Cadre de gestion des risques liés au respect de la vie privée et à la sécurité

Institut canadien d'information sur la santé
Canadian Institute for Health Information

La production du présent document est rendue possible grâce à un apport financier de Santé Canada et des gouvernements provinciaux et territoriaux. Les opinions exprimées dans ce rapport ne représentent pas nécessairement celles de Santé Canada ou celles des gouvernements provinciaux et territoriaux.

À moins d'indication contraire, les données utilisées proviennent des provinces et territoires du Canada.

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
icis.ca
droitdauteur@icis.ca

Comment citer ce document :
Institut canadien d'information sur la santé. *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité*. Ottawa, ON : ICIS; 2020.

This publication is also available in English under the title *Privacy and Security Risk Management Framework*.

Table des matières

1 Introduction

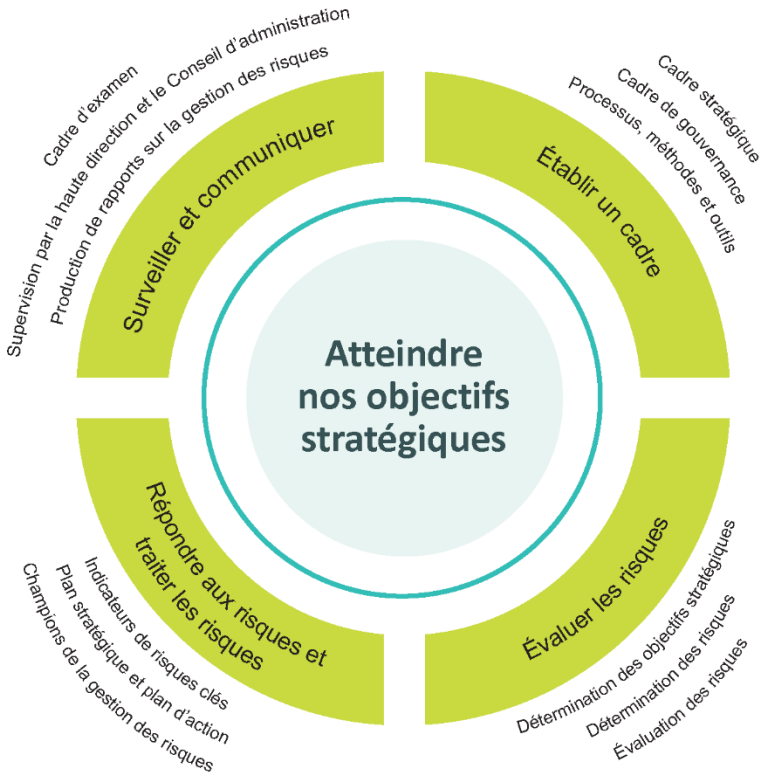
1.1 Aperçu

La gestion des risques en matière de respect de la vie privée et de sécurité est un processus officiel pouvant être reproduit. Elle vise la détection, l'évaluation, la prise en charge et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leur incidence possible.

Le présent Cadre de gestion des risques liés au respect de la vie privée et à la sécurité donne un aperçu de la gestion des risques en matière de respect de la vie privée et de sécurité à l'Institut canadien d'information sur la santé (ICIS), notamment son harmonisation avec le cadre de gestion des risques de l'ICIS, les facteurs qui en sont à l'origine, le modèle de gouvernance, la tolérance aux risques de l'ICIS et la méthodologie.

2 Harmonisation avec le cadre de gestion des risques de l'ICIS

Le Cadre de gestion des risques liés au respect de la vie privée et à la sécurité a été conçu de façon à s'harmoniser au cadre de gestion des risques de l'ICIS illustré ci-dessous et à s'y intégrer.



La gestion des risques liés au respect de la vie privée et à la sécurité oriente les activités de gestion des risques de l'ICIS et s'y harmonise puisqu'elle

- repose sur une méthodologie, une terminologie et une structure de gouvernance semblables;
- permet de déceler les risques liés au respect de la vie privée et à la sécurité qui pourraient être inclus au registre des risques.

