

4.4.2. En tenant compte du traitement du risque proposé, réanalysez le score de risque résiduel.

4.4.3. Documentez le traitement et le risque résiduel dans le registre des risques.

4.5 Communication

4.5.1. Une fois la confirmation obtenue auprès de la ou du propriétaire du service, assurez-vous que les résultats sont communiqués au CNS avec le niveau d'abstraction approprié, une fois les programmes d'évaluation terminés. Notez que cette façon de faire entraînera fréquemment la communication simultanée de plusieurs risques.

4.5.2. La ou le propriétaire du risque est responsable de la communication des informations à toutes les parties prenantes concernées et du partage avec la communauté des informations relatives aux risques. Reportez-vous à *SEC-05 Politique de gestion des risques liés à la cybersécurité* (paragraphe 4.6) pour plus de détails.

4.6 Maintenance

4.6.1. Le registre des risques doit être révisé régulièrement. Reportez-vous à *SEC-05 Politique de gestion des risques liés à la cybersécurité* (paragraphe 4.5) pour plus de détails.

4.6.2. Il est recommandé de planifier une révision pour assurer la réévaluation continue des risques.

5. Références

SEC-05 Politique de gestion des risques liés à la cybersécurité

Annexe A : Catégories de risques

Chaque catégorie de risques ci-dessous comprend des sous-catégories. Les risques sont consignés dans une sous-catégorie individuelle. Reportez-vous au registre des risques pour des exemples de risques déjà consignés dans les sous-catégories.

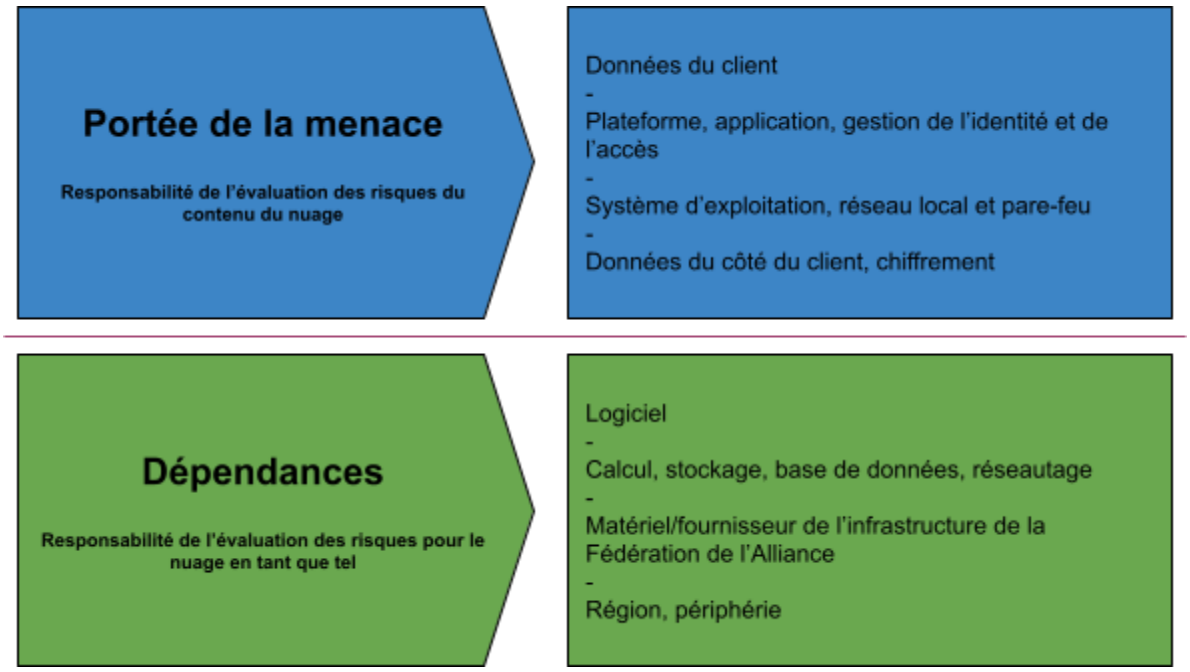
Catégorie de risques	Sous-catégories	Remarques
Ressources humaines et facteurs humains	Soutien inadéquat Compétences et connaissances insuffisantes Gestion inadéquate des ressources Inconduite d'un membre du personnel Ingénierie sociale	Inclut les risques liés aux facteurs humains tels que la formation, l'ingénierie sociale et le comportement.
Physiques	Vol de biens matériels Défaillance environnementale et catastrophe naturelle Contrôle inadéquat de la sécurité d'un centre de données	Cette catégorie inclut les risques aux actifs qui traitent, acheminent ou stockent l'information (p. ex., les serveurs, les clés USB, les câbles de réseau, etc.); les dispositifs de contrôle (par exemple, les serrures, les murs, etc.) et les environnements où se trouvent ces actifs et dispositifs (p. ex., les édifices, les salles de données, les conduits, etc.).
Exploitation du système	Flux de données non géré Mauvaise configuration Saturation des ressources Erreur de documentation Défaillance du matériel Service inutile ou non autorisé Incapacité à détecter les anomalies	Problèmes opérationnels qui créent des risques généralement liés aux ressources des systèmes, à leur disponibilité et/ou à leur bon fonctionnement et à leur configuration.
Télécommunications	Accès non autorisé à un réseau Interception des données Déni de service et congestion du réseau	Risques liés à la réseautique, y compris le déni de service (à la fois malveillant ou autre) et l'utilisation non autorisée du réseau.
Logiciel	Logiciels malveillants Cycle de vie inadéquat du logiciel Défaillance d'un logiciel Accès non autorisé à un logiciel	Risque lié au logiciel, malveillant ou autre; notez que la mauvaise configuration d'un logiciel relève de l'exploitation du système. Cela inclut les bogues et les

