



Centre de la sécurité
des télécommunications

Communications
Security Establishment

CENTRE CANADIEN POUR LA **CYBERSÉCURITÉ**

Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie **Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée**

Praticien·nes

Avant-propos

L'ITSP.10.036, Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal, Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

La présente publication remplace l'annexe 1 – Activités de gestion des risques liés à la sécurité des TI du document La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33).

Pour obtenir de plus amples renseignements ou suggérer des modifications, veuillez communiquer avec le Centre pour la cybersécurité :

- par courriel : contact@cyber.gc.ca
- par téléphone : [613-949-7048](tel:613-949-7048) ou [1-833-CYBER-88](tel:1-833-CYBER-88).

Date d'entrée en vigueur

Cette publication entre en vigueur le 14 septembre 2026.

Historique des révisions

Révision	Modifications	Date
1	Première version	14 septembre 2026

D97-3/10-036-2026F-PDF

ISBN 978-1-100-00242-2

Vue d'ensemble

La présente publication fait partie d'une série de lignes directrices publiées par le Centre pour la cybersécurité, conformément au document Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie. Elle décrit un processus de gestion des risques pour la cybersécurité et la vie privée qui comprend des activités au niveau organisationnel.

La présente publication a été créée comme outil pour faciliter le travail des praticiennes et praticiens de la sécurité et de la protection de la vie privée chargés de la protection des organisations conformément aux lois, aux politiques, aux directives et aux normes applicables. Elle décrit un cadre de gestion des risques conçu pour s'assurer que les organisations gèrent efficacement les risques et obtiennent l'approbation des autorités appropriées par rapport à ces risques.

Cette publication met l'accent sur les quatre objectifs principaux qui orientent les organisations et leur permettent de gérer efficacement les risques et d'assurer la conformité :

- déterminer et comprendre les besoins des programmes et des services de l'organisation en matière de cybersécurité et de protection de la vie privée et sélectionner un ensemble d'activités et de contrôles sur mesure qui répondent à ces besoins;
- attribuer des contrôles de sécurité qui satisfont aux besoins en matière de cybersécurité et de protection de la vie privée, ainsi qu'aux exigences relatives à la cybersécurité et à la gestion des risques découlant de la réglementation, des politiques, des directives et des normes applicables (pour le gouvernement du Canada [GC], notamment les instruments de politique du Secrétariat du Conseil du Trésor du Canada [SCT]);
- surveiller et évaluer continuellement le niveau de performance des activités et des contrôles en matière de sécurité et de protection de la vie privée pour détecter les incidents et relever les vulnérabilités et les lacunes de façon opportune;
- mettre à jour les activités et les contrôles mis en œuvre de manière à intervenir en cas d'incident, à corriger les vulnérabilités et à améliorer continuellement la posture des systèmes organisationnels en ce qui a trait à la cybersécurité et à la protection de la vie privée.

Remarque propre au GC

Dans le GC, le respect des lignes directrices énoncées dans le document Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie offre de nombreux avantages pour les organismes, notamment :

- la conformité à la stratégie globale de gestion des risques et aux objectifs fixés par le SCT;
- la prise en compte des principaux aspects liés à la cybersécurité et à la protection de la vie privée;
- une gestion efficace, uniforme et rentable des risques pour cybersécurité et la protection de la vie privée.

Table des matières

1	Introduction.....	7
1.1	Objet.....	7
1.2	Contexte au sein du gouvernement du Canada.....	7
1.3	Portée et applicabilité.....	8
1.4	Auditoire.....	9
1.5	Hiérarchie de la publication	10
1.6	Organisation de la publication.....	11
2	Processus de gestion des risques pour la cybersécurité et la vie privée	12
3	Relations avec les processus externes.....	15
4	Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée	16
4.1	Définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée	19
4.1.1	Définir la portée des activités d'évaluation des risques pour la cybersécurité et la vie privée	19
4.1.2	Définir les besoins opérationnels en matière de sécurité et de protection de la vie privée.....	20
4.1.3	Procéder à l'évaluation et à la catégorisation du préjudice associé aux activités opérationnelles de l'organisation.....	21
4.1.4	Sélectionner la méthodologie d'évaluation des menaces et des risques pour la cybersécurité de l'organisation	22
4.1.5	Sélectionner la méthodologie d'évaluation de la protection de la vie privée de l'organisation.....	22
4.1.6	Procéder à l'évaluation organisationnelle des menaces à la cybersécurité.....	23
4.2	Élaborer les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée	24
4.2.1	Définir les domaines opérationnels.....	25
4.2.2	Définir les approches architecturales à la sécurité.....	26
4.2.3	Sélectionner les activités et les contrôles organisationnels de sécurité et de protection de la vie privée	27
4.2.4	Approuver le ou les profils de l'organisation.....	29
4.3	Attribuer les activités et les contrôles de sécurité et de protection de la vie privée	30
4.3.1	Attribuer les activités et les contrôles communs	30
4.3.2	Attribuer les activités et les contrôles propres au système.....	31
4.4	Surveiller et évaluer le niveau de performance des activités et des contrôles en matière de sécurité et de protection de la vie privée	32

4.5	Maintenir l'autorisation	33
4.6	Mettre à jour le ou les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée	34
5	Processus d'évaluation et de catégorisation du préjudice	36
5.1	Concepts	36
5.1.1	Systèmes de sécurité nationale	36
5.1.2	Sécurité	37
5.1.3	Protection de la vie privée	37
5.1.4	Perspective adverse	38
5.1.5	Préjudice post-compromission	38
5.2	Processus d'évaluation et de catégorisation du préjudice	38
5.3	Description du processus d'évaluation et de catégorisation du préjudice	42
5.3.1	Élaborer le tableau d'évaluation du préjudice propre à l'organisation	42
5.3.2	Déterminer les processus organisationnels et les ressources informationnelles connexes	45
5.3.3	Évaluer les préjudices découlant d'une compromission liée aux menaces	46
5.3.4	Déterminer la catégorie de préjudice associée à chaque activité opérationnelle	48
5.3.5	Préparer le rapport de catégorisation du préjudice	48
5.4	Exemples	48

Liste des figures

Figure 1 :	Processus de gestion des risques pour la cybersécurité et la vie privée	12
Figure 2 :	Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée	17
Figure 3 :	Processus d'évaluation et de catégorisation du préjudice	39

Liste des tableaux

Tableau 1 :	Exemples d'attribution d'activités et de contrôles communs	31
Tableau 2 :	Exemples de types et de niveaux de préjudice (dans le contexte du GC)	42
Tableau 3 :	Exemples de types et de niveaux de préjudice	44

Tableau 4 :	Confidentialité – Intérêt non national (PROTÉGÉ)	50
Tableau 5 :	Confidentialité – Intérêt national (Classifié)	50
Tableau 6 :	Intégrité et disponibilité	50

Liste des annexes

Annexe A	Conversion des niveaux de préjudice du gouvernement du Canada	50
----------	---	----

1 Introduction

Le processus mentionné dans la présente publication décrit un cadre de gestion des risques conçu pour s'assurer que les organisations gèrent efficacement les risques pour la cybersécurité et la vie privée et obtiennent l'approbation des autorités appropriées par rapport à ces risques. Cette publication propose également des spécifications sur la façon d'effectuer une évaluation et une catégorisation du préjudice dans le cadre de la gestion des risques. Il est possible d'adapter le processus décrit dans la présente publication de manière à répondre aux besoins de votre organisation.

1.1 Objet

La présente publication fait partie d'une série de lignes directrices publiées par le Centre pour la cybersécurité, conformément au document *Gestion des risques liés à la cybersécurité et à la vie privée* : Une méthode axée sur le cycle de vie. Elle vise à soutenir les organisations lors de la mise en œuvre d'une approche structurée à la gestion des risques. Cette publication décrit un ensemble d'activités qui aideront les organisations à déterminer et à atteindre un niveau approprié de sécurité qui convient à leurs exigences organisationnelles et au contexte opérationnel. Elle fournit également des conseils sur la structuration d'un cadre d'évaluation et d'autorisation de sécurité (EAS), lequel officialise la façon dont les risques pour la cybersécurité sont évalués, documentés et gérés dans l'ensemble d'une organisation. Elle décrit la façon de procéder à l'évaluation et à la catégorisation d'un préjudice découlant des processus opérationnels de l'organisation et de l'information connexe selon leur incidence potentielle sur la confidentialité, l'intégrité et la disponibilité (CID).

1.2 Contexte au sein du gouvernement du Canada

Dans sa [Directive sur la gestion de la sécurité](#) (DGS), le SCT confère aux hautes et hauts fonctionnaires de la gouvernance de la sécurité ministérielle la responsabilité de participer au processus et d'en faire rapport au ministère. Il leur incombe également d'affecter les responsabilités liées à la sécurité des programmes, des services et des activités.

La DGS du SCT stipule que les hautes et hauts fonctionnaires de la gouvernance de la sécurité ministérielle doivent déterminer les exigences de sécurité et les besoins connexes en matière de ressources pour les programmes. Elle leur conseille aussi de s'assurer que les pratiques et les contrôles de sécurité sont bien définis, documentés, mis en œuvre, surveillés et tenus à jour pour répondre aux exigences de sécurité applicables aux programmes, aux services et aux activités. Il est impératif que ces hautes et hauts fonctionnaires documentent ou recommandent les mesures à prendre par rapport aux risques résiduels associés aux programmes, aux services et aux activités. Elles et ils doivent établir les processus visant à surveiller les menaces, les vulnérabilités, les incidents de sécurité et les autres événements de sécurité, à prendre les mesures nécessaires pour intervenir et à en faire rapport. Il leur incombe de gérer les événements de sécurité qui pourraient avoir une incidence sur les programmes, les services et les activités ou ceux qui exigent une prise de mesures immédiate ou coordonnée à l'échelle du gouvernement. Elles et ils doivent surveiller l'efficacité des pratiques et des contrôles de sécurité, en faire rapport et communiquer les résultats à la dirigeante principale ou au dirigeant principal de la sécurité (DPS).

La [Loi sur la protection des renseignements personnels](#) (LPRP) fédérale, parallèlement à l'[ensemble de gouvernance de la protection de la vie privée](#) du SCT, stipule que le mandat d'assurer la conformité aux exigences législatives et politiques revient aux hautes et hauts fonctionnaires et aux gardiennes et gardiens de l'information qui supervisent les programmes

visant à collecter et à utiliser les renseignements personnels. Par ailleurs, la responsabilité d'évaluer la conformité à ces activités est confiée à la ou au chef de l'organisme gouvernemental, bien que ce rôle soit souvent délégué concrètement à une haute ou un haut fonctionnaire.

La gestion des risques pour la cybersécurité chevauche la gestion des risques pour la vie privée dans la mesure où les données comportant des renseignements personnels sont de plus en plus présentes dans les systèmes d'information tout au long du cycle de vie des données. Des atteintes à la vie privée peuvent survenir lors d'incidents de cybersécurité si une perte de confidentialité et/ou d'intégrité est constatée durant le traitement des données. La présente publication aborde les risques d'atteinte à la vie privée dans le seul contexte des systèmes informatiques.

Le [Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée \(ITSP.10.033\)](#) comprend maintenant des activités et des contrôles de protection de la vie privée pour veiller à ce que les institutions gouvernementales protègent et gèrent les renseignements personnels. Ces nouveaux ajouts facilitent la détermination, l'évaluation, la surveillance et l'atténuation des lacunes sur le plan de la conformité qui existent dans les activités et les programmes dans le cadre desquels des renseignements personnels sont collectés, créés, conservés, utilisés, divulgués et éliminés. Ils visent également à s'assurer que la protection de la vie privée est prise en compte dans l'architecture, puis la conception et l'exploitation des systèmes d'information du GC.

Les organisations mettent en pratique les [Directives sur les pratiques relatives à la protection de la vie privée – Annexe C : Norme sur l'évaluation des facteurs relatifs à la vie privée](#) de manière à soutenir cet objectif et veillent à ce que les implications relatives à la protection de la vie privée soient correctement déterminées, évaluées et résolues avant la mise en place d'une activité ou d'un programme nouveau ou considérablement modifié comportant des renseignements personnels. L'évaluation des facteurs relatifs à la vie privée (EFVP) est la composante de la gestion des risques qui vise à assurer la conformité aux exigences stipulées dans la LPRP. Elle évalue également les implications relatives à la protection de la vie privée pour les activités et les programmes nouveaux ou considérablement modifiés comportant des renseignements personnels. Les EFVP devraient être effectuées d'une manière proportionnelle aux facteurs relatifs à la vie privée qui ont été déterminés et conforme à l'environnement d'exploitation de l'institution gouvernementale.

1.3 Portée et applicabilité

La présente publication propose aux organisations des lignes directrices sur les activités de gestion des risques pour la cybersécurité et la vie privée qui sont menées par des fonctions responsables de la cybersécurité et de la protection de la vie privée dans le cadre d'un programme de cybersécurité organisationnel. Le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037) fournit les lignes directrices sur les activités de gestion des risques pour la cybersécurité et la vie privée qui sont effectuées au niveau des systèmes.

Le respect de ces lignes directrices offre de nombreux avantages pour les organisations. Il leur est notamment possible d'adopter une stratégie et des objectifs établis en matière de gestion des risques, de s'attaquer aux principaux aspects de la cybersécurité et de la protection de la vie privée de manière efficace et de gérer de façon uniforme et rentable les risques pour la cybersécurité et la vie privée.

Remarque propre au GC

Les lignes directrices mentionnées dans la présente publication s'appliquent aux ministères et organismes¹ sujets à la [Politique sur la sécurité du gouvernement \(PSG\)](#) du SCT, qui ont recours à des systèmes d'information pour soutenir des activités, des programmes et des services non critiques à critiques dans des environnements non classifiés, protégés et classifiés. Il est impératif que les ministères fédéraux désignés se conforment aux exigences stipulées dans la PSG et ses instruments complémentaires.

1.4 Auditoire

Cette publication vise à aider un public varié, notamment :

- les personnes exerçant des responsabilités de niveau organisationnel, dont les architectes d'entreprise et les architectes de sécurité d'entreprise;
- les personnes ayant des responsabilités liées au développement de systèmes, y compris les propriétaires de la mission ou des activités, les gestionnaires de programmes, les ingénieures et ingénieurs de systèmes, les ingénieures et ingénieurs de la sécurité des systèmes, les praticiennes et praticiens de la protection de la vie privée, les développeuses et développeurs de matériel et de logiciels, les intégratrices et intégrateurs de systèmes, ainsi que les responsables et les cadres chargées et chargés de l'acquisition et de l'approvisionnement;
- les personnes exerçant des responsabilités liées à la logistique et à la disposition, y compris les gestionnaires de programmes, les responsables ou les cadres chargées et chargés de l'approvisionnement, les intégratrices et intégrateurs de systèmes et les gestionnaires immobilières ou immobiliers;
- les personnes exerçant des responsabilités liées aux opérations et à la mise en œuvre de la sécurité et de la protection de la vie privée, y compris les propriétaires de la mission ou des activités, les propriétaires de systèmes, les gardiennes et gardiens de l'information, les administratrices et administrateurs de systèmes, les planificatrices et planificateurs de la continuité et les agentes et agents de la sécurité des systèmes et de la protection de la vie privée;
- les personnes exerçant des responsabilités liées à la surveillance et à l'évaluation de la sécurité et de la protection de la vie privée, y compris les vérificatrices et vérificateurs, les évaluatrices et évaluateurs de systèmes, les évaluatrices et évaluateurs des contrôles, les vérificatrices et vérificateurs indépendants, les responsables de la validation et les analystes;
- les hautes et hauts fonctionnaires ou cadres supérieures et supérieurs en matière de sécurité et de protection de la vie privée (par exemple, les dirigeantes principales ou dirigeants principaux de l'information [DPI], les DPS et les chefs de la protection des renseignements personnels [CPRP]);

¹ On entend les ministères définis à l'article 2 et les entités figurant aux annexes IV et V de la [Loi sur la gestion des finances publiques](#), à l'exception de celles qui sont expressément exclues en vertu d'une loi, d'un règlement ou d'un décret.

