Politique de gestion des risques liés à la cybersécurité

ID du document: **SEC-05**
À l'attention de: Fédération de l'Alliance
Approuvé le 2022-02-15
Approuvé par le Conseil consultatif et directeur sur la cybersécurité (CCDC)

1. Introduction

Les risques liés à la cybersécurité sont un sous-ensemble du risque organisationnel. Ils concernent la confidentialité, l'intégrité et la disponibilité de la mise en œuvre, de l'exploitation et de la gestion des systèmes d'information. C'est un élément important qui doit être traité dans le cadre des responsabilités continues en matière de gestion des risques.

Le but de la présente politique est de :

- Promouvoir une culture de gestion de la cybersécurité basée sur les risques dans l'ensemble de la Fédération de l'Alliance.
- Mettre en place des structures de gouvernance appropriées pour la gestion des risques.
- Aider les personnes au sein de la Fédération de l'Alliance à comprendre leurs responsabilités face aux risques cybernétiques associés aux systèmes.
- Veiller à ce que le cycle de vie du processus de gestion des risques liés à la cybersécurité de la Fédération de l'Alliance soit mené efficacement dans toute l'organisation.

2. Définitions

En cas de divergence entre les définitions données ci-dessous et celles du Glossaire de la sécurité de l'information de la Fédération de l'Alliance, ces dernières auront préséance.

- **Risque :** Événement ou condition qui, lorsqu'il ou elle survient, affecte la capacité d'une organisation dans la réalisation de ses objectifs opérationnels ou stratégiques.

- **Gestion des risques :** Approche planifiée et systématique pour l'identification, l'évaluation, la réponse et la surveillance à l'égard des risques, afin de maximiser les opportunités et de minimiser les pertes.

- **Tolérance au risque :** Niveau de risque qu'une organisation est disposée à prendre pour atteindre ses objectifs stratégiques.

- **Propriétaire du risque :** Rôle de la personne responsable de la gestion d'un risque particulier ou d'une catégorie de risques. Il s'agit généralement d'un rôle de direction ou de gestion qui détient l'autorité et la responsabilité d'assumer les risques au nom de l'organisation, et de faire en sorte que ceux-ci soient gérés efficacement.

- **Propriétaire du service :** Rôle du ou de la principal(e) responsable de la gestion d'un service, d'une infrastructure ou d'un groupe de services; agissant sur les directives de la ou du propriétaire du risque, ce rôle inclut les interventions pour répondre à un risque, le documenter et surveiller son évolution.

- **Rendeuse ou rendeur de compte :** Rôle de la personne qui répond d'une activité ou d'une décision.

- **Responsable :** Rôle ou rôles des personnes qui ont l'obligation comme l'autorisation d'effectuer une tâche. Ce rôle peut s'ajouter à d'autres rôles.

- **Service national :** Un service faisant appel au calcul informatique de pointe (CIP) et aux capacités connexes offertes par la Fédération de l'Alliance (voir la carte des services).

3. Applicabilité

3.1 La présente politique s'applique aux risques liés à la cybersécurité qui sont associés aux personnes, aux processus et à la technologie nécessaires à la mise en œuvre, l'exploitation et la gestion des services nationaux. Les éléments qui n'ont aucune dépendance avec les services nationaux sont considérés hors de la portée des présentes.

3.2 Rôles et responsabilités (matrice « RACI »)
La matrice RACI décrit les niveaux d'intervention du CCDC, du Conseil de sécurité nationale (CNS), des propriétaires de risques, des propriétaires de services et des communications de la Fédération de l'Alliance.

	CCDC	CNS	Propriétaire du risque	Propriétaire du service	Comms
Registre des risques		RC	R	R	
Communication des risques	I	C	RC	C	R
Évaluation des risques		I	R	RC	

Réponse aux risques	I	I	RC	R	
Acceptation des risques	I	I	RC	R	
Surveillance des risques	I	R	C	RC	

RC = Rendeur de compte, R = Responsable, C = Partie consultée, I = Partie informée

Pour un risque identifié donné, le propriétaire du service et le propriétaire du risque doivent être identifiés et approuvés par les organes de gouvernance appropriés.

4. Application de la politique de gestion des risques

4.1 Propriété

Pour chaque service national, une ou un propriétaire du service et une ou un propriétaire du risque doivent être identifiés et consignés dans le registre des risques. Dans le cas où l'identification d'une ou d'un propriétaire n'est pas possible, le CCDC, en collaboration avec l'Alliance de recherche numérique du Canada, contribuera à établir les rôles.

4.2 Évaluation des risques

Les risques couverts par la présente politique doivent être évalués en suivant la procédure d'évaluation des risques de la Fédération de l'Alliance ainsi que la matrice des risques; les risques seront consignés dans le registre des risques de la Fédération de l'Alliance. Reportez-vous à la matrice des risques au paragraphe 5.

4.3 Traitement des risques

Dans la mesure du possible, tous les risques doivent être traités. Si le score de risque est de huit (8) ou plus selon la procédure d'évaluation des risques, ce risque doit être traité en temps opportun, selon les instructions du CNS. Avant d'envisager d'accepter un risque, celui-ci doit être réduit au plus petit risque résiduel possible en utilisant une ou plusieurs approches de traitement des risques – notamment :

- Atténuation/Réduction : Mise en œuvre de contrôles pour réduire la probabilité ou la conséquence du risque.
- Évitement : Décider de ne pas procéder avec les architectures ou l'activité introduisant le risque inacceptable, ou choisir une solution de rechange qui n'implique pas ce risque.
- Transfert/partage : Associer un tiers (p. ex., un assureur) pour déplacer l'impact du risque.

4.4 Acceptation du risque
L'acceptation d'un score de risque résiduel supérieur à huit (8) doit être approuvée par le propriétaire du service, en consultation avec le CCDC et doit suivre la procédure d'acceptation des risques décrite dans les procédures de gestion des risques. L'acceptation doit être documentée.

4.5 Surveillance des risques
Le registre des risques doit être révisé régulièrement, et au moins une fois par an. L'examen doit inclure une réévaluation des risques basée sur les changements relevés dans les systèmes d'information organisationnels et les environnements dans lesquels les systèmes fonctionnent. On se concentrera sur les changements à même d'affecter les risques (surveillance des changements), y compris les changements dans la faisabilité de la mise en œuvre continue des mesures de réponse aux risques. Les risques acceptés doivent être réévalués à chaque cycle. De plus, des efforts doivent être entrepris pour optimiser les mesures de réponse aux risques, dans la mesure du possible.

4.6 Communication et rapport sur les risques
Toute mise à jour du registre des risques doit être communiquée afin que les parties prenantes appropriées de la Fédération de l'Alliance soient informées des risques et de leur traitement. Les modifications importantes doivent faire l'objet d'un rapport au CCDC.

5. Information connexe

SEC-00 Glossaire de la sécurité de l'information
Procédure d'évaluation des risques
Registre des risques de la Fédération de l'Alliance
Matrice des risques

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				