		vulnérabilités liés au logiciel lui-même, ou à un accès non autorisé (IP) à un logiciel.
Contrôle de l'accès et gestion des identités	Répudiation inadéquate Contrôle inadéquat de l'accès Authenticité/identité inadéquate Abus des droits d'accès Compte compromis	Tous les risques liés à la gestion de l'identité, à l'authentification, à l'autorisation et aux secrets connexes – notamment des mesures de protection insuffisantes.
Sécurité des données et confidentialité	Protection inadéquate des renseignements personnels Atteinte à la confidentialité Atteinte à l'intégrité Atteinte à la disponibilité	Risques liés aux données et à l'information : à distinguer des contrôles techniques utilisés pour les protéger. Inclut le risque si l'une de ces atteintes survenait ou en l'absence de pratiques adéquates pour les prévenir.
Gouvernance	Gestion inadéquate du cycle de vie de la gestion des services informatiques Responsabilité inadéquate Gouvernance inadéquate des documents	Risques liés à la gouvernance, généralement liés à la surveillance, aux politiques et procédures, ou à leur absence.

Annexe B

Reconnaissance de la portée

L'évaluation examinera la configuration de la portée de la menace particulière, en traçant une ligne entre la portée de la menace et les dépendances qui peuvent se créer. Les exemples ci-dessous sont basés sur une machine virtuelle installée sur un serveur à authentification multifacteur dans le nuage Arbutus.



Exemple 1 : Contrôles d'authentification insuffisants sur la machine virtuelle par rapport à des contrôles d'authentification insuffisants sur le pare-feu du centre de données.

- L'impact serait isolé sur la machine virtuelle et ses dépendances internes.
- La probabilité qu'un acteur puisse se connecter à la machine virtuelle et la probabilité que le pare-feu soit compromis ne sont pas reliées.

Exemple 2 : Système d'exploitation non corrigé par rapport à un élément non corrigé d'OpenStack Neutron.

- L'impact serait isolé sur la machine virtuelle et les applications qui résident sur ce système, ainsi que ses dépendances internes, comparativement à un impact potentiel sur tous les systèmes dans l'environnement OpenStack.
- La probabilité qu'un acteur puisse exploiter la vulnérabilité sur le système d'exploitation d'une machine virtuelle n'est pas reliée à la capacité d'exploiter la vulnérabilité dans OpenStack.

Annexe C

Exemples de contrôles existants qui sont liés aux menaces

Exemple 1 : Accès non autorisé en raison de la faible segmentation du réseau.

Exemple 2 : Compte compromis en raison de l'exposition accidentelle d'un mot de passe en clair; l'un des contrôles étant l'authentification multifacteur.

- Relevez les menaces possibles liées à la liste des catégories et sous-catégories de risques.
- Adressez-vous aux experts en sécurité et aux administrateurs de système pour consigner les contrôles actuels (description des contrôles actuels dans le registre des risques).
- Analysez les contrôles actuels comme point de référence pour déterminer le score de probabilité et d'impact.

Registre des risques

Catégorie de risques	Sous-catégorie de risques	Menaces possibles	Description des contrôles actuels
Télécommunications	Accès non autorisé au réseau	Les utilisateurs malveillants peuvent accéder à un segment de réseau au-delà de leur portée	Segmentation du réseau; Pare-feu du périmètre et pare-feu de l'hôte
Contrôle de l'accès et gestion des identités	Compte compromis	Le compte sans privilèges est compromis et peut être utilisé par des utilisateurs malveillants	Exigence que toutes les connexions à distance passent par l'authentification multifacteur

Annexe D

Exemples d'utilisation de la matrice pour obtenir des scores de risque

Dans le calcul du score de risque, il est important que tous adoptent une approche standard en rapport avec la probabilité et l'impact. Ce qui suit décrit comment aborder chaque score à partir des descriptions dans la matrice.