- les entités commerciales, y compris les partenaires de l'industrie, qui fabriquent des produits et des systèmes de composants, élaborent des technologies liées à la sécurité et à la protection de la vie privée, ou fournissent des services ou des capacités qui soutiennent la cybersécurité ou la protection de la vie privée.

Remarque propre au GC

Dans le GC, la présente publication s'adresse au public cité ci-dessus, ainsi qu'aux personnes qui soutiennent les activités de gestion des risques pour la cybersécurité et la vie privée, comme :

- les personnes exerçant des responsabilités associées à la gestion et à la surveillance des systèmes, de la sécurité de l'information, de la protection de la vie privée ou des risques, y compris les DPI, les DPS, les cadres supérieures et supérieurs de la gouvernance de la sécurité du ministère, les agentes désignées et agents désignés pour la cybersécurité et les hautes et hauts fonctionnaires ou cadres supérieures et supérieurs en matière de protection de la vie privée appropriés;
- les CPRP, les cadres supérieures et supérieurs avec délégation de pouvoirs en vertu de la LPRP et les praticiennes et praticiens de la protection de la vie privée;
- les personnes qui participent à la définition, à la conception, au développement, à l'installation et à l'exploitation des systèmes d'information et plus particulièrement les autorisatrices et autorisateurs, les gestionnaires de projet, les architectes de la cybersécurité, les ingénieures et ingénieurs de la cybersécurité, les évaluatrices et évaluateurs de la cybersécurité et les membres des groupes responsables des opérations de cybersécurité.

1.5 Hiérarchie de la publication

La présente publication fait partie d'une série de lignes directrices relevant du document Gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie. Les documents de la série se présentent comme suit :

- Aperçu de la gestion des risques liés à la cybersécurité et à la vie privée : Une méthode axée sur le cycle de vie (ITSP.10.035)
- Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée (ITSP.10.036)
- Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037)
- [Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée \(ITSP.10.033\)](#)
- [Proposition de profil d'activités et de contrôles organisationnels de sécurité et de protection de la vie privée – Incidence moyenne \(ITSP.10.033-01\)](#)
- Évaluation des contrôles et des activités d'assurance de la sécurité et de la protection de la vie privée (ITSP.10.033-02)

1.6 Organisation de la publication

La suite de cette publication sera structurée comme suit :

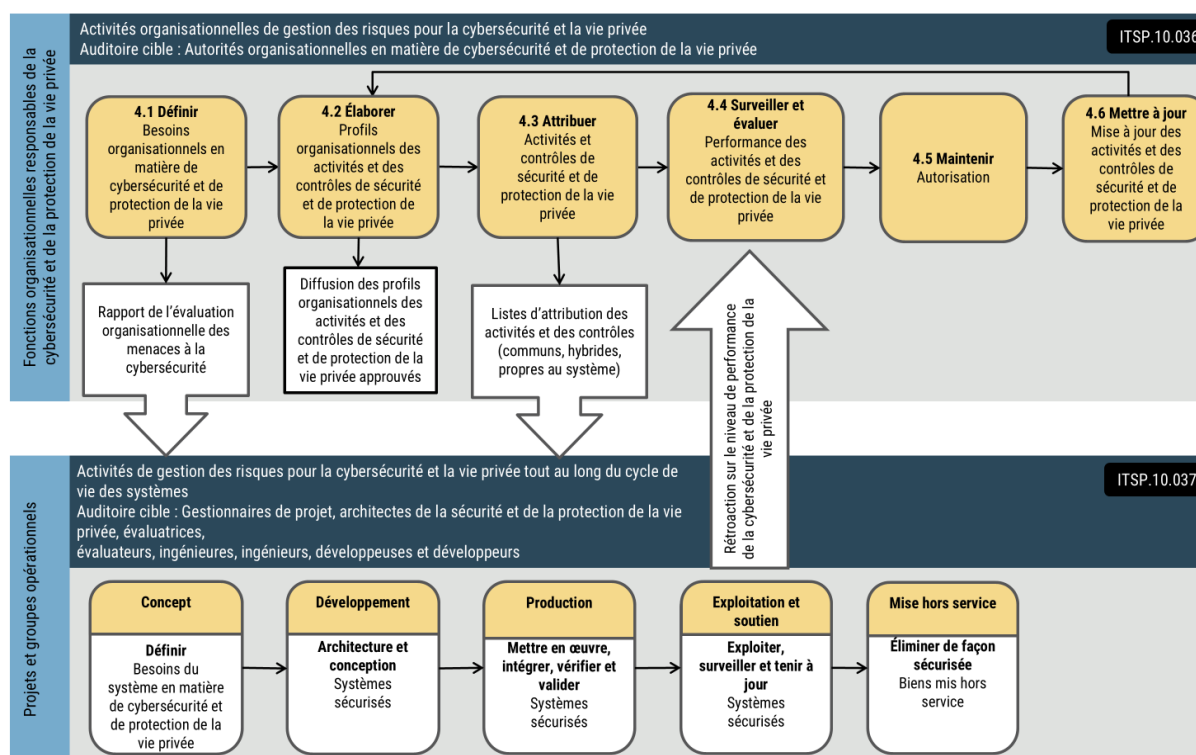
- la [section 2 – Processus de gestion des risques pour la cybersécurité et la vie privée](#) présente le processus de gestion des risques pour la cybersécurité et la vie privée de façon générale et explique comment il influe sur le processus au niveau du système que l'on retrouve dans l'ITSP.10.037;
- la [section 3 – Relations avec les processus externes](#) décrit comment le processus de gestion des risques pour la cybersécurité et la vie privée interagit avec les processus externes;
- la [section 4 – Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée](#) décrit le processus détaillé de gestion des risques pour la cybersécurité et la vie privée au sein d'une organisation;
- la [section 5 – Processus d'évaluation et de catégorisation du préjudice](#) présente le processus d'évaluation et de catégorisation du préjudice, notamment les définitions des principaux concepts et des exemples concrets.

2 Processus de gestion des risques pour la cybersécurité et la vie privée

Afin de gérer les risques pour la cybersécurité et la vie privée avec efficacité et de manière à optimiser les coûts, les documents ITSP.10.036 et ITSP.10.037 décrivent une approche que les organisations peuvent adapter selon leur culture, leur mission, leurs objectifs organisationnels, leurs besoins opérationnels en matière de sécurité et de protection de la vie privée et les menaces qui pèsent sur leurs activités.

La [figure 1](#) illustre le processus de gestion des risques pour la cybersécurité et la vie privée suggérés dans les documents ITSP.10.036 et ITSP.10.037. Elle démontre que les activités de gestion des risques pour la cybersécurité et la vie privée sont menées à deux niveaux distincts dans une organisation : au niveau organisationnel et au niveau des systèmes.

Figure 1 : Processus de gestion des risques pour la cybersécurité et la vie privée



Description longue – Figure 1 : Processus de gestion des risques pour la cybersécurité et la vie privée

Cette figure définit les activités organisationnelles générales de gestion des risques pour la cybersécurité et la vie privée. Elle décrit également les activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes qui sont menées dans le cadre de projets et au sein de groupes opérationnels. Elle souligne le fait que les activités de gestion des risques pour la cybersécurité et la vie privée aux deux niveaux agissent de concert dans un cycle continu pour maintenir et améliorer efficacement la posture de sécurité des systèmes organisationnels.

La figure **Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée** est destinée aux autorités organisationnelles à cet égard et regroupe les étapes suivantes :

4.1 Définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée

- Transmission du rapport organisationnel d'évaluation des cybermenaces aux équipes de projet et aux groupes opérationnels responsables des activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes

4.2 Élaborer les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée

- Diffusion des profils organisationnels des activités et des contrôles de sécurité et de protection de la vie privée approuvés

4.3 Attribuer les activités et les contrôles de sécurité et de protection de la vie privée

- Transmission des listes d'attribution des activités et des contrôles (communs, hybrides ou propres au système) aux équipes de projet et aux groupes opérationnels responsables des activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes

4.4 Surveiller et évaluer le niveau de performance des activités et des contrôles en matière de sécurité et de protection de la vie privée

4.5 Maintenir l'autorisation

4.6 Mettre à jour le ou les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée

- Retour à l'étape 2, Élaborer les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée

Les activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes, qui sont menées par les équipes de projet et les groupes opérationnels, s'adressent notamment aux gestionnaires de projet, aux architectes de sécurité et de protection de la vie privée, aux évaluatrices et évaluateurs, aux ingénieures et ingénieurs ainsi qu'aux développeuses et développeurs. Elles comprennent les étapes suivantes :

1. Concept : Définir les besoins du système en matière de cybersécurité et de protection de la vie privée
2. Développement : Élaborer l'architecture et la conception des systèmes sécurisés
3. Production : Mettre en œuvre, intégrer, vérifier et valider les systèmes sécurisés
4. Exploitation et soutien : Assurer l'exploitation, la surveillance et la maintenance des systèmes sécurisés
 - Transmission de la rétroaction sur le niveau de performance en matière de cybersécurité et de protection de la vie privée aux autorités organisationnelles responsables de la cybersécurité et de la protection de la vie privée afin d'éclairer l'étape 4, Surveiller et évaluer le niveau de performance des activités et des contrôles en matière de sécurité et de protection de la vie privée
5. Mise hors service : Éliminer les biens de façon sécurisée lors de leur mise hors service

Au niveau de l'organisation, ce qui fait l'objet de la présente publication, les activités de gestion des risques pour la cybersécurité et la vie privée sont effectuées par les fonctions responsables de la cybersécurité et de la protection de la vie privée dans l'organisation (voir la [section 4](#)). Pour mener à bien ce processus, les programmes organisationnels de cybersécurité et de protection de la vie privée doivent collaborer étroitement, puisque leurs objectifs pourraient converger et être complémentaires. Les objectifs de ces activités consistent à faire ce qui suit :

- définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée, ainsi que les activités et les contrôles connexes;
- attribuer la responsabilité pour les activités et les contrôles de sécurité et de protection de la vie privée;
- surveiller et évaluer continuellement le niveau de performance des activités et des contrôles attribués;
- établir les mises à jour à appliquer aux activités et aux contrôles (changements apportés aux activités et aux contrôles existants ou ajout d'activités et de contrôles) selon les résultats des activités de surveillance continue, d'évaluation et de maintien des autorisations, et superviser la mise en œuvre de ces mises à jour.

Au niveau du système, les activités de gestion des risques pour la cybersécurité et la vie privée sont effectuées par les projets de technologies de l'information (TI) et de technologie opérationnelle (TO) et les groupes opérationnels de TI et de TO. Ceux-ci suivent les phases de mise en œuvre, d'exploitation et d'élimination des systèmes décrites dans le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037). Les objectifs des activités au niveau des systèmes consistent à faire ce qui suit :

- définir les besoins en matière de cybersécurité et de protection de la vie privée ainsi que les activités et les contrôles connexes pour les systèmes basés sur les activités menées par les fonctions responsables de la cybersécurité et de la protection de la vie privée;
- concevoir, développer ou acquérir des systèmes qui répondent aux activités et aux contrôles définis;
- intégrer, tester et installer des systèmes qui répondent aux besoins en matière de sécurité et de protection de la vie privée;
- exploiter, surveiller et tenir à jour les systèmes de sécurité et de protection de la vie privée au cours de la phase d'exploitation et de maintenance;
- éliminer les biens de façon sécurisée lors de la mise hors service des systèmes;
- éliminer les biens de renseignements personnels de façon sécurisée lorsqu'ils ne sont plus nécessaires à l'organisation.

3 Relations avec les processus externes

Pour tirer pleinement avantage de la présente publication, les organisations doivent être au courant des importantes relations suivantes qui existent entre les activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée et les autres processus :

- **Gestion intégrée des risques**
 - Les activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée peuvent soutenir la gestion intégrée des risques de l'organisation, conformément à ce qui est énoncé dans le [Cadre stratégique de gestion du risque](#) du SCT.
 - Ces activités forment une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques pour la cybersécurité et la vie privée du point de vue de l'organisation dans son ensemble.
- **Analyse des répercussions sur les activités**
 - Les analyses des répercussions sur les activités fournissent de l'information précieuse sur la façon de déterminer les exigences de l'organisation en matière de sécurité et de protection de la vie privée et d'évaluer la sensibilité et la criticité de ses activités opérationnelles.
 - Ensemble, ces facteurs déterminent la catégorie de sécurité appropriée pour ces activités.
- **Architecture d'entreprise** – La fonction responsable de l'architecture d'entreprise fournit les principaux éléments nécessaires pour faire en sorte que les exigences en matière de cybersécurité et de protection de la vie privée à l'échelle de l'organisation soient prises en compte au moment de définir, d'attribuer et de mettre à jour les activités et les contrôles.

Remarque propre au GC

Dans le GC, il convient d'envisager un autre processus : l'**évaluation de l'incidence algorithmique (EIA)**. Il s'agit d'un outil obligatoire d'évaluation des risques visant à appuyer la [Directive sur la prise de décisions automatisée](#) du SCT. Il génère un indice de risque qui reflète les risques potentiels qui pèsent sur le système décisionnel automatisé et les ministères et organismes devraient considérer ce score dans le cadre de leurs activités de gestion des risques.

4 Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée

Cette section décrit les activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée que le Centre pour la cybersécurité recommande d'incorporer dans le programme de sécurité et de protection de la vie privée d'une organisation. Elle propose également des lignes directrices sur la façon de les accomplir efficacement.

Remarque propre au GC

Avant d'intégrer les activités de l'ITSP.10.036 dans leur programme ministériel de sécurité et de protection de la vie privée, les ministères devraient s'assurer que leur structure de gouvernance (rôles, responsabilités et responsables de la prise de décisions) est conforme à celle décrite dans les plus récents instruments de politique du SCT.

La [figure 2](#), **Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée**, décrit les activités du processus de gestion des risques pour la cybersécurité et la vie privée qui sont effectuées au niveau de l'organisation. Le principal objectif de ces activités est d'attribuer et de tenir à jour un ensemble d'activités et de contrôles de sécurité et de protection de la vie privée adaptés aux besoins et aux objectifs de l'organisation à cet égard.

La protection des renseignements personnels² est une responsabilité partagée à plusieurs facettes qui exige des efforts concertés et coordonnés de la part des fonctions responsables de la sécurité et de la protection de la vie privée tout au long du processus de gestion des risques.

Les principaux résultats des activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée sont des profils d'activités et de contrôles, ainsi que des référentiels de menaces organisationnels, qui servent d'éléments clés au niveau du système d'information dans le cadre du processus de gestion des risques associé au déploiement d'activités et de contrôles dans les systèmes d'information.