3 Pourquoi la gestion des risques liés au respect de la vie privée et à la sécurité?

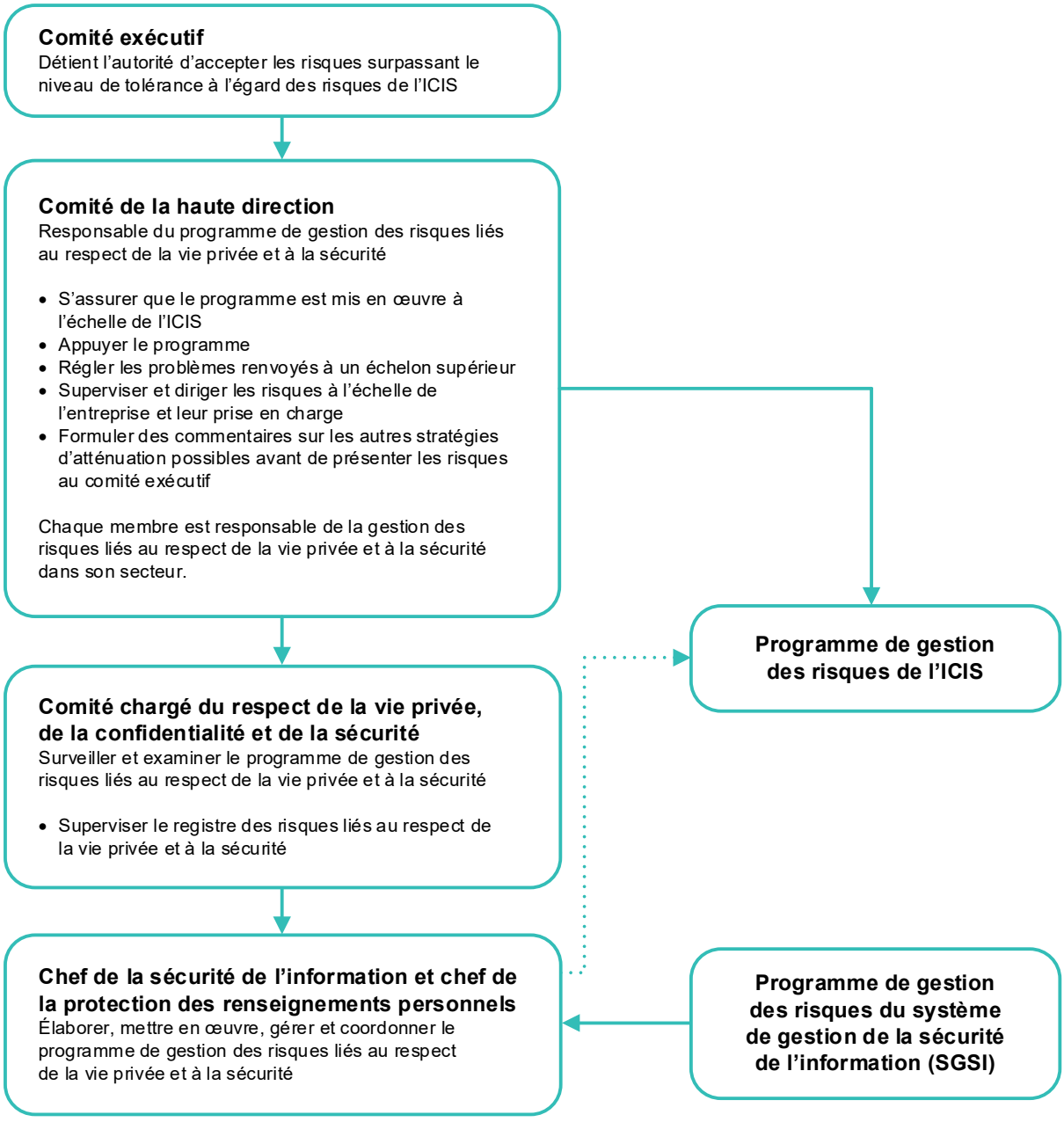
Une gestion efficace des risques liés au respect de la vie privée et à la sécurité est essentielle pour permettre à l'ICIS d'atteindre ses objectifs stratégiques, et il s'agit d'une exigence fondamentale au statut d'entité prescrite qui lui est conféré en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) de l'Ontario.

L'adoption d'un programme efficace et rigoureux de gestion des risques en matière de respect de la vie privée et de sécurité aide à maintenir la confiance des intervenants et du public puisqu'elle démontre que l'ICIS accorde une grande importance à la protection des renseignements personnels sur la santé dont il a la garde.

En mettant en œuvre un processus continu, proactif et systématique permettant de comprendre, de gérer et de communiquer les risques liés au respect de la vie privée et à la sécurité, l'ICIS pourra prendre de bonnes décisions stratégiques et tactiques fondées sur les risques, les coûts et les avantages réels.

4 Gouvernance de la gestion des risques

Le chef de la sécurité de l'information et le chef de la protection des renseignements personnels sont les principaux responsables du programme de gestion des risques liés au respect de la vie privée et à la sécurité de l'ICIS. L'ICIS a défini des responsabilités en matière de gestion et un cadre de gouvernance pour la gestion efficace des risques liés au respect de la vie privée et à la sécurité, comme l'illustre la figure ci-dessous.



5 Tolérance de l'ICIS à l'égard des risques

Il n'est pas toujours efficace ou possible d'éliminer les risques en raison du temps, des coûts ou des efforts nécessaires, ou d'autres contraintes. Cependant, des risques qui vont nettement à l'encontre de la vision, du mandat et des objectifs stratégiques de l'ICIS peuvent être jugés inacceptables. C'est pourquoi l'ICIS a élaboré un énoncé sur la tolérance à l'égard des risques liés au respect de la vie privée et à la sécurité qui indique le degré de risques résiduels que l'organisme est prêt à accepter dans le cadre des pratiques normales de gestion.