Probabilité						
Presque certain/s'est déjà produit	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Possible	3	3	6	9	12	15
Peu probable	2	2	4	6	8	10
Rare	1	1	2	3	4	5
		1	2	3	4	5
		Sans importance	Mineur	Modéré	Majeur	Critique
		Impact				

Probabilité :
Comme pour les exemples qui précèdent, rappelez-vous que les contrôles existants doivent être pris en compte dans l'examen de la probabilité.

- **Presque certain (5)** : se produit actuellement ou est presque certain de se produire dans un avenir prévisible.
    - Ce score signifie qu'on sait que le risque existe actuellement à d'autres endroits. Un bon exemple serait un exploit utilisé actuellement par de mauvais acteurs dans une organisation ou infrastructure similaire.

- **Probable (4)** : se produira probablement dans un avenir prévisible (s'est déjà produit dans des établissements similaires comportant des configurations et/ou des contrôles similaires).
    - Dans ce cas, on sait que la situation s'est présentée dans d'autres organisations similaires ou sur leur infrastructure, mais rien n'indique que la menace s'est concrétisée au moment où l'on se parle. Comme dans l'exemple ci-dessus, la menace peut être liée à une vulnérabilité qui a été exploitée dans des

environnements similaires, mais il n'y a aucune preuve d'une exploitation actuelle.

- **Possible (3)** : peut se produire dans un avenir prévisible (on sait que cela s'est produit ailleurs).
    - Ce score se rapporte aux risques s'étant peu fréquemment présentés dans d'autres environnements, dans une industrie, un pays ou des conditions différentes. Il n'y a cependant aucune preuve que la situation s'est produite dans des circonstances similaires.

- **Peu probable (2)** : ne se produira probablement pas dans un avenir prévisible, mais demeure possible.
    - Il n'y a aucune preuve que la situation s'est jamais présentée; cependant, le cas de figure ne nécessite pas les mêmes circonstances exceptionnelles comparativement au score 1; ce classement peut donc être distingué du score 3 (étant donné le manque de preuves) et du score 1 (étant donné que des circonstances exceptionnelles ne sont pas nécessaires pour que la situation se présente).

- **Rare (1) :** peu susceptible de se produire, sauf dans des circonstances exceptionnelles.
    - Ce score fait référence à un risque de nature quasi théorique. Les exemples incluent les inondations dans une zone qui n'a jamais été inondée, les impacts de météorites, les troubles civils causant des dommages à un centre de données, etc.

Impact

De nombreux facteurs peuvent être pris en compte lors de l'examen de l'impact (voir le tableau ci-dessous). Lorsque vous envisagez l'impact, supposez ce qui se passerait si le risque se concrétisait. Ensuite, évaluez l'impact. Examinez tous les facteurs possibles et trouvez celui qui a le score le plus élevé. C'est le score qui doit être utilisé dans le calcul du score de risque. Même si tous les autres facteurs sont sans importance, si un seul est jugé critique, le score serait alors critique.