² Selon la définition qui est donnée à l'article 3 de la LPRP, les « renseignements personnels » désignent les renseignements relatifs à un individu identifiable, quelle que soit la manière dont ils sont consignés.

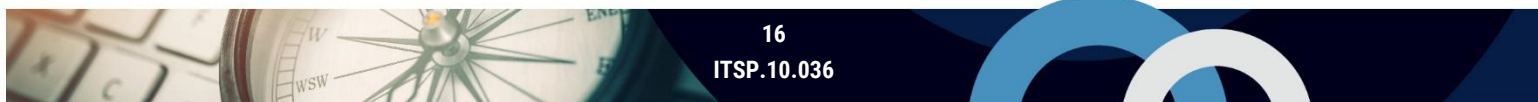
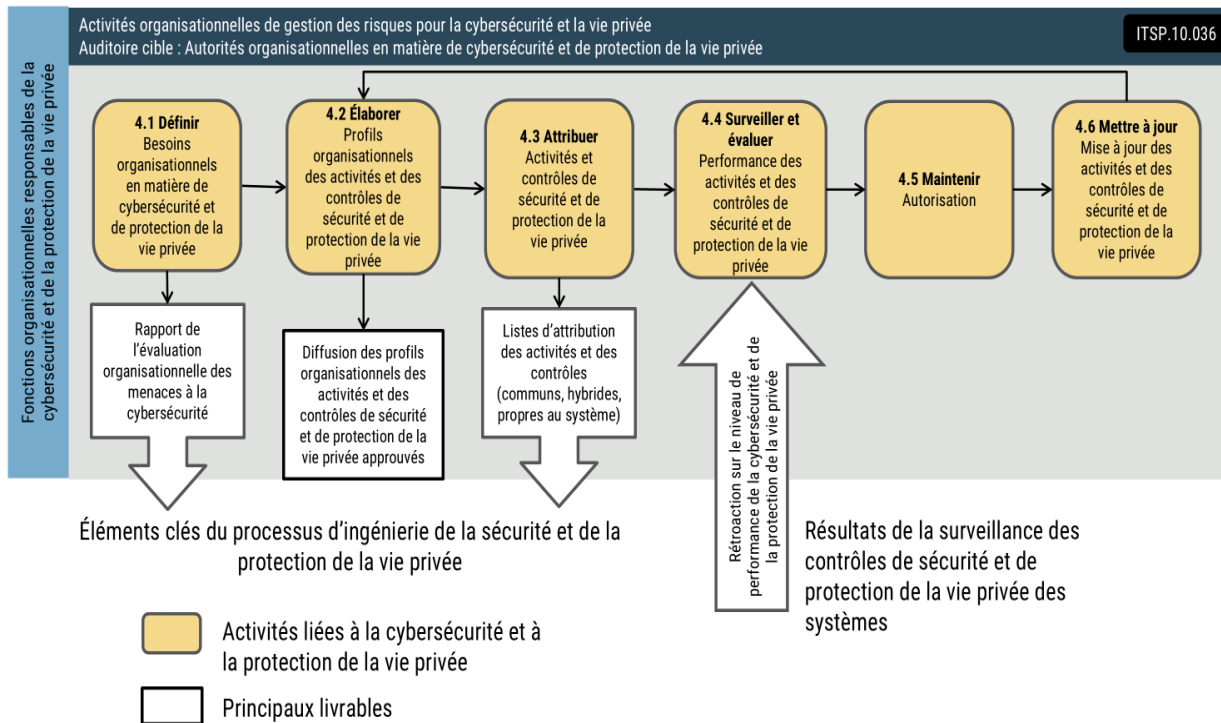


Figure 2 : Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée**Description longue – Figure 2 : Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée**

La figure présente un diagramme horizontal de flux de processus intitulé « Activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée ». Un en-tête foncé s'étend sur toute la largeur au haut de la figure et indique que le public cible est constitué d'autorités organisationnelles en matière de cybersécurité et de protection de la vie privée. Sur le côté gauche de la figure, une barre verticale porte la mention « Fonctions organisationnelles responsables de la cybersécurité et de la protection de la vie privée ».

Au centre, six rectangles jaunes représentant les principales activités organisationnelles sont disposés de gauche à droite et reliés par des flèches pointant vers la droite. Ces activités sont les suivantes :

- 4.1 Définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée
- 4.2 Élaborer les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée
- 4.3 Attribuer les activités et les contrôles de sécurité et de protection de la vie privée
- 4.4 Surveiller et évaluer le niveau de performance des activités et des contrôles en matière de sécurité et de protection de la vie privée
- 4.5 Maintenir l'autorisation
- 4.6 Mettre à jour le ou les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée

Chacune des trois premières activités est reliée par une flèche descendante à une case blanche correspondant aux principaux livrables situés en dessous :

- Sous 4.1 : Rapport de l'évaluation organisationnelle des menaces à la cybersécurité
- Sous 4.2 : Diffusion des profils organisationnels des activités et des contrôles de sécurité et de protection de la vie privée approuvés
- Sous 4.3 : Listes d'attribution des activités et des contrôles (communs, hybrides, propres au système)

Sous les activités 4.1 et 4.3, une flèche descendante accompagne une légende indiquant : « Éléments clés du processus d'ingénierie de la sécurité et de la protection de la vie privée ».

Une grande flèche blanche pointant vers le haut est située sous la section 4.4. Elle porte l'étiquette « Rétroaction sur le niveau de performance de la cybersécurité et de la protection de la vie privée » et indique que les résultats de la surveillance alimentent le processus organisationnel. À droite de la flèche ascendante, une note indique « Résultats de la surveillance des contrôles de sécurité et de protection de la vie privée des systèmes » afin de préciser que la surveillance effectuée au niveau des systèmes produit une rétroaction dont l'organisation se sert pour réévaluer et mettre à jour, au besoin, ses profils et ses attributions de contrôles.

Enfin, l'activité 4.6 Mettre à jour est reliée à l'étape antérieure 4.2 « Élaborer les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée » par une flèche de rétroaction qui forme une boucle dans la partie supérieure du diagramme.

Les activités organisationnelles de gestion des risques pour la cybersécurité et la vie privée visent à atteindre les objectifs suivants :

- établir et documenter les besoins organisationnels pour ce qui a trait aux activités opérationnelles en matière de sécurité et de protection de la vie privée;
- réaliser et tenir à jour les évaluations des menaces organisationnelles que les autorités, les praticiennes et les praticiens en matière de sécurité et de protection de la vie privée peuvent utiliser pour identifier les auteurs de menace pertinents, orienter la détermination des risques et de la robustesse tout au long du cycle de vie de développement et produire des résultats uniformes;
- élaborer les profils organisationnels des activités et des contrôles adaptés aux besoins opérationnels en matière de sécurité et de protection de la vie privée;
 - utiliser le ou les profils dans les projets qui visent à mettre en œuvre ou à mettre à jour les systèmes d'information organisationnels;
- attribuer les activités et les contrôle de sécurité et de protection de la vie privée dans l'infrastructure de sécurité d'entreprise;
- définir les activités et contrôles communs, hybrides ou propres au système nécessaires pour soutenir l'attribution de responsabilités dans l'ensemble de l'entreprise;
- assurer la coordination des fonctions responsables de la sécurité et de la protection de la vie privée de l'organisation (par exemple, la sécurité physique et la sécurité du personnel) afin d'adopter une approche uniforme pour ce qui a trait à la conception et à l'exploitation de systèmes d'information fiables;

- surveiller et évaluer le niveau de performance des activités et des contrôles mis en place pour protéger les activités opérationnelles de l'organisation; élaborer et mettre en œuvre des mesures correctives pour améliorer le rendement de l'organisation, ainsi que sa posture globale en matière de sécurité et de protection de la vie privée.

4.1 Définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée

La présente section décrit le processus visant à définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée. Elle comprend les sous-activités suivantes :

- définir la portée des activités liées à l'évaluation des risques pour la cybersécurité et la vie privée de l'organisation ([section 4.1.1](#));
- déterminer les besoins opérationnels en matière de sécurité et de protection de la vie privée associés aux activités opérationnelles de l'organisation ([section 4.1.2](#) **Error! Reference source not found.**);
- procéder à l'évaluation à la catégorisation du préjudice associé aux activités opérationnelles de l'organisation ([section 4.1.3](#));
- sélectionner la méthodologie d'évaluation des menaces et des risques (EMR) liés à la cybersécurité de l'organisation ([section 4.1.4](#));
- sélectionner la méthodologie d'évaluation de la protection de la vie privée de l'organisation ([section 4.1.5](#));
- procéder à l'évaluation des menaces à la cybersécurité de l'organisation ([section 4.1.6](#)).

Chacune de ces activités visant à définir les besoins organisationnels en matière de cybersécurité et de protection de la vie privée est décrite dans les sections suivantes. Ces activités sont effectuées lors de la première mise en œuvre des lignes directrices présentées dans cette publication, puis au besoin selon l'évaluation de la posture de sécurité et de protection de la vie privée des systèmes d'information d'une organisation (voir la [section 4.6](#)).

4.1.1 Définir la portée des activités d'évaluation des risques pour la cybersécurité et la vie privée

Objectif : Définir la portée des activités organisationnelles d'évaluation des risques pour la cybersécurité et la vie privée.

Rôles connexes suggérés : Responsables principales et principaux de la sécurité (par exemple, DPS, dirigeante principale ou dirigeant principal de la sécurité de l'information [DPSI]), responsables principales et principaux de la protection de la vie privée, conseillères et conseillers en cybersécurité, architectes de sécurité d'entreprise, conseillères et conseillers en protection de la vie privée, architectes de la protection de la vie privée, directrices et directeurs de projet

La portée peut être caractérisée par les éléments suivants :

- les programmes, les services, l'information et les activités opérationnelles de l'organisation qui doivent être protégés;
- les programmes, les services et les activités de l'organisation qui consistent à créer, à collecter et à traiter les renseignements personnels en son contrôle;
- les biens informatiques importants (par exemple, les applications commerciales, les systèmes d'information, les centres de données, les réseaux locaux, les données traitées et stockées, l'information) et leurs emplacements géographiques;
- les technologies de base utilisées dans les systèmes d'information de l'organisation;
- les stratégies d'approvisionnement (par exemple, en interne, externalisation).

La portée devrait clairement définir les activités opérationnelles et les biens de l'organisation qui relèvent de son champ d'application, ainsi que ceux qui en sont exclus avec une justification de l'exclusion. Elle devrait également indiquer les dépendances externes, comme les fournisseurs de services externes.

Résultat : Définition de la portée des activités organisationnelles d'évaluation des risques pour la cybersécurité et la vie privée et de l'inventaire des renseignements personnels.

4.1.2 Définir les besoins opérationnels en matière de sécurité et de protection de la vie privée

Objectif : Déterminer les besoins opérationnels en matière de sécurité et de protection de la vie privée associés aux activités opérationnelles de l'organisation.

Rôles connexes suggérés : Responsables principales et principaux de la sécurité (comme les DPS et les DPSI), responsables principaux et principaux de la protection de la vie privée, conseillères et conseillers en cybersécurité, conseillères et conseillers en protection de la vie privée et directrices et directeurs de projets

Dans le contexte de la gestion des risques pour la cybersécurité et la protection de la vie privée, on entend par besoins opérationnels en matière de sécurité et de protection de la vie privée, le besoin de protéger les activités et l'information opérationnelles de l'organisation contre les événements préjudiciables qui pourraient empêcher l'organisation de mener à bien sa mission, ses objectifs et ses obligations. Les besoins opérationnels en matière de sécurité et de protection de la vie privée nécessaires pour assurer la conformité reposent sur les lois et les règlements qui prescrivent les exigences de protection des systèmes d'information et des renseignements personnels. Les besoins opérationnels en matière de sécurité et de protection de la vie privée, quant à eux, définissent les objectifs officiels à cet égard. Les besoins peuvent découler des éléments suivants :

- les exigences stipulées dans les lois, les règlements, les politiques, les directives, les normes, la jurisprudence et les objectifs qui régissent les activités opérationnelles de l'organisation et la gestion de l'information (par exemple, dans le GC, un cadre ministériel des résultats);
- les expositions aux menaces et les exigences en matière de conformité relatives aux systèmes d'information reconnus par l'organisation ou de manière générale;

- les obligations contractuelles ou négociées (par exemple, les contrats, les protocoles d'entente [PE], les accords sur les niveaux de service [ANS] et les accords d'échange de renseignement [AER]).

Les besoins opérationnels en matière de sécurité incluent les exigences relatives à la protection de la vie privée qui doivent être prises en compte aux fins de gestion des risques pour la vie privée.

Les exemples de besoins opérationnels en matière de sécurité et de protection de la vie privée comprennent la nécessité de faire ce qui suit :

- restreindre l'accès à l'information sensible du programme ou aux renseignements personnels aux personnes autorisées pour l'exécution d'actions autorisées;
- limiter les utilisations ou divulgations secondaires de renseignements personnels;
- vérifier l'identité des citoyennes et citoyens avant de divulguer des renseignements personnels qui les concernent;
- s'assurer que seules les personnes autorisées peuvent approuver le paiement effectué en faveur d'une ou un bénéficiaire.

Les organisations devraient établir leurs besoins en matière de sécurité et de protection de la vie privée avec l'aide des analystes des activités, des propriétaires de systèmes, des architectes de systèmes, ainsi que des architectes de sécurité et de protection de la vie privée. Les éléments utiles pour cette activité incluent la documentation des processus opérationnels (par exemple, descriptions, scénarios d'utilisation, concepts d'opérations [CONOPS]) et les évaluations des répercussions (par exemple, analyse des répercussions sur les activités [ARA], évaluation des facteurs relatifs à la vie privée [EFVP], évaluation de l'incidence algorithmique).

Résultat : Document précisant les besoins opérationnels en matière de sécurité et de protection de la vie privée associés aux activités opérationnelles de l'organisation.

4.1.3 Procéder à l'évaluation et à la catégorisation du préjudice associé aux activités opérationnelles de l'organisation

Objectif : Procéder à l'évaluation et à la catégorisation du préjudice associé aux activités opérationnelles de l'organisation.

Rôles connexes suggérés : Conseillères et conseillers en sécurité, conseillères et conseillers en protection de la vie privée, directrice ou directeur de projet

Une catégorie de préjudice exprime les niveaux les plus élevés de préjudices prévus qui découlent des compromissions liées aux menaces par rapport aux objectifs de sécurité et de protection de la vie privée portant sur la confidentialité, l'intégrité et la disponibilité. Les exigences relatives à la sécurité peuvent améliorer la catégorisation en matière d'intégrité et de disponibilité.

Pour catégoriser les activités opérationnelles, il convient d'abord de déterminer les préjudices prévus qu'une compromission liée à une cybermenace pourrait avoir sur les intérêts nationaux et non nationaux servis par ces activités opérationnelles, puis de déterminer le niveau de ces préjudices prévus. Bien que l'atteinte à la sécurité des renseignements personnels puisse donner lieu à différents niveaux de préjudice, les obligations en matière de conformité ne changent pas en fonction du type de renseignement personnel. La catégorisation exhaustive de la sécurité de l'information devrait prendre en considération la présence de renseignements personnels.

Les organisations peuvent catégoriser leurs activités opérationnelles conformément au processus indiqué à la [section 5](#).