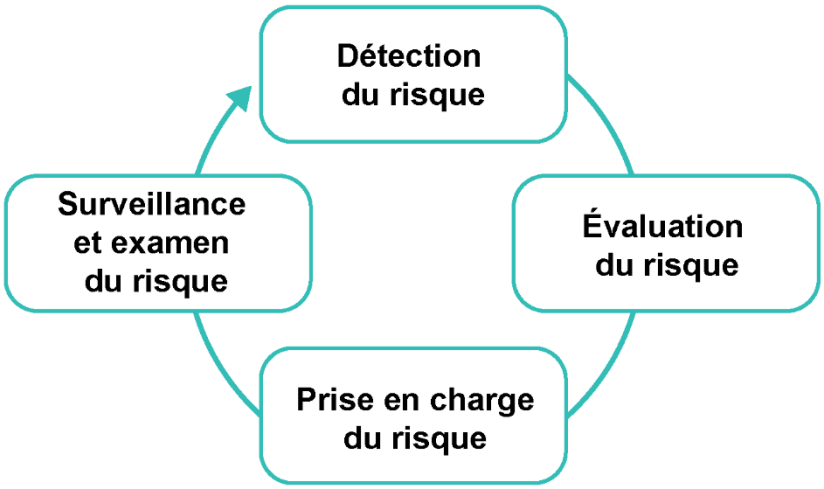
L'ICIS est prêt à accepter les risques qui

- peuvent entraîner de légers retards dans l'atteinte de ses objectifs;
- n'entraînent pas de pertes financières;
- peuvent entraîner des plaintes, une couverture médiatique négative et des problèmes de non-conformité qui sont sans gravité;
- peuvent avoir certaines répercussions sur la perception du public;
- peuvent soulever de légères préoccupations chez les intervenants;
- peuvent avoir une incidence minime sur la prestation des services.

Si ces risques surviennent, leurs conséquences pourraient être atténuées par les activités normales ou exiger peu d'efforts.

Tolérance de l'ICIS à l'égard des risques liés au respect de la vie privée et à la sécurité : **FAIBLE**

6 Méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité



La méthodologie de gestion des risques liés au respect de la vie privée et à la sécurité de l'ICIS est composée des 4 étapes suivantes :

1. **Détection du risque :** les risques sont détectés au moyen de diverses sources et sont inscrits dans le registre des risques liés au respect de la vie privée et à la sécurité.
2. **Évaluation du risque :** la probabilité d'un risque et son incidence possible sont évalués afin de déterminer si le risque doit être pris en charge. Les risques mentionnés dans l'énoncé de tolérance aux risques de l'ICIS ne nécessitent aucune prise en charge.
3. **Prise en charge du risque :** les options de prise en charge du risque sont l'atténuation, le transfert, l'évitement ou l'acceptation du risque.
4. **Surveillance et examen du risque :** les risques et les mesures de prise en charge connexes doivent être surveillés continuellement pour veiller à ce que les actifs informationnels de l'ICIS soient adéquatement protégés.

Annexe : Texte de remplacement pour les figures

Texte de remplacement du cadre de gestion des risques de l'ICIS

Première étape : établir le cadre (c'est-à-dire le cadre stratégique, le cadre de gouvernance, le processus, les méthodes et les outils). Deuxième étape : évaluer les risques (c'est-à-dire procéder à la détermination des objectifs stratégiques et des risques et à l'évaluation des risques). Troisième étape : répondre aux risques et les traiter (c'est-à-dire les indicateurs de risques clés, le plan stratégique et le plan d'action, et les champions de la gestion des risques). Quatrième étape : surveiller et communiquer (c'est-à-dire l'examen du cadre, la supervision par la haute direction et le Conseil d'administration, et la production de rapports sur la gestion des risques).

Texte de remplacement pour le cadre de gouvernance

Le comité exécutif de l'ICIS détient l'autorité d'accepter les risques surpassant le seuil de tolérance aux risques de l'ICIS.

Le comité de la haute direction est responsable du programme de gestion des risques liés au respect de la vie privée et à la sécurité. Il

- s'assure que le programme est mis en œuvre à l'échelle de l'ICIS;
- appuie le programme;
- règle les problèmes renvoyés à un échelon supérieur;
- supervise et dirige les risques à l'échelle de l'entreprise et leur prise en charge;
- formule des commentaires sur les autres stratégies d'atténuation possibles avant de présenter les risques au comité exécutif.

Chaque membre est responsable de la gestion des risques liés au respect de la vie privée et à la sécurité de son secteur.

Le comité chargé du respect de la vie privée, de la confidentialité et de la sécurité surveille et examine le programme de gestion des risques liés au respect de la vie privée et à la sécurité, ainsi qu'il supervise le registre des risques liés au respect de la vie privée et à la sécurité.

Le chef de la sécurité de l'information et le chef de la protection des renseignements personnels élaborent, mettent en œuvre, gèrent et coordonnent le programme de gestion des risques liés au respect de la vie privée et à la sécurité.

Le comité de la haute direction, le chef de la sécurité de l’information et le chef de la protection des renseignements personnels formulent des commentaires sur le programme de gestion des risques de l’ICIS.

Le programme de gestion des risques du système de gestion de la sécurité de l’information (SGSI) de l’ICIS oriente les activités du programme de gestion des risques liés au respect de la vie privée et à la sécurité.

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 602
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

22660-0720