Facteurs	Sans importance	Mineur	Modéré	Majeur	Critique
Fonctionnement	Aucun effet sur la capacité des sites à fournir tous les services à l'ensemble des utilisateurs	Les sites peuvent encore fournir tous les services critiques, mais avec une baisse d'efficacité	Les sites touchés ont perdu la capacité de fournir un service critique à un sous-ensemble d'utilisateurs du système, ou un service national est touché	Tous les sites ont perdu la capacité de fournir un service critique à un sous-ensemble d'utilisateurs du système	Tous les sites sont incapables de fournir certains services critiques aux utilisateurs
Information	Aucune information n'est exfiltrée, modifiée, supprimée ou autrement compromise	On confirme que de l'information à faible risque a été exfiltrée, modifiée, supprimée ou autrement compromise	On soupçonne que de l'information à moyen risque a été exfiltrée, modifiée, supprimée ou autrement compromise	On soupçonne que de l'information à haut ou à très haut risque a été exfiltrée, modifiée, supprimée ou autrement compromise OU On confirme que de l'information à moyen risque a été exfiltrée, modifiée, supprimée ou autrement compromise	On confirme que de l'information à haut ou à très haut risque a été exfiltrée, modifiée, supprimée ou autrement compromise
Comptes compromis	Un seul compte d'utilisateur sans privilèges est soupçonné d'avoir été compromis	Un seul compte d'utilisateur sans privilèges a été compromis	Un seul compte d'utilisateur avec privilèges est soupçonné d'avoir été compromis ou Plus d'un compte d'utilisateur a été compromis ou est soupçonné d'avoir été compromis	Un compte d'utilisateur avec privilèges a été compromis et a été utilisé dans le passé par un utilisateur qui n'y était pas autorisé OU Un nombre important de comptes d'utilisateurs ont été compromis	Un compte d'utilisateur avec privilèges a été compromis et est activement utilisé par un utilisateur qui n'y est pas autorisé et/ou Plus d'un compte d'utilisateur avec privilèges a été compromis ou est soupçonné d'avoir été compromis
Récupérabilité	Il est possible de prévoir le temps d'attente pour la reprise, à l'aide des ressources existantes du site	Il est possible de prévoir le temps d'attente pour la reprise, à l'aide des ressources internes	Il est impossible de prévoir le temps d'attente pour la reprise, à l'aide des ressources internes; une assistance externe n'est pas nécessaire	Il est impossible de prévoir le temps d'attente pour la reprise, à l'aide d'une assistance externe	L'incident a rendu la reprise impossible (p. ex., des données sensibles ont été exfiltrées et publiées); il faut lancer une enquête
Productivité et facteurs humains	Aucun impact	Perturbation minimale sur le personnel ou perte minimale de productivité (< 30 jours-personnes)	Perte de quelques emplois ou perte importante de productivité (> ou = 30 jours-personnes)	Risque de perte de vie ou de blessure non négligeable, ou pertes d'emplois majeures	Risque concret ou élevé de perte de vie ou de blessure
Réputation	Impact sans importance sur l'expérience utilisateur ou sur la perception du public	Une certaine perte de confiance en rapport avec les services touchés uniquement	Une certaine perte de confiance en rapport avec le ou les sites touchés	Importante perte de confiance en rapport avec le ou les sites touchés	Importante perte de confiance envers la Fédération de l'Alliance; le nom de l'organisation est synonyme d'inconduite et de mésaventure organisationnelle
Réglementation	L'organisme réglementaire n'est pas intéressé; la production de rapports est optionnelle	L'organisme réglementaire exige des rapports réguliers, jusqu'à la résolution	L'organisme réglementaire impose des exigences	L'organisme réglementaire exige la conformité sous peine de pénalité ou de résiliation du service	Un ou plusieurs sites sont fermés ou des dirigeants font face à des poursuites en responsabilité personnelle

Exemple 1 : Accès non autorisé en raison de la faible segmentation du réseau.

Dans cet exemple, il est prouvé qu'un accès réseau non autorisé s'est produit dans d'autres organisations semblables. Il n'y a cependant aucune preuve d'exploitation actuelle. En tenant compte des contrôles actuels tels que la segmentation du réseau, le pare-feu du périmètre et le pare-feu de l'hôte, il n'y a aucune preuve que la situation se produira dans un environnement similaire, mais c'est certainement possible. Le score de probabilité est donc de 3.

Si ce risque s'est présenté, l'examen des impacts est plus complexe et différentes personnes peuvent évaluer différents facteurs un peu différemment; cependant, lors de l'examen des impacts, le score le plus élevé qui semble raisonnable pour ce risque est Modéré (3).

En utilisant la matrice avec un impact de 3 et une probabilité de 3, on arrive à un score de risque de 9.

Exemple 2 : Le compte sans privilèges est compromis et peut être utilisé par des utilisateurs malveillants.

Dans cet exemple, nous avons la preuve que la situation s'est produite dans notre propre infrastructure, mais il n'y a aucune preuve que cela se produit actuellement. Compte tenu des contrôles actuels, il y a de fortes chances que la situation se reproduise, et le score de probabilité est donc évalué à Probable (4).

Pour l'impact, il est important de noter qu'il s'agit d'un compte sans privilèges; compte tenu de tous les facteurs en présence, on l'évalue entre Mineur (2) et Modéré (3).

En utilisant la matrice avec un impact de 3 et une probabilité de 4, on arrive à un score de risque de 12.

Exemple de simulation d'un registre des risques :

Catégorie de risques	Sous-catégorie de risques	Menaces possibles	Description des contrôles actuels	Probabilité de la menace (1–5)	Impact (1–5)	Score de risque (Probabilité × Impact) (1–25)
Télécoms	Accès non autorisé à un réseau	Les utilisateurs malveillants peuvent accéder à un segment de réseau au-delà de leur portée	Segmentation du réseau; Pare-feu du périmètre et pare-feu de l'hôte	3	3	9

Contrôle de l'accès et gestion des identités	Compte compromis	Le compte sans privilèges est compromis et peut être utilisé par des utilisateurs malveillants	Exigence que toutes les connexions à distance passent par l'authentification multifacteur	4	3	12