Résultat : Rapport de catégorisation du préjudice pour les activités opérationnelles de l'organisation.

4.1.4 Sélectionner la méthodologie d'évaluation des menaces et des risques pour la cybersécurité de l'organisation

Objectif : Sélectionner la méthodologie selon laquelle les menaces et les risques liés à la sécurité et à la protection de la vie privée seront évalués par l'organisation.

Rôles connexes suggérés : Responsables principales et principaux de la sécurité (DPS, DPSI), conseillères et conseillers en sécurité

Une méthodologie d'EMR de la cybersécurité doit être sélectionnée à cette étape, puisqu'une organisation utilisera la partie relative à l'évaluation des menaces lorsqu'elle évaluera les menaces qui pèsent sur ses activités opérationnelles. De plus, les projets utiliseront cette méthodologie pour mener à bien les activités d'EMR.

La [méthodologie harmonisée d'évaluation des menaces et des risques \(EMR\) \(TRA-1\) du CST et de la GRC](#) est un exemple de méthodologie d'EMR souvent utilisée dans le GC.

Résultat : Sélection d'une méthodologie organisationnelle d'EMR liés à la cybersécurité.

4.1.5 Sélectionner la méthodologie d'évaluation de la protection de la vie privée de l'organisation

Objectif : Sélectionner la méthodologie selon laquelle les risques pour la protection de la vie privée et les lacunes sur le plan de la conformité seront évalués par l'organisation.

Rôles connexes suggérés : Responsables principales et principaux de la protection de la vie privée, conseillères et conseillers en protection de la vie privée

À cette étape, une méthodologie d'évaluation de la protection de la vie privée doit être sélectionnée pour relever, évaluer et atténuer les risques potentiels pour la vie privée qui sont associés à des programmes, des technologies ou des projets nouveaux ou modifiés.

Dans le GC, les évaluations de la protection de la vie privée sont conformes à la politique du SCT et elles commencent par l'élaboration d'un modèle pour la liste de vérification de la protection de la vie privée. Cette liste de vérification aide à déterminer si une initiative exige un protocole de protection de la vie privée, une EFVP ou une aucune autre évaluation de la protection de la vie privée. Chaque méthodologie d'évaluation repose sur son modèle correspondant. Par conséquent, le fait de sélectionner le modèle approprié permet également de déterminer l'approche d'évaluation à adopter.

Résultat : Sélection de la méthodologie organisationnelle d'évaluation de la protection de la vie privée. Dans le GC, cette étape permettra également de créer une liste de vérification de la protection de la vie privée qui détermine le modèle à utiliser pour toute analyse additionnelle à cet égard.

4.1.6 Procéder à l'évaluation organisationnelle des menaces à la cybersécurité

Objectif : Procéder à une évaluation panorganisationnelle initiale des menaces à la cybersécurité qui permettra d'orienter la sélection d'activités et de contrôles de sécurité et de protection de la vie privée dont les projets pourront tirer avantage lors de la mise en œuvre des systèmes³.

Rôles connexes suggérés : Analystes du renseignement, analystes des menaces à la cybersécurité

Cette activité déterminera et qualifiera les menaces pertinentes pour les activités opérationnelles de l'organisation abordées dans la présente.

L'évaluation des menaces à la cybersécurité remplit deux objectifs :

- éclairer l'EMR;
- soutenir les décisions liées au contexte de menace.

Les organisations peuvent indiquer un sous-ensemble de toutes les menaces potentielles contre lesquelles elles veulent protéger leurs activités opérationnelles. Cela signifie que certaines menaces peuvent être relevées et envisagées, tout en étant exclues de la portée pour diverses raisons. Par exemple, une organisation peut conclure qu'il serait trop coûteux ou trop complexe de se protéger contre une menace, ou que la protection est susceptible de limiter de façon excessive une fonctionnalité destinée à soutenir des activités opérationnelles. Le renseignement sur les menaces, y compris les décisions et la justification en ce qui concerne l'exclusion de menaces particulières, est documenté en fonction du contexte de menace de l'organisation.

Une évaluation des menaces à l'échelle de l'organisation est un outil précieux que l'on peut utiliser pour sélectionner, adapter, attribuer, mettre à jour et améliorer les activités et les contrôles de sécurité et de protection de la vie privée mis en œuvre. Ses résultats, en plus des besoins opérationnels de l'organisation en matière de sécurité et de protection de la vie privée, forment une base solide pour l'élaboration des profils d'activités et de contrôles organisationnels.

À l'élaboration de ces profils, l'accent pourrait être mis sur des référentiels de menaces plus précis et propres aux domaines afin de documenter le renseignement détaillé sur les menaces qui touchent les domaines opérationnels.

Une évaluation efficace des menaces organisationnelles devrait évaluer et considérer ce qui suit :

- les principales activités opérationnelles de l'organisation;
- l'évaluation du préjudice associé à ces activités;
- les menaces pertinentes qui pèsent sur les activités;
- les expositions générales qui pourraient avoir une incidence sur les activités opérationnelles (par exemple, des lieux physiques vulnérables aux séismes).

Dans le GC, les évaluations des menaces ministérielles devraient être réalisées par des équipes multidisciplinaires avec l'aide du bureau de la ou du DPI, des principaux organismes de sécurité du GC et des praticiennes et praticiens de la protection de la vie privée.

³ Une évaluation organisationnelle des menaces est un processus continu qui soutient également les activités de gestion des risques pour la cybersécurité et la vie privée qui pèsent sur les systèmes. Pour de plus amples détails, prière de consulter le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037).

Résultat : Le référentiel d'évaluation des menaces de l'organisation documente les menaces et les expositions qui sont pertinentes pour les activités.

4.2 Élaborer les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée

Objectif : Créer des profils organisationnels des activités et des contrôles en matière de sécurité et de protection de la vie privée adaptés aux besoins à cet égard.

Rôles connexes suggérés : Responsables principales et principaux de la sécurité, comme les DPS et les DPSI, responsables principales et principaux de la protection de la vie privée, architectes de sécurité d'entreprise, architectes de la protection de la vie privée, conseillères et conseillers en sécurité, conseillères et conseillers en protection de la vie privée

Selon leur champ d'activités (par exemple, la gestion d'une seule initiative, la supervision de plusieurs projets ou l'exploitation de multiples domaines de sécurité) et la complexité de leurs activités opérationnelles, les organisations peuvent maintenir un seul profil panorganisationnel ou plusieurs profils propres aux domaines adaptés aux différents secteurs de leurs activités.

On s'attend à ce que les fonctions responsables de la cybersécurité et de la protection de la vie privée d'une organisation collaborent à l'élaboration des profils, puisque des activités non autorisées sur les systèmes pourraient poser des risques pour la vie privée. Cela dit, les risques pour la vie privée associés à la manutention de renseignements personnels dans un système d'information ne relèvent pas tous de la sécurité de l'information. Ils peuvent être le résultat d'activités liées à la création, à la collecte, à la conservation, à la précision, à l'utilisation, à la divulgation ou à l'élimination des renseignements personnels sous le contrôle d'une organisation. Par conséquent, la fonction responsable de la protection de la vie privée au sein d'une organisation sélectionnera, attribuera, surveillera et évaluera également les contrôles de protection de la vie privée afin de se conformer à ces exigences législatives.

Il est préférable d'élaborer les profils organisationnels en tirant avantage de plusieurs processus de gestion de l'information clés à l'échelle de l'organisation. Ces processus d'entreprise s'ajoutent aux processus de gestion des risques pour la cybersécurité et la vie privée et peuvent aider les organisations à sélectionner et à adapter les activités et les contrôles à cet égard de façon appropriée. Les processus de soutien sont les suivants :

- l'examen des activités opérationnelles de l'organisation et ses besoins en matière de sécurité et de protection de la vie privée;
- la priorisation des activités opérationnelles de l'organisation selon les objectifs stratégiques dictés par la disponibilité et la continuité des activités (de manière générale, cela signifie s'assurer que la plupart des activités critiques se poursuivront ou resteront disponibles);
- la définition des types de biens d'information nécessaires pour mener à bien les activités opérationnelles d'un ministère, leur criticité, leur sensibilité et leurs flux internes et externes;
- la création de dictionnaires de données qui documentent les collectes de renseignements personnels dans l'organisation;
- la définition de l'architecture conceptuelle d'entreprise qui comprend les exigences en matière de cybersécurité et de protection de la vie privée.

L'élaboration des profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée s'effectue en quatre étapes :

1. définir les domaines opérationnels;
2. définir les approches architecturales à la sécurité;
3. sélectionner les activités et les contrôles de sécurité et de protection de la vie privée;
4. approuver les profils organisationnels des activités et des contrôles en matière de sécurité et de protection de la vie privée.

Ces quatre étapes sont décrites en détail dans les sous-sections ci-dessous.

4.2.1 Définir les domaines opérationnels

Objectif : Définir les domaines opérationnels d'une organisation pour faciliter l'élaboration des profils organisationnels des activités et des contrôles en matière de sécurité et de protection de la vie privée.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Un domaine opérationnel se caractérise par les catégories de sécurité de ses activités opérationnelles et les menaces pertinentes qui pèsent sur la cybersécurité. Par conséquent, les domaines opérationnels peuvent avoir différents besoins en matière de protection, ce qui donne lieu à des profils différents.

Par exemple, il convient d'envisager un ensemble d'activités opérationnelles portant sur la diffusion de publications non sensibles et un second ensemble portant sur des transactions financières essentielles à valeur élevée. Dans ce dernier scénario, les activités financières donneraient probablement lieu à un niveau de préjudice plus élevé et feraient l'objet de menaces plus grandes. Cette analyse mènerait à la définition de deux domaines exigeant deux profils de domaine différents.

Les organisations ont une certaine souplesse dans la façon dont elles définissent leurs domaines opérationnels. Elles devraient documenter en détail la manière dont ces domaines sont définis, les catégories de préjudice des activités opérationnelles et l'importance de l'environnement de menace. Il importe de souligner que les activités opérationnelles de l'organisation devraient être définies tôt (en totalité ou en partie), durant l'activité d'évaluation et de catégorisation du préjudice (voir la [section 4.1.3](#)).

Les définitions des domaines opérationnels sont créées dans le cadre de cette activité. Chaque domaine opérationnel défini devrait comprendre ce qui suit :

- une description des objectifs opérationnels, des processus et des biens d'information du domaine opérationnel;
- la catégorie de préjudice associée au domaine opérationnel;
- une caractérisation de l'environnement de menace en rapport avec le domaine opérationnel (à savoir, le niveau de menace délibérée [Md] le plus élevé à atténuer);
- un énoncé indiquant le niveau de risque le plus élevé que la ou le propriétaire opérationnel juge acceptable.

Résultat : Définitions des domaines opérationnels, ce qui comprend les objectifs, les processus et les biens l'information, la catégorie de préjudice, l'environnement de menace et un énoncé du niveau de risque jugé acceptable.

4.2.2 Définir les approches architecturales à la sécurité

Objectif : Définir un ensemble d'approches architecturales à la sécurité en accord avec la philosophie, la culture, les objectifs et les priorités de l'organisation en matière de cybersécurité et de protection de la vie privée.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Au niveau organisationnel, les approches architecturales à la sécurité influent sur la sélection de certaines activités et de certains contrôles de sécurité techniques associés aux principes d'ingénierie de la sécurité mis en œuvre dans l'approche adoptée. Au niveau du système d'information, les approches architecturales à la sécurité s'avèrent tout aussi importantes qu'un guide mis en place pour adapter les contrôles de sécurité dans les profils selon les besoins des systèmes d'information en matière de sécurité et préciser les conceptions de sécurité appropriées.

Les architectes de sécurité d'entreprise et les architectes de protection de la vie privée s'efforceront probablement d'obtenir l'approbation de la haute direction quant aux approches architecturales à la sécurité à adopter, puisque ces décisions ont souvent des implications sur le plan budgétaire et des capacités.

Lorsqu'elles définissent les approches architecturales à la sécurité, les organisations devraient tenir compte de ce qui suit :

- les besoins opérationnels en matière de sécurité et de protection de la vie privée ([section 4.1.2](#));
- l'évaluation et la catégorisation du préjudice lié aux activités opérationnelles ([section 4.1.3](#));
- les menaces documentées dans l'évaluation des menaces de l'organisation ([section 4.1.6](#));
- les pratiques exemplaires et les principes généralement acceptés en matière de cybersécurité, notamment :
 - le document [Enterprise Security Architecture – A Business-Driven Approach](#) (en anglais seulement) de Sherwood Applied Business Security Architecture (SABSA);
 - le document [Exigences de base en matière de sécurité pour les zones de sécurité de réseau \(ITSP.80.022. version 2.0\)](#) du Centre pour la cybersécurité;
 - le document [Special Publication \(SP\) 800-160 Vol.1 Rev.1 Engineering Trustworthy Secure Systems](#) (en anglais seulement) du National Institute of Standards and Technology's (NIST);
 - le document [SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach](#) (en anglais seulement) du NIST;
- les pratiques exemplaires et les principes généralement reconnus en matière de protection de la vie privée, notamment :
 - les principes de traitement équitable de l'information;
 - les principes généralement reconnus en matière de protection des renseignements personnels (PPRP).

Vous trouverez ci-dessous des exemples d'approches architecturales à la sécurité qui influent sur la sélection des activités et des contrôles en matière de sécurité et de protection de la vie privée, ainsi que la spécification des conceptions de sécurité que les organisations peuvent utiliser :

- une approche globale comparativement à une approche fragmentaire à la conception, où l'approche globale considère la sécurité et la protection de la vie privée à différentes couches d'un système d'information (par exemple, les couches des applications, de la gestion des données, des intergiciels, de la plateforme et des communications) et permet de comprendre les flux d'information entre ces couches;

- une défense en profondeur ou multicouche comparativement à une attention portée exclusivement à une protection monocouche;
- des approches à conception de type coquille d'œuf (périmètre robuste et centre vulnérable) comparativement à en nid d'abeilles et comparativement à la protection des points d'extrémité;
- des modes de fonctionnement appropriés de la sécurité (dédié, système haut, compartimenté, multiniveau, niveaux de sécurité multiples et indépendants [MILS pour *Multiple Independent Levels of Security*]);
- une architecture d'applications à plusieurs niveaux (présentation, logique applicative, référentiels de données) appliquant le zonage de sécurité comparativement à une architecture de système monolithique;
- l'utilisation de services de sécurité communs avec interface de programmation d'applications normalisées (par exemple, un système d'authentification organisationnel) comparativement à la mise en œuvre de services de sécurité personnalisés;
- la sécurité de l'infrastructure comparativement à la sécurité des biens de données (par exemple, la gestion des droits numériques);
- les considérations sociétales (par exemple, la vie privée du personnel par rapport à la surveillance) comparativement à l'application de contrôles difficiles à utiliser, mais plus sécurisés.

Résultat : Liste des approches architecturales à la sécurité sélectionnées et justifications.

4.2.3 Sélectionner les activités et les contrôles organisationnels de sécurité et de protection de la vie privée

Objectif : Sélectionner les activités et les contrôles organisationnels de sécurité et de protection de la vie privée.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée, conseillères et conseillers en sécurité, conseillères et conseillers en protection de la vie privée

Les organisations élaborent un profil d'activités et de contrôles pour chacun des domaines opérationnels qu'elles ont définis. Si une organisation définit plusieurs domaines opérationnels, elle peut alors développer les profils progressivement, en commençant par celui dont elle a le plus besoin, puis en ajoutant les autres au fil du temps.

Trois approches peuvent être mises en œuvre pour les activités et les contrôles :

- une approche de mise en œuvre commune (héritable);
- une approche de mise en œuvre propre au système;
- une approche de mise en œuvre hybride.

Les approches de mise en œuvre définissent la portée de l'applicabilité pour le contrôle ou l'activité, sa nature partagée ou sa transmissibilité, et la responsabilité à l'égard de son développement, de sa mise en œuvre et de son autorisation. Chaque approche de mise en œuvre est associée à une orientation et à un objectif précis pouvant aider les organisations à sélectionner les activités et les contrôles appropriés, à les appliquer de manière efficace et à répondre aux exigences de sécurité et de protection de la vie privée. Une approche de mise en œuvre particulière peut permettre de faire des économies en tirant parti des capacités liées à la sécurité et à la protection de la vie privée dans divers systèmes et environnements opérationnels.

Une activité et un contrôle communs sont déployés sous forme de service partagé au sein de l'organisation. La mise en œuvre d'activités et de contrôles communs engendre une capacité dont plusieurs systèmes ou programmes peuvent hériter. La responsabilité des activités et des contrôles propres au système relève de la ou du propriétaire du système. Les organisations peuvent mettre en œuvre un contrôle ou une activité hybride si une partie des activités ou des contrôles sont communs (héritables) et que l'autre partie est propre au système. Par exemple, une organisation peut mettre en œuvre le contrôle de la planification d'urgence CP-02 à l'aide d'un modèle prédéfini pour tous les systèmes organisationnels alors que chaque propriétaire du système d'information adapte le plan pour des usages propres au système, lorsque cela s'avère approprié. En ce qui a trait à la protection de la vie privée, une politique ou procédure panorganisationnelle serait un exemple d'activité ou de contrôle commun en matière de protection de la vie privée. Pour de plus amples renseignements, prière de consulter la [section 2, Approches de mise en œuvre, du Catalogue des activités d'assurance et des contrôles de sécurité et de protection de la vie privée \(ITSP.10.033\)](#).

Les profils d'activités et de contrôles organisationnels sont utilisés par les fonctions responsables de la cybersécurité et de la protection de la vie privée pour coordonner l'attribution des activités et des contrôles communs à l'architecture d'entreprise. Ils éclairent également les projets pour ce qui est des activités et des contrôles hérités par le système, ainsi que ceux qu'ils visent à mettre en œuvre pour sécuriser le système en cours de développement ou de mise à jour.

Au moment d'élaborer leurs profils d'activités et de contrôles, les organisations sélectionnent les activités et les contrôles dans le catalogue ITSP.10.033 et les adaptent de manière à répondre à leurs besoins en matière de sécurité et de protection de la vie privée ([section 4.1.2](#)). La sélection et l'adaptation des activités et des contrôles sont orientées par les résultats de l'évaluation organisationnelle de la protection de la vie privée ([section 4.1.5](#)), de l'évaluation organisationnelle de la cybersécurité ([section 4.1.6](#)) et les approches architecturales à la sécurité définies ([section 4.2.2](#)). Pour les organisations où on retrouve une fonction responsable de l'architecture d'entreprise, les praticiennes et praticiens de la sécurité et de la protection de la vie privée devraient également tenir compte des artéfacts liés à la cybersécurité lors de la sélection et de l'adaptation des activités et des contrôles propres au système.

Les profils organisationnels devraient également documenter les hypothèses et le contexte opérationnel en fonction desquels ils ont été élaborés en décrivant ce qui suit :

- les activités opérationnelles prises en compte et les besoins opérationnels connexes en matière de sécurité et de protection de la vie privée;
- l'évaluation et la catégorisation du préjudice lié aux activités opérationnelles prises en compte;
- le contexte de menace;
- les artéfacts de conformité aux exigences législatives et aux politiques;
- les approches architecturales à la sécurité ayant été définies;
- toute autre contrainte technique ou hypothèse susceptible d'influer sur la sélection des activités et des contrôles.

Le référentiel organisationnel des menaces est un élément clé du processus d'élaboration d'un profil d'activités et de contrôles (voir la [section 4.1.6](#)). Lors de l'élaboration des profils des domaines, les organisations peuvent peaufiner les définitions des menaces de l'organisation selon le renseignement additionnel sur les menaces propre aux activités opérationnelles de chaque domaine. Dans une telle situation, les organisations peuvent documenter ces définitions de menace dans les référentiels des menaces propres au domaine.

On devrait envisager d'attribuer plusieurs des activités et des contrôles mentionnés dans le catalogue ITSP.10.033 en tant qu'activités et contrôles communs.

Voici des exemples d'activités et de contrôles communs en matière de sécurité et de protection de la vie privée :

- un programme organisationnel de filtrage de sécurité du personnel pour appuyer la sélection du personnel de cybersécurité;
- un programme de sécurité physique pour soutenir la protection des installations technologiques;
- une gestion des incidents de sécurité et des atteintes à la vie privée réalisée par des fonctions responsables de la cybersécurité et de la protection de la vie privée pour assurer une connaissance approfondie de la situation;
- un système exploité par un groupe opérationnel de TI et de TO qui propose une solution commune à l'authentification des utilisatrices ou utilisateurs finaux;
- un système panorganisationnel de surveillance des journaux exploité par une équipe relevant de la fonction responsable de la cybersécurité, permettant de séparer les tâches entre les fonctions responsables des opérations de TI ou de TO et celles qui sont responsables de la cybersécurité;
- un programme de sensibilisation et de formation en matière de cybersécurité administré par le centre d'apprentissage de l'organisation.

Pour élaborer leur profil, les organisations peuvent tirer avantage du profil à incidence moyenne décrit dans le document ITSP.10.033-01, qui est fondé sur le catalogue de l'ITSP.10.033.

Résultat : Un profil panorganisationnel des activités et des contrôles en matière de sécurité et de protection de la vie privée ou un ensemble de profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée propres au domaine.

4.2.4 Approuver le ou les profils de l'organisation

Objectif : Approuver le ou les profils organisationnels des activités et des contrôles en matière de sécurité et de protection de la vie privée.

Rôles connexes suggérés : Responsables principales et principaux de la sécurité; responsables principales et principaux de la protection de la vie privée

Une fois que le ou les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée sont terminés, les membres de la haute direction responsables de la gouvernance de l'organisation à cet égard devraient les passer en revue et obtenir l'approbation des autorités de l'organisation (par exemple, PDG, DPI, DPS, DPSI, CPRP, administratrice générale ou administrateur général) au besoin. Dans le cadre de ce processus, ces membres de la haute direction devraient également s'assurer que les activités et les contrôles organisationnels indiqués dans les profils répondent aux besoins de l'organisation en matière de sécurité et de protection de la vie privée, et qu'ils permettent de remplir ses obligations à cet égard. Elles et ils devraient faire en sorte qu'un bon équilibre soit maintenu entre la mise en œuvre des activités et des contrôles et les niveaux de risque résiduel que l'organisation est prête à assumer.

Résultat : Un ou plusieurs profils organisationnels des activités et des contrôles en matière de sécurité et de protection de la vie privée approuvés.

4.3 Attribuer les activités et les contrôles de sécurité et de protection de la vie privée

Objectif : Coordonner l'attribution des activités et des contrôles de sécurité et de protection de la vie privée.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Après l'approbation des profils organisationnels des activités et des contrôles en matière de sécurité et de protection de la vie privée, les membres de la haute direction responsables de la gouvernance de l'organisation à cet égard et leur personnel peuvent commencer à coordonner l'attribution des activités et des contrôles.

L'élaboration d'une stratégie pour l'attribution des activités et des contrôles de sécurité et de protection de la vie privée commence par la détermination des activités et des contrôles communs, hybrides ou propres au système. Il est également important d'identifier les parties responsables de la mise en œuvre et de l'exploitation des activités et des contrôles communs et hybrides dans l'organisation. Obtenir le soutien du comité de l'architecture d'entreprise peut faciliter ce processus.

4.3.1 Attribuer les activités et les contrôles communs

Objectif : Coordonner et documenter l'attribution des activités et des contrôles communs.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Dans une organisation bien établie, il est possible que certaines activités et certains contrôles soient déjà fournis par l'intermédiaire de services partagés ou communs. Ceux-ci devraient être indiqués et documentés dans l'architecture de sécurité d'entreprise. Dans le cas des activités et des contrôles qui ne sont pas déjà en place, les responsabilités devraient être clairement définies et attribuées avec la fonction responsable de l'architecture de sécurité d'entreprise.

Les organisations peuvent attribuer les activités et les contrôles communs en matière de sécurité et de protection de la vie privée de plusieurs façons. Ils peuvent être attribués :

- à des fonctions responsables de la cybersécurité et de la protection de la vie privée;
- à un groupe opérationnel de TI et de TO de l'organisation;
- à d'autres groupes dans l'organisation ou être externalisés à une autre organisation ou à un autre fournisseur de services;
- à un nouveau service partagé ou commun.

Le [tableau 1](#) donne des exemples des activités et des contrôles communs en matière de sécurité et de protection de la vie privée qu'il est possible d'attribuer.

Tableau 1 : Exemples d'attribution d'activités et de contrôles communs

Activités et contrôles communs	Attribution par la fonction responsable de l'architecture de sécurité d'entreprise	Autorité opérationnelle
CA-07 Surveillance continue	Mettre en œuvre une infrastructure de surveillance automatisée	Autorités de cybersécurité (comme composante de la fonction de cybersécurité)
SC-07 Protection des frontières	Mettre en œuvre une infrastructure de protection des frontières	Groupe opérationnel de TI ou de TO – Opérations réseau
CP-07 Site de traitement auxiliaire	Contrat de services	Fournisseur de services
IA-02 Identification et authentification (utilisatrices et utilisateurs de l'organisation)	S'abonner à un service partagé existant d'identification et d'authentification du GC	Services partagés Canada (SPC) ⁴
PT-01 Politique et procédures de traitement des renseignements personnels et de transparence	L'autorité des politiques d'entreprise publie les politiques et les procédures relatives au traitement des renseignements personnels	Autorités de protection de la vie privée (comme composante d'une fonction de protection de la vie privée)

Si l'attribution d'une activité ou d'un contrôle de sécurité ou de protection commun exige la mise en œuvre de systèmes de soutien, les organisations devraient le faire dans le cadre de projets qui respectent le processus décrit dans le document Activités de gestion des risques pour la cybersécurité et la vie privée tout au long du cycle de vie des systèmes (ITSP.10.037).

Résultat : Document dressant la liste des activités et des contrôles de sécurité et de protection de la vie privée communs ayant été attribués.

4.3.2 Attribuer les activités et les contrôles propres au système

Objectif : Coordonner et documenter l'attribution des activités et des contrôles propres à un système.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Pour mettre en œuvre les activités et les contrôles de sécurité et de protection de la vie privée sélectionnés, la fonction responsable de l'architecture de sécurité d'entreprise attribuera un ensemble d'activités et de contrôles appropriés à ce système. Les contrôles techniques propres au système doivent être déterminés au début du cycle de vie du projet pour veiller à ce qu'ils aient la portée, les ressources et les fonds budgétaires nécessaires. Cette approche proactive permet de garantir que les activités et les contrôles sont intégrés facilement dans le développement et l'exploitation du système, plutôt que d'être reconfigurés après la mise en œuvre, augmentant par la même occasion les coûts ou la complexité.

⁴ Fournisseur désigné des services partagés du GC.

Le processus d'attribution comprend la mise en correspondance des contrôles applicables (dont les contrôles hybrides) aux contextes du système et la coordination des responsabilités de mise en œuvre entre les parties prenantes responsables de la cybersécurité, de la protection de la vie privée et des activités.

Les groupes opérationnels de TI ou de TO et ceux chargés des projets mettent en œuvre et exploitent les activités et les contrôles de sécurité et de protection de la vie privée dans les systèmes conformément aux activités de gestion des risques pour la cybersécurité et la vie privée décrites dans l'ITSP.10.037.

Une documentation claire des attributions des activités et des contrôles permet également de soutenir une assurance continue, l'état de préparation à la vérification et la capacité de gérer l'efficacité des contrôles au fil du temps.

Résultat : Liste des activités et des contrôles de sécurité et de protection de la vie privée attribués dans les systèmes.

4.4 Surveiller et évaluer le niveau de performance des activités et des contrôles en matière de sécurité et de protection de la vie privée

Objectif : Procéder à une surveillance et à une évaluation continues des activités et des contrôles de sécurité et de protection de la vie privée ayant été mis en œuvre.

Rôles connexes suggérés : Groupes opérationnels de TI ou de TO, évaluatrices et évaluateurs de la sécurité, évaluatrices et évaluateurs de la protection de la vie privée

Les organisations surveillent et évaluent le niveau de performance des activités et des contrôles communs, hybrides et propres au système qui ont été mis en œuvre en misant sur la collecte, la consolidation et l'analyse continue des indicateurs de performance. Un bon nombre des tâches de surveillance et d'évaluation seront effectuées par les groupes opérationnels de TI ou de TO, et les rapports récapitulatifs seront fournis aux fonctions responsables de la cybersécurité et de la protection de la vie privée aux fins d'analyse panorganisationnelle. Certaines tâches de surveillance sensibles peuvent être effectuées par les fonctions responsables de la cybersécurité et de la protection de la vie privée (si elles sont exigées par un profil d'activités et de contrôles en matière de sécurité et de protection de la vie privée) lorsque la séparation des tâches est nécessaire.

Les tâches liées à l'évaluation continue⁵ considèrent plus que le niveau de performance des activités et des contrôles de sécurité et de protection de la vie privée. Elles devraient entre autres tenir compte de ce qui suit :

- relever les vulnérabilités, les faiblesses et les inefficacités;
- passer en revue les changements liés à la sécurité et à la protection de la vie privée;
- passer en revue les rapports d'incidents et de problèmes liés à la sécurité et à la protection de la vie privée;
- procéder à des tests de la sécurité, ce qui pourrait comprendre des tests fonctionnels de la sécurité, des évaluations des vulnérabilités et des tests d'intrusion;
- passer en revue la configuration de sécurité des composants du système.

⁵ Par évaluation continue, on n'entend pas nécessairement une évaluation en temps réel. Certaines activités d'évaluation, comme l'examen des journaux d'événements, peuvent être effectuées automatiquement en temps réel, tandis que d'autres, comme l'examen des procédures de sauvegarde des systèmes, sont généralement réalisées manuellement selon un horaire prédéfini.

Les résultats de la surveillance et de l'évaluation informeront les autorités de l'organisation de l'état actuel de la posture de sécurité et de protection de la vie privée des systèmes organisationnels. Une posture de sécurité et de la protection de la vie privée stable et adéquate permettra au système de maintenir son autorisation d'exploiter. Une détérioration de la posture pourrait forcer les autorités de l'organisation à révoquer l'autorisation d'exploiter jusqu'à ce que les mesures d'atténuation nécessaires soient prises (voir la [section 4.5](#) et la [section 4.6](#)).

Résultat : Rapport sur le niveau de performance des activités et des contrôles de sécurité et de protection de la vie privée, ainsi sur la posture des systèmes en matière de sécurité et de protection de la vie privée.

4.5 Maintenir l'autorisation

Objectif : Maintenir l'état d'autorisation des systèmes.

Rôles connexes suggérés : Autorisatrices et autorisateurs, analystes des activités, conseillères et conseillers en sécurité, conseillères et conseillers en protection de la vie privée, architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Lorsqu'elles suivent le processus suggéré de gestion des risques pour la cybersécurité et la vie privée, les organisations autorisent d'abord l'exploitation de leurs systèmes dans le cadre du processus détaillé dans l'ITSP.10.037. Par la suite, les organisations maintiennent l'état d'autorisation de leurs systèmes en s'assurant de surveiller, d'évaluer et de mettre à jour continuellement les activités et les contrôles de sécurité et de protection de la vie privée.

Le processus de maintien des autorisations consiste à effectuer les activités suivantes :

- procéder à l'examen régulier de l'évaluation et de la catégorisation du préjudice lié aux activités opérationnelles prises en charge;
- réévaluer l'environnement de menace et le niveau de performance des environnements techniques en matière de sécurité;
- réévaluer la collecte et l'utilisation des renseignements personnels pour comprendre les changements apportés à la conception initiale du programme;
- passer en revue les résultats de l'évaluation du niveau de performance des activités et des contrôles de sécurité et de protection de la vie privée;
- passer en revue les activités du groupe opérationnel de TI ou de TO pour confirmer qu'elles ont permis de maintenir adéquatement la posture de sécurité et de protection de la vie privée des systèmes conformément aux dispositions stipulées dans les plans opérationnels en matière de sécurité et de protection de la vie privée.

Lorsque les résultats des activités de maintien de l'autorisation démontrent que le fonctionnement d'un système ne respecte plus les niveaux acceptables de risque résiduel, les organisations peuvent remédier à la situation de plusieurs manières, notamment en faisant ce qui suit :

- mettre en œuvre des mesures de sécurité temporaires pour protéger les activités opérationnelles prises en charge (par exemple, déconnecter un système d'information d'Internet, activer une partie d'un plan d'urgence);
- mettre à jour les artéfacts de protection de la vie privée (par exemple, les avis et énoncés de confidentialité et les fichiers de renseignements personnels connexes, sous réserve de l'obtention des approbations nécessaires);

- mettre à jour les activités et les contrôles mis en œuvre pour corriger les lacunes en matière de sécurité et de protection de la vie privée et rétablir le système à son état d'exploitation autorisé (voir la [section 4.6](#));
- accepter le nouveau niveau de risque résiduel.

Si le niveau de risque résiduel demeure inacceptable après l'application des mesures initiales, les responsables de l'autorisation peuvent choisir de révoquer l'autorisation d'exploiter jusqu'à la prise de plus amples mesures correctives. La révocation de l'autorisation donnera lieu à des activités additionnelles d'analyse de la sécurité et des facteurs relatifs à la vie privée afin de relever les lacunes propres au contexte opérationnel. Ces activités seront suivies par l'application de mesures correctives ou d'améliorations aux activités et aux contrôles pour rétablir le système à son état autorisé.

Les organisations devraient préciser dans leur plan de sécurité organisationnel à quelle fréquence il convient d'effectuer les activités d'évaluation et d'examen de la sécurité (par exemple, l'examen des rapports d'incidents de sécurité, l'examen de l'environnement de menace, l'examen des activités opérationnelles du groupe opérationnel de TI ou de TO). Autrement, les responsables de l'autorisation pourraient déterminer la fréquence de ces activités au cours de la mise en œuvre initiale d'un système selon des facteurs tels que la catégorisation du préjudice en matière de sécurité, les menaces, les niveaux de risque résiduel et les lacunes de sécurité non résolues.

Les résultats des activités de maintien de l'autorisation comprennent des évaluations actualisées du risque résiduel et les dispositions en matière de sécurité qui ont été mises à jour dans le plan opérationnel. Les dispositions en matière de sécurité stipulées dans le plan opérationnel devraient comprendre des plans et des calendriers d'atténuation pour toutes les lacunes de sécurité non résolues qui ont été relevées dans le cadre de la réalisation de l'évaluation de sécurité (voir la [section 4.6](#)).

Dans le GC, les programmes doivent revoir chaque année les risques relevés lors du processus d'évaluation de la protection de la vie privée et mettre à jour les mesures d'atténuation des risques.

Résultats : Mise à jour des évaluations du risque résiduel et des dispositions du plan opérationnel en matière de sécurité.

4.6 Mettre à jour le ou les profils d'activités et de contrôles en matière de sécurité et de protection de la vie privée

Objectif : S'assurer que la posture du programme en matière de sécurité et de protection de la vie privée, ainsi que celle du système, demeurent adéquates en tenant à jour l'ensemble des activités et des contrôles mis en œuvre. Au besoin, ajouter des activités et des contrôles pour renforcer la posture de sécurité et de protection de la vie privée.

Rôles connexes suggérés : Architectes de sécurité d'entreprise, architectes de la protection de la vie privée

Les organisations pourraient avoir à mettre à jour les activités et les contrôles de sécurité et de protection de la vie privée qu'elles ont mis en œuvre pour diverses raisons, notamment dans les cas suivants :

- un changement apporté aux missions ou aux objectifs de l'organisation;
- un changement apporté à l'activité opérationnelle de l'organisation (par exemple, la collecte de nouveaux renseignements plus sensibles dans le cadre d'un programme organisationnel existant);
- un changement apporté aux besoins opérationnels en matière de sécurité et de protection de la vie privée (par exemple, en raison de changements législatifs ou de politique);

- un changement apporté dans la collecte, l'utilisation ou la divulgation de renseignements personnels;
- la nécessité d'apporter des changements en raison de la mise à jour d'une évaluation des menaces de l'organisation (à savoir, lorsqu'un programme est ciblé par plusieurs auteurs de menace dotés de moyens sophistiqués);
- la nécessité d'apporter des changements en raison de la surveillance du niveau de performance (par exemple, une activité ou un contrôle de sécurité et de protection de la vie privée s'avère inefficace pour protéger adéquatement les systèmes ou les renseignements personnels concernés).

Les principaux éléments de cette activité comprennent les profils d'activités et de contrôles de l'organisation, les référentiels des menaces, les résultats de la surveillance du niveau de performance, ainsi que les activités de maintien des évaluations et des autorisations (voir la [section 4.4](#) et la [section 4.5](#)). Cette approche permet de révéler les lacunes dans les activités et les contrôles existants, ce qui donnera lieu à des mises à jour ou à l'ajout de nouvelles activités et de nouveaux contrôles. Il pourrait également être nécessaire de revoir les activités et les contrôles de cybersécurité et de protection de la vie privée plus tôt afin de redéfinir les exigences, de mettre à jour les profils d'activités et de contrôles et les référentiels de menaces (voir, par exemple, la [section 4.1.3](#), la [section 4.1.6](#) ou la [section 4.2](#)), d'attribuer de nouvelles activités ou de nouveaux contrôles (voir la [section 4.3](#)) ou de procéder à une surveillance et une évaluation plus poussées (voir la [section 4.4](#)).

Résultat : Rapport sur la nécessité d'améliorer les activités et les contrôles de sécurité et de protection de la vie privée, d'en créer de nouveaux ou de mettre à jour le ou les profils.

5 Processus d'évaluation et de catégorisation du préjudice

La présente section décrit la façon dont les organisations peuvent réaliser les évaluations et la catégorisation du préjudice lié à leurs activités opérationnelles afin de mieux définir les profils de leurs activités et de leurs contrôles en matière de sécurité et de protection de la vie privée. Par activités opérationnelles, on entend les processus opérationnels et les biens d'information connexes, ce qui comprend les renseignements personnels.

Le processus d'évaluation et de catégorisation du préjudice est un instrument qui permet d'établir l'importance relative des activités opérationnelles de l'organisation. Au niveau de l'organisation, les catégories de préjudice des activités opérationnelles servent de données d'entrée pour les évaluations des menaces et l'élaboration des profils d'activités et de contrôles. Au niveau du système, les catégories de préjudice des activités opérationnelles servent de données d'entrée pour ce qui est d'établir les exigences d'assurance de sécurité, de sélectionner et d'adapter les activités et les contrôles de sécurité et de protection de la vie privée, et de réaliser une EMR.

5.1 Concepts

La compromission des activités opérationnelles par des cybermenaces pourrait causer un préjudice aux intérêts nationaux⁶ ou aux intérêts non nationaux⁷ qu'elles visent à servir. Le préjudice pourrait résulter d'une utilisation, d'une divulgation ou d'une modification non autorisée, d'un refus d'accès à l'information ou de la corruption ou de l'interruption des processus opérationnels. Un préjudice causé par une utilisation ou une divulgation non autorisée d'information relève de l'**objectif de confidentialité** de la sécurité de l'information. Un préjudice causé par une modification de l'information ou la corruption de processus opérationnels relève de l'**objectif d'intégrité** (à savoir, l'exactitude, l'exhaustivité, l'authenticité, l'utilisation prévue) de la sécurité de l'information. Un préjudice causé par un refus d'accès à l'information ou à l'interruption des processus opérationnels relève de l'**objectif de disponibilité** de la sécurité de l'information.

Le processus d'évaluation et de catégorisation du préjudice détermine un niveau de préjudice pour chaque objectif de sécurité associé à une activité opérationnelle. La désignation d'un niveau de préjudice suppose une compromission fructueuse par un auteur de menace. L'évaluation peut ainsi mettre l'accent sur les préjudices qui pourraient raisonnablement résulter de cet événement.

5.1.1 Systèmes de sécurité nationale

Un système de sécurité nationale (SSN) est un système dont la compromission, que ce soit sur le plan de la confidentialité, de l'intégrité ou de la disponibilité, pourrait porter atteinte à la sécurité nationale. Bien que la désignation des SSN corresponde souvent au niveau de classification (par exemple, CONFIDENTIEL, SECRET, TRÈS SECRET), la classification n'est pas un facteur déterminant en soi. Certains systèmes peuvent porter la mention NON CLASSIFIÉ, mais tout de même être considérés comme des SSN si leur compromission peut raisonnablement porter atteinte à la sécurité nationale.

⁶ Intérêts nationaux : La sécurité et la stabilité sociopolitique et économique du Canada.

⁷ Intérêts non nationaux : La sûreté, la santé et le bien-être des personnes; la situation financière et la réputation des citoyennes, des citoyens et des entreprises canadiennes.

Au Canada, le SCT confère à la mention NON CLASSIFIÉ le sens de « non sensible ». Cela dit, le niveau de classification d'un système n'élimine pas son incidence potentielle. Par exemple, la compromission d'un système d'armement militaire à bord d'un navire ou d'un véhicule blindé pourrait causer une atteinte à la sécurité nationale. À ce titre, il convient d'identifier ce système comme SSN lors du processus de catégorisation du préjudice. Les principaux points à considérer pour la désignation des SSN sont le préjudice potentiel envers la sécurité nationale, et non le niveau de classification. Les évaluations du préjudice devraient porter sur les conséquences de la compromission plutôt que sur le fait qu'un système est considéré comme étant classifié ou non classifié.

5.1.2 Sécurité

Lors de l'évaluation de systèmes essentiels à la sécurité dont la défaillance pourrait donner lieu à des répercussions sur la santé, à des pertes de vie, à des pertes ou dommages matériels ou à la dégradation de l'environnement, il est essentiel de tenir compte de la classification de l'information et de la façon dont les exigences de sécurité influent sur le potentiel de dommages advenant la compromission des systèmes. Dans de tels cas, les exigences de sécurité peuvent amplifier l'incidence potentielle sur la disponibilité, l'intégrité et, dans certains contextes, la confidentialité, ce qui se traduira par des niveaux de préjudice plus élevés lors du processus de catégorisation du préjudice. Les systèmes essentiels à la sécurité sont généralement soumis à des exigences rigoureuses en matière de disponibilité et d'intégrité, et la confidentialité pourrait également être importante selon le contexte opérationnel. Au final, la gravité affectée au préjudice devrait être proportionnelle au niveau de préjudice qui pourrait raisonnablement résulter de la compromission du système.

5.1.3 Protection de la vie privée

Les évaluations du préjudice doivent tenir compte de l'incidence potentielle sur la vie privée des individus si les activités opérationnelles comportent des renseignements personnels. Les renseignements personnels compromis peuvent causer des préjudices aux individus et aux organisations et se traduire par ce qui suit :

- un vol d'identité ou une fraude;
- une atteinte à la réputation ou un préjudice émotionnel;
- une perte de confiance du public;
- des conséquences sur les plans juridique et réglementaire.

Le niveau varie selon la sensibilité, le volume et le contexte des renseignements personnels. En plus des atteintes à la sécurité des renseignements personnels, un préjudice découlant de l'atteinte à la vie privée pourrait également résulter de la corruption de données personnelles et mener à des décisions erronées ou à une perturbation de services essentiels à l'accès à des prestations ou à du soutien. Cela est particulièrement important dans les systèmes essentiels à la sécurité ou essentiels aux services, comme les services de santé ou d'urgence. Les risques d'atteinte à la vie privée devraient être considérés parallèlement aux objectifs de confidentialité, d'intégrité et de disponibilité dans le cadre du processus de catégorisation du préjudice. Lorsque des renseignements personnels sont utilisés pour faciliter la prise de décisions administratives, une EFVP devrait être réalisée en plus des évaluations des risques et des menaces pour s'assurer que les activités et les contrôles de sécurité et de protection de la vie privée appropriés ont été sélectionnés.

5.1.4 Perspective adverse

Le processus d'évaluation et de catégorisation du préjudice exige la formulation de la compromission selon une perspective adverse. Les praticiennes et praticiens de la sécurité et de la protection de la vie privée devraient évaluer le préjudice en supposant qu'un auteur de menace a réussi à compromettre le système et envisager des scénarios où ce dernier aurait obtenu un plus grand contrôle. La plupart des organisations sous-estiment les préjudices potentiels, puisque leur approche au risque repose sur la bonne foi et des hypothèses raisonnables. Certains auteurs de menaces sont toujours prêts à adopter des comportements extraordinaires et moralement répréhensibles pour atteindre leurs objectifs.

Par exemple, on devrait considérer qu'un processus opérationnel, comme le fonctionnement des systèmes de maintien des fonctions vitales dans un hôpital, a le potentiel d'entraîner un préjudice grave à la santé des patientes et patients, ou même de causer des lésions corporelles ou des pertes de vie. Pour citer un autre exemple, un ministère doté d'un mandat de sécurité pourrait, advenant sa compromission, être utilisé par un criminel ou un outil hostile contrôlé par un auteur de menace, en contradiction totale avec son mandat.

La question qu'il convient de se poser est la suivante : Quel est le pire des scénarios?

5.1.5 Préjudice post-compromission

L'évaluation du préjudice doit reposer sur la présomption qu'une attaque fructueuse est survenue. À cette étape, on ne devrait pas tenir compte de la probabilité d'une menace ni de la présence de contrôles d'atténuation. Lors de l'évaluation du préjudice potentiel, même les scénarios jugés comme étant très peu probables doivent être envisagés comme s'ils s'étaient déjà concrétisés.

Par exemple, bien que le bombardement d'un centre de données puisse être considéré comme fort improbable, le préjudice qui en résulterait – la perte totale de toutes les fonctionnalités du site – reste un facteur valide à considérer dans l'évaluation. De même, l'existence de centres de données redondants ne réduit pas la gravité du préjudice à cette étape du processus.

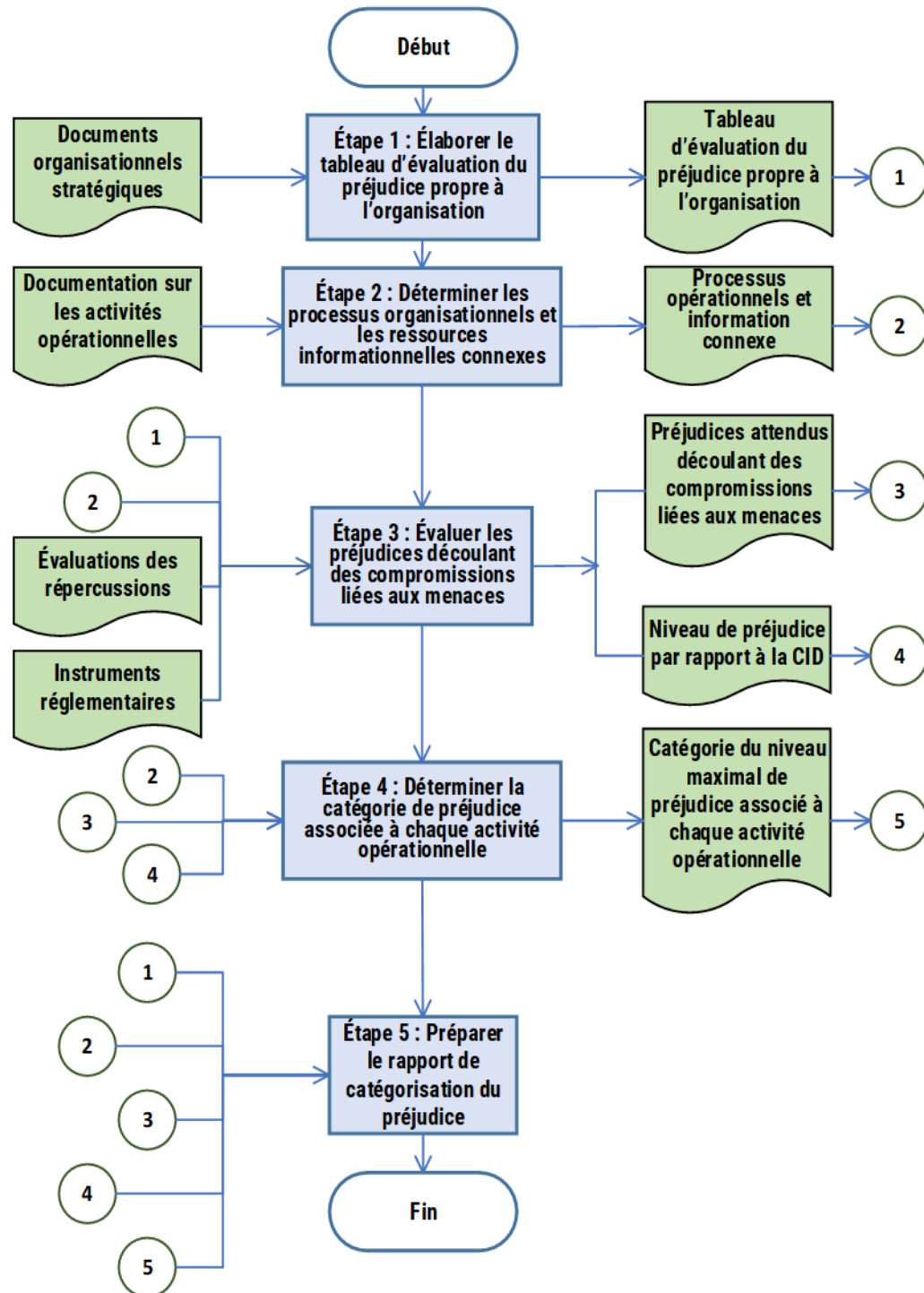
La question qu'il convient de se poser est la suivante : Qu'advient-il si le pire des scénarios se concrétise?

5.2 Processus d'évaluation et de catégorisation du préjudice

Comme il est illustré dans la [figure 3](#), le processus d'évaluation et de catégorisation du préjudice lié à une activité opérationnelle peut être résumé en cinq étapes :

1. Élaborer un tableau d'évaluation personnalisé du préjudice;
2. Déterminer les processus opérationnels et les biens d'information, dont les renseignements personnels, relatifs à l'activité opérationnelle;
3. Évaluer le préjudice prévu résultant d'une compromission de l'activité opérationnelle par une menace présumée et déterminer sa gravité en matière de confidentialité, d'intégrité et de disponibilité;
4. Déterminer la catégorie de préjudice de l'activité opérationnelle en identifiant le plus haut niveau de préjudice prévu en matière de confidentialité, d'intégrité et de disponibilité;
5. Préparer un rapport d'évaluation et de catégorisation du préjudice.

Figure 3 : Processus d'évaluation et de catégorisation du préjudice



Description longue – Figure 3 : Processus d'évaluation et de catégorisation du préjudice

La figure présente un organigramme vertical illustrant le processus d'évaluation et de catégorisation du préjudice. Une colonne centrale unique montre les cinq étapes numérotées du processus, de haut en bas, chacune représentée par un rectangle bleu relié au suivant par une flèche descendante. Le processus commence par un ovale bleu intitulé « Début » et se termine par un ovale bleu intitulé « Fin ». À plusieurs étapes, des intrants apparaissent à gauche du diagramme et alimentent l'étape correspondante au moyen de flèches, tandis que les extrants sont représentés à droite sous forme d'encadrés blancs en forme de document. Chaque encadré des extrants comporte un petit cercle numéroté servant d'identificateur de référence permanent pour indiquer ultérieurement où cet extrant est réutilisé comme intrant.

La séquence centrale est la suivante :

- Début : un ovale bleu intitulé « Début », suivi d'une flèche descendante menant à l'étape 1.
- Étape 1 : Élaborer le tableau d'évaluation du préjudice propre à l'organisation
 - Intrant à gauche : une étiquette rectangulaire intitulée « Documents organisationnels stratégiques » alimente l'étape 1.
 - Extrant à droite : un encadré en forme de document intitulé « Tableau d'évaluation du préjudice propre à l'organisation », identifié par un petit cercle portant le numéro 1. Il s'agit de l'extrant 1.
 - Remarque concernant la réutilisation : l'extrant 1 sert ultérieurement d'intrant à l'étape 3, comme l'indique le petit cercle 1 situé à gauche de cette étape.
- Étape 2 : Déterminer les processus organisationnels et les ressources informationnelles connexes
 - Intrant à gauche : une étiquette rectangulaire intitulée « Documentation sur les activités opérationnelles » alimente l'étape 2.
 - Extrant à droite : un encadré en forme de document intitulé « Processus opérationnels et information connexe », identifié par un petit cercle portant le numéro 2. Il s'agit de l'extrant 2.
 - Remarque concernant la réutilisation : l'extrant 2 sert ultérieurement d'intrant aux étapes 3 et 4, comme l'indique le petit cercle 2 situé à gauche de ces étapes.
- Étape 3 : Évaluer les préjudices découlant des compromissions liées aux menaces
 - Intrants à gauche :
 - deux sources rectangulaires alimentent l'étape 3 et sont intitulées « Évaluations des répercussions » et « Instruments réglementaires ».
 - les cercles 1 et 2, représentant respectivement les extrants 1 et 2, alimentent également cette étape. Ils indiquent que le tableau d'évaluation du préjudice propre à l'organisation, ainsi que les processus opérationnels et l'information connexe recensés, sont utilisés dans l'évaluation des préjudices.
 - Extrants à droite :
 - un encadré intitulé « Préjudices attendus découlant des compromissions liées aux menaces » est identifié par un cercle 3. Il s'agit de l'extrant 3.
 - un second encadré intitulé « Niveau de préjudice par rapport à la CID » est identifié par le cercle 4. Il s'agit de l'extrant 4.

- Remarque concernant la réutilisation : les extrants 3 et 4 servent ultérieurement d'intrants à l'étape 4, comme l'indiquent les petits cercles 3 et 4 situés à gauche de cette étape.
- Étape 4 : Déterminer la catégorie de préjudice associée à chaque activité opérationnelle
 - Intrants à gauche :
 - une colonne verticale composée des cercles 2, 3 et 4 indique la réutilisation des extrants 2, 3 et 4 pour déterminer la catégorie de préjudice.
 - Extrant à droite :
 - un encadré blanc intitulé « Catégorie du niveau maximal de préjudice associé à chaque activité opérationnelle » est identifié par le cercle 5. Il s'agit de l'extrant 5. L'expression « catégorie du niveau maximal » indique que la catégorie retenue correspond au niveau de gravité le plus élevé attendu parmi les critères de confidentialité, d'intégrité et de disponibilité.
 - Remarque concernant la réutilisation : l'extrant 5 sert d'intrant à l'étape 5, comme l'indique le petit cercle 5 situé à gauche.
- Étape 5 : Préparer le rapport de catégorisation du préjudice
 - Intrants à gauche : une série verticale de cercles 1, 2, 3, 4 et 5 indique que le rapport final regroupe l'ensemble des extrants précédents : extrant 1 (tableau propre à l'organisation), extrant 2 (processus opérationnels et information), extrant 3 (préjudices attendus), extrant 4 (niveau de préjudice par rapport à la CID) et extrant 5 (catégorie du niveau maximal de préjudice).
 - Aucun encadré d'extrant n'est représenté à droite; le processus se poursuit jusqu'à la fin.
- Fin : un ovale bleu intitulé « Fin », situé sous l'étape 5, marque la conclusion du processus.

Remarque propre au GC

L'objectif du processus de catégorisation de la sécurité est de déterminer la sensibilité et la criticité des activités opérationnelles en fonction d'un test de préjudice. Il s'agit d'un objectif similaire à celui du questionnaire d'évaluation de la sensibilité que l'on retrouve dans l'énoncé de sensibilité (ES) de plusieurs ministères et organismes. Un ES comprend les types de biens d'information stockés et traités par un système d'information, ainsi que la classification de cette information (par exemple, PROTÉGÉ B). L'ES collecte également l'importance générale de l'intégrité, ainsi que la criticité du programme ou des services, laquelle est souvent exprimée en tant que durée maximale d'indisponibilité permise.

Bien que le préjudice se reflète dans la mention de classification de l'information, le processus de catégorisation de la sécurité énonce clairement le test de préjudice en matière de confidentialité. Par ailleurs, le processus de catégorisation de la sécurité étend ces tests de préjudice explicites à l'intégrité et à la disponibilité. Il en résulte une mention de sécurité qui reflète le niveau attendu de préjudice pour la confidentialité, l'intégrité et la disponibilité (par exemple, PROTÉGÉ B, intégrité moyenne, disponibilité moyenne ou PBMM).

Dans les ministères et les organismes où le processus d'ES est bien établi depuis plusieurs années, le fait d'abandonner entièrement ce processus familier pourrait ne pas constituer la meilleure approche à adopter pour faciliter la transition vers le processus de catégorisation de la sécurité. Les ministères et les organismes pourraient tirer avantage de la familiarité et de l'acceptabilité suscitées par leur processus d'ES et intégrer tout simplement un test de préjudice dans les sections de leur questionnaire d'évaluation de la sensibilité traitant de la confidentialité, de l'intégrité et de la disponibilité.

5.3 Description du processus d'évaluation et de catégorisation du préjudice

L'organisation devrait mettre en place un groupe de travail dédié à l'exécution efficace du processus d'évaluation et de catégorisation du préjudice. Ce groupe devrait généralement comprendre des membres de la haute direction exerçant des responsabilités opérationnelles, des responsables principales et principaux de la sécurité (comme la ou le DPS ou des personnes déléguées), les responsables principales et principaux de la protection de la vie privée (comme la ou le CPRP ou des personnes déléguées), des conseillères et conseillers en sécurité et en protection de la vie privée, et des analystes des activités. Selon l'organisation et le contexte, d'autres rôles pourraient comprendre une ou un responsable de la gestion des risques, une conseillère ou un conseiller juridique, une agente ou un agent de la conformité, des architectes de la sécurité et de la protection de la vie privée, et une ou un responsable des communications et des relations publiques.

5.3.1 Élaborer le tableau d'évaluation du préjudice propre à l'organisation

En ce qui concerne l'évaluation et la catégorisation du préjudice, les organisations devraient créer leurs propres tableaux des préjudices. De petites organisations n'ayant qu'un seul ou un petit nombre de programmes servant des intérêts communs peuvent n'avoir qu'un seul tableau des préjudices, tandis que des organisations ayant plusieurs programmes servant différents intérêts peuvent en avoir plusieurs. Si les seuils financiers sont intégrés dans le tableau personnalisé des préjudices, les sommes exprimées en dollars devraient être proportionnelles au budget global de l'organisation afin d'assurer la pertinence selon le contexte. Par exemple, dans le GC, les intérêts servis par le programme Administration des pensions fédérales de Services publics et Approvisionnement Canada (SPAC) sont fort différents de ceux servis par les Services linguistiques de SPAC.

Pour développer un tableau d'évaluation du préjudice propre à l'organisation qui permettra d'éclairer les futures évaluations des risques, il est recommandé de consulter les documents organisationnels stratégiques, comme les plans d'activités, les engagements en matière de rendement et les cadres d'établissement des priorités, sur lesquels reposent les objectifs et les obligations de l'organisation. Les analystes des activités devraient prendre part activement à ce processus, puisqu'elles et ils possèdent des connaissances contextuelles essentielles et peuvent aider à définir des scénarios de préjudice réalistes et pertinents. Des sources additionnelles, comme les rapports réglementaires, les rapports de parties prenantes et les résultats d'audits internes, peuvent également fournir de l'information précieuse sur les incidences et les priorités organisationnelles.

Le [tableau 2](#) contient des exemples de types et de niveaux de préjudice qui aideront les ministères du GC à élaborer leurs tableaux. Les ministères ne devraient inclure dans leurs tableaux des préjudices que les types et les niveaux qui se rapportent aux intérêts que visent à satisfaire leurs programmes, leurs services et leurs activités.

Tableau 2 : Exemples de types et de niveaux de préjudice (dans le contexte du GC)

Type de préjudice	Niveau de préjudice très faible	Niveau de préjudice faible	Niveau de préjudice modéré	Niveau de préjudice élevé	Niveau de préjudice très élevé
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, entraves publiques	Émeute	Sabotage de biens indispensables (par exemple, des infrastructures essentielles)	Désordre civil à grande échelle ou actes de sabotage nécessitant l'imposition de la loi martiale
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse psychologique	Trouble de santé mentale	Préjudice psychologique généralisé ou grave
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress ou inconfort	Baisse de la qualité de vie	Perte de sécurité financière	Sans objet
Perte financière pour des entreprises canadiennes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Baisse de rendement	Réduction de la compétitivité	Perte de viabilité	Sans objet
Perte financière pour le gouvernement du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Baisse de rendement d'un programme	Détérioration des résultats d'un programme	Perte de viabilité du programme	Perte de viabilité des principaux programmes
Préjudice causé à l'économie canadienne	Sans objet	Sans objet	Baisse de rendement	Baisse de compétitivité à l'échelle internationale	Compromission des secteurs économiques clés
Préjudice causé à la réputation du Canada	Préjudice négligeable ou aucun préjudice raisonnable prévu	Perte de la confiance du public canadien	Embarras (au Canada ou à l'étranger)	Relations fédérales-provinciales compromises	Relations diplomatiques et internationales compromises
Perte de la souveraineté canadienne	Sans objet	Sans objet	Entraves à l'établissement de politiques gouvernementales importantes	Entraves à l'application efficace de la loi Cessation des activités du gouvernement	Perte de la souveraineté territoriale

Le [tableau 3](#) présente des exemples des types et des niveaux de préjudice qui sont les plus généralement applicables. Les organisations ne devraient inclure dans leurs tableaux des préjudices que les types et les niveaux qui se rapportent aux intérêts que visent à satisfaire leurs programmes, leurs services et leurs activités.

Tableau 3 : Exemples de types et de niveaux de préjudice

Type de préjudice	Niveau de préjudice très faible	Niveau de préjudice faible	Niveau de préjudice modéré	Niveau de préjudice élevé	Niveau de préjudice très élevé
Protestation contre l'organisation	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, entraves publiques	Émeute	Destruction de biens immobiliers	Sans objet
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleurs physiques, blessures, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse psychologique	Trouble de santé mentale	Préjudice psychologique généralisé ou grave
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress ou inconfort	Baisse de la qualité de vie	Perte de sécurité financière	Sans objet
Perte financière pour l'organisation	Préjudice négligeable ou aucun préjudice raisonnable prévu	Baisse de rendement	Réduction de la compétitivité	Perte de viabilité	Faillite
Mesures juridiques ou réglementaires prises contre l'organisation	Aucune mesure juridique ou réglementaire anticipée Avertissements	Amendes minimales Frais de dédommagement minimales	Amendes modérées Ordres d'arrêt des travaux Frais de dédommagement modérés	Amendes importantes Révocation temporaire des permis Limitation des activités Frais de dédommagement importants	Amendes sévères Révocation permanente des permis Ordonnance de cessation des activités

Type de préjudice	Niveau de préjudice très faible	Niveau de préjudice faible	Niveau de préjudice modéré	Niveau de préjudice élevé	Niveau de préjudice très élevé
Poursuites civiles	Aucune attente raisonnable ou négligeable de responsabilité Règlement à l'amiable pour un montant symbolique	Responsabilité minimale Règlement à l'amiable	Responsabilité modérée Indemnisation	Responsabilité importante Procès très médiatisé Indemnités financières importantes	Responsabilité lourde Recours collectif Sanctions financières importantes Perte de confiance de la clientèle
Atteinte à la réputation	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence minimale sur la réputation Coûts minimaux de gestion de la réputation Faible couverture négative dans les médias et sur les réseaux sociaux	Incidence modérée sur la réputation exigeant des mesures correctives Hausse des coûts liés à la fidélisation et à l'acquisition de clients Couverture négative soutenue dans les médias et sur les réseaux sociaux	Préjudice notable à la réputation exigeant des mesures correctives immédiates Coûts importants liés à la fidélisation et à l'acquisition de clients Couverture étendue et persistante dans les médias et les réseaux sociaux Perte de clientèle attendue	Atteinte à la réputation grave et potentiellement irréparable Perte de clients stratégiques Déclin à long terme de la réputation de la marque

5.3.2 Déterminer les processus organisationnels et les ressources informationnelles connexes

La deuxième étape du processus d'évaluation et de catégorisation du préjudice vise à déterminer les processus organisationnels et les biens d'information connexes, dont les renseignements personnels, qui sont pertinents pour l'activité opérationnelle.

Plusieurs sources peuvent servir à déterminer et à décrire les processus opérationnels et les biens d'information connexes. Les bonnes sources à consulter comprennent :

- les analyses de rentabilisation;
- les CONOPS;
- les exigences fonctionnelles des activités;
- la documentation de l'architecture d'entreprise qui inclut normalement une description des processus opérationnels et des biens d'information connexes de l'organisation;
- les discussions ou les entrevues avec des analystes des activités et d'autres personnes des communautés d'affaires connexes.

Le résultat de cette étape est une brève description des processus opérationnels et des biens d'information connexes qui sont pertinents pour les activités opérationnelles.

5.3.3 Évaluer les préjudices découlant d'une compromission liée aux menaces

La troisième étape du processus est l'évaluation du préjudice. L'objectif est de déterminer le préjudice potentiel des compromissions liées aux menaces pour chaque processus opérationnel et bien d'information relevé à l'étape précédente. Pour ce faire, on doit d'abord déterminer les préjudices qui sont susceptibles de survenir si des auteurs de menace arrivent à compromettre la confidentialité, l'intégrité et la disponibilité des processus opérationnels et des biens d'information connexes, puis y attribuer les niveaux appropriés.

En règle générale, la confidentialité, l'intégrité et la disponibilité s'appliquent aux biens d'information, tandis que l'intégrité et la disponibilité s'appliquent aux processus opérationnels. Dans le GC, la confidentialité peut s'appliquer aux processus opérationnels dans certaines situations exceptionnelles où la sécurité nationale ou la défense nationale sont en cause. Dans le secteur privé, ces exceptions concerneraient habituellement les secrets commerciaux.

Les niveaux de préjudice qui s'appliquent aux activités opérationnelles peuvent déjà être documentés dans les éléments livrables, comme les analyses des répercussions sur les activités, les EFVP, les ES, les évaluations des risques organisationnels et les EMR. Il peut également s'avérer utile de passer en revue les instruments réglementaires, comme les lois, les politiques et la réglementation qui pourraient s'appliquer à des processus opérationnels ou à de l'information en particulier. Dans certaines circonstances, le non-respect de ces exigences réglementaires pourrait entraîner des mesures punitives ou des sanctions susceptibles de causer un préjudice. Les organisations peuvent tirer avantage de cette information lorsqu'elles évaluent les préjudices associés à l'échec de leurs activités opérationnelles.

Au moment d'évaluer les préjudices, les praticiennes et praticiens de la sécurité devraient tenir compte de plusieurs facteurs pouvant influencer sur les résultats, ce qui comprend l'agrégation, l'inférence et l'interdépendance.

5.3.3.1 Agrégation

À mesure que le nombre de biens augmente, le préjudice résultant d'une compromission peut augmenter également. Par exemple, la divulgation non autorisée d'un seul dossier du personnel peut causer un certain embarras à la personne concernée et amener le public à s'inquiéter de la capacité de l'organisation de protéger les renseignements personnels. Cela dit, si tous les dossiers des ressources humaines d'une grande société étaient divulgués de façon inopportune, les répercussions négatives pourraient être considérablement pires.

Du point de vue de la confidentialité, l'agrégation a deux dimensions :

- la sensibilité a tendance à augmenter avec le nombre de données ajoutées à un dossier;
- la sensibilité a tendance à augmenter avec le nombre de dossiers réunis dans un fichier ou une base de données.

Dans chaque cas, la valeur de confidentialité de l'ensemble peut être plus grande que celle de ses diverses parties en raison du préjudice accru que causerait leur divulgation non autorisée.

L'agrégation s'applique aussi aux valeurs de disponibilité et d'intégrité. Par exemple, la destruction d'un bien (comme un seul véhicule), peut entraîner des conséquences clairement définies, alors que la perte de tout un parc serait beaucoup plus

sérieuse. La modification non autorisée d'un seul dossier ou la corruption complète d'une grande base de données serait l'équivalent sur le plan de l'intégrité.

5.3.3.2 Inférence

De par sa nature même, l'inférence ne s'applique qu'à la confidentialité, car l'accès à des données en apparence inoffensives dont la sensibilité est faible ou nulle peut permettre à une personne avertie de tirer des conclusions beaucoup plus préjudiciables sur les capacités ou les intentions d'une autre organisation. Par exemple, l'étude des mouvements de personnel afin d'identifier les qualifications et les affiliations des cadres supérieures et supérieurs ou d'autres employés et employés sélectionnés pour différents postes peut fournir des indicateurs utiles de futurs programmes stratégiques ou plans opérationnels.

Malheureusement, la relation entre différentes données et sources de données peut être très subtile, ténue même, de sorte que les occasions d'inférence sont généralement beaucoup plus difficiles à identifier et à évaluer. D'un point de vue pratique, l'inférence doit être évaluée avec prudence, car les scénarios complexes peuvent exagérer le risque et donner lieu à une surclassification inutile. Les scénarios d'inférence qui soulèvent des préoccupations sont ceux où les agrégations dans un système de sécurité non nationale donnent lieu à des préjudices envers la sécurité nationale.

5.3.3.3 Interdépendance

Les interdépendances font en sorte que la perte ou la dégradation d'un processus opérationnel et de son information peut influencer sur les autres processus et biens d'information. Le but de l'analyse des interdépendances est de déterminer s'il est possible qu'un effet de cascade important résultant de la compromission d'un processus opérationnel ou d'une information ait une incidence sur un autre processus ou une autre information.

Comme pour le problème d'agrégation, le préjudice qui pourrait résulter de la perte successive d'un élément peut être plus grand que le niveau de préjudice attribué à chacun des éléments individuellement. Parmi les types d'interdépendances, on retrouve :

- l'interdépendance physique (par exemple, le matériel produit par une infrastructure que l'on utilise sur une autre);
- l'interdépendance géographique (par exemple, un couloir commun);
- l'interdépendance logique (par exemple, une dépendance découlant des marchés financiers).

Cette étape génère une liste des préjudices prévus et des niveaux de préjudice pour la confidentialité, l'intégrité et la disponibilité selon les processus opérationnels et les biens d'information connexes.

Remarque propre au GC

Pour assurer l'uniformité au sein des ministères et entre ces derniers, les praticiennes et praticiens de la sécurité et de la protection de la vie privée devraient adopter un schéma commun de marquage pour la catégorisation. À titre indicatif, il est recommandé de présenter les catégories de préjudice selon le format de marquage suivant :

- Confidentialité : Niveau protégé ou classifié
- Intégrité : Très faible, Faible, Modéré, Élevé, Très élevé
- Disponibilité : Très faible, Faible, Modéré, Élevé, Très élevé

Par exemple : PROTÉGÉ B, intégrité moyenne, disponibilité moyenne (PBMM)

5.3.4 Déterminer la catégorie de préjudice associée à chaque activité opérationnelle

La quatrième étape du processus d'évaluation et de catégorisation du préjudice consiste à déterminer la catégorie de préjudice de chaque activité opérationnelle.

Dans des circonstances normales, la catégorie de préjudice d'une activité opérationnelle devrait indiquer les niveaux de préjudice les plus élevés de tous les processus et biens d'information connexes pour chacun des objectifs de sécurité. Individuellement, on peut attribuer différents niveaux de préjudice à ces éléments en fonction d'un objectif de protection donné. Par exemple, une activité opérationnelle peut comporter un type d'information avec un niveau de préjudice évalué à Faible pour la confidentialité, et un autre type d'information avec un niveau de préjudice évalué à Modéré pour le même objectif de sécurité (les deux pour des intérêts non nationaux). Ces valeurs individuelles sont importantes et devraient être documentées. La catégorie de préjudice de l'activité opérationnelle devrait toutefois refléter le niveau le plus élevé de préjudice. Dans l'exemple précédent, le niveau de confidentialité de l'activité opérationnelle serait établi à « Modéré ».

Cela dit, une analyse plus poussée pourrait être nécessaire dans certaines circonstances pour déterminer la catégorie de préjudice la plus appropriée. Par exemple, des praticiennes et praticiens de la sécurité ou de la protection de la vie privée peuvent attribuer un niveau plus élevé que le point de référence « Élevé » en raison de l'effet combiné des compromissions résultant d'une menace ou d'une interdépendance envers un processus essentiel qui ne relève pas de l'activité opérationnelle.

Cette étape permet d'attribuer une catégorie de préjudice à chaque activité opérationnelle, laquelle peut être exprimée au moyen du même format de marquage de la catégorisation employé pour les processus opérationnels et l'information.

5.3.5 Préparer le rapport de catégorisation du préjudice

La dernière étape du processus d'évaluation et de catégorisation du préjudice consiste à préparer le rapport à cet égard.

Les praticiennes et praticiens de la sécurité et de la protection de la vie privée devraient résumer dans un rapport les résultats de l'évaluation du préjudice aux fins de la reddition de compte et afin d'être pris en compte dans l'élaboration du profil d'activités et de contrôles organisationnels en matière de sécurité et de protection de la vie privée. Pour chaque processus opérationnel et information connexe, le rapport de catégorisation du préjudice devrait comprendre ce qui suit :

- une brève description du processus opérationnel et du ou des biens d'information connexes;
- une description des préjudices prévus découlant des compromissions associées à chaque menace;
- les niveaux de préjudice prévu en ce qui a trait aux atteintes à la confidentialité, à l'intégrité et à la disponibilité;
- la justification de l'attribution des niveaux de préjudice.

5.4 Exemples

Il existe une feuille de calcul comportant des exemples simples qui faciliteront la représentation du processus d'évaluation et de catégorisation du préjudice pour les activités opérationnelles. Pour demander une copie de cette feuille de calcul, prière de communiquer avec le [Centre d'appel](#)

Annexe A Conversion des niveaux de préjudice du gouvernement du Canada

D'autres cadres d'évaluation du préjudice peuvent utiliser une échelle à trois niveaux (Faible, Modéré et Élevé) plutôt que l'échelle à cinq niveaux décrite dans la présente publication. Lorsque c'est le cas, les ministères peuvent utiliser les conversions d'échelle indiquées dans les tableaux 4, 5 et 6 pour convertir les niveaux de préjudice de leur échelle à trois ou quatre niveaux à l'échelle à cinq niveaux présentée dans l'ITSP.10.036.

Dans le tableau de conversion 6, la catégorie « Faible » de l'échelle à trois niveaux de préjudice peut correspondre à « Très faible » ou « Faible » sur l'échelle à cinq niveaux, tandis que la catégorie « Élevé » peut correspondre à « Élevé » ou « Très élevé ». Pour assurer une catégorisation appropriée, il est recommandé de revoir l'évaluation du préjudice en fonction de l'échelle à cinq niveaux directement, tout en tenant compte du contexte particulier et du niveau de granularité voulu.

Tableau 4 : Confidentialité – Intérêt non national (PROTÉGÉ)

Valeur sur l'échelle à quatre niveaux	Valeur sur l'échelle à cinq niveaux
Aucun préjudice prévu – NON CLASSIFIÉ	Très faible
Faible – PROTÉGÉ A	Faible
Modéré – PROTÉGÉ B	Modéré
Élevé – PROTÉGÉ C	Élevé
s.o.	Très élevé

Tableau 5 : Confidentialité – Intérêt national (Classifié)

Valeur sur l'échelle à quatre niveaux	Valeur sur l'échelle à cinq niveaux
Aucun préjudice prévu – NON CLASSIFIÉ	Très faible
s.o.	Faible
Faible – CONFIDENTIEL	Modéré
Modéré – SECRET	Élevé
Élevé – TRÈS SECRET	Très élevé

Tableau 6 : Intégrité et disponibilité

Valeur sur l'échelle à quatre niveaux	Valeur sur l'échelle à cinq niveaux
Aucun préjudice prévu	Très faible
Faible	
Faible	Faible

Modéré	Modéré
Élevé	Élevé
Élevé	Très élevé