Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) 2019

Publié : le 2020-05-11

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

Nº de catalogue BT22-182/2019F-PDF
ISBN or ISSN: 978-0-660-34802-5

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019

Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) 2019

Du Secrétariat du Conseil du Trésor du Canada

Sur cette page

1.0 Préambule

▼ **Titres de la section**

1.1 À propos du présent document

Dans le présent document, on décrit le Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC). Ce Plan expose les intervenants et les actions à accomplir pour assurer une gestion cohérente, concertée et rapide des événements de cybersécurité dans l'ensemble du gouvernement. Tous les ans, le Plan sera mis à l'essai et sera modifié au besoin.

1.2 Date d'entrée en vigueur

Le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) entrera en vigueur le 8 avril 2020. Il remplace la version à jour du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) du 26 janvier 2018.

1.3 Champ d'application

Le plan est préparé dans l'exercice des responsabilités conférées au Secrétariat du Conseil du Trésor du Canada (SCT) en vertu de la *Politique sur la sécurité du gouvernement* (PSG) et s'adresse à tous les ministères et organismes assujettis à la PSG.

1.4 Définitions

Remarque : Les définitions sont tirées de la *Politique sur la sécurité du gouvernement*. De plus amples exemples sont fournis afin de clarifier le sens de certains termes aux fins du présent Plan.

Compromission :
Une atteinte à la sécurité du gouvernement. Ceci comprend, sans toutefois s'y limiter :

- l'accès, la divulgation, la modification, l'utilisation, l'interruption, la suppression ou la destruction non autorisés de biens ou de renseignements de nature délicate qui entraînent une perte de confidentialité, d'intégrité, de disponibilité ou de valeur;
- des événements qui engendrent la perte d'intégrité ou de disponibilité des services ou des activités du gouvernement.

Événement de sécurité :
Un événement, un acte, une omission ou une situation pouvant nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité.

- Voici des exemples d'événements de cybersécurité : La divulgation d'une nouvelle vulnérabilité ou une information indiquant qu'on menace de lancer une attaque contre un système d'information du gouvernement du Canada (GC) (p. ex., une attaque par déni de service distribué), ou tente de déjouer le périmètre du réseau, entre autres.

Incident de sécurité :
Tout événement (ou série d'événements), tout acte, toute omission ou toute situation qui a entraîné une compromission.

- Tous les incidents de cybersécurité sont considérés comme des événements de cybersécurité (ou un ensemble d'événements de cybersécurité), mais les événements de cybersécurité ne sont pas tous considérés comme des incidents de cybersécurité (veuillez consulter la figure 1).
- Voici des exemples d'incidents de cybersécurité : Exploitation active d'une ou de plusieurs vulnérabilités connues, exfiltration de données, défaillance d'une mesure de sécurité, intrusion d'un service du GC (Gouvernement du Canada) hébergé ou géré en nuage.

Menace :
Tout événement ou acte éventuel, délibéré ou accidentel, qui pourrait entraîner une compromission.

Vulnérabilité :
Un facteur qui pourrait accroître la susceptibilité à la compromission.

Figure 1 : Événements de cybersécurité et incidents de cybersécurité

▼ Figure 1 - Version textuelle

La figure 1 montre la différence entre les événements de cybersécurité et les incidents de cybersécurité comme ils sont définis dans le PGEC GC à l'aide de deux cercles l'un dans l'autre. Le premier grand cercle représente les événements de cybersécurité, et le deuxième cercle, beaucoup plus petit, représente les incidents de cybersécurité en tant que sous-ensemble d'événements de cybersécurité.

1.5 Glossaire des acronymes et des abréviations

BCP (Bureau du Conseil privé)	Bureau du Conseil privé
BDPI (Bureau du dirigeant principal de l'information)	Bureau du dirigeant principal de l'information, partie intégrante du Secrétariat du Conseil du Trésor
CCC (Centre canadien pour la cybersécurité)	Centre canadien pour la cybersécurité, partie intégrante du Centre de la sécurité des télécommunications
CCSNS (Comité canadien sur les systèmes nationaux de sécurité)	Comité canadien sur les systèmes nationaux de sécurité
CIDG (Comité d'intervention des directeurs généraux)	Comité d'intervention des directeurs généraux
COG (Centre des opérations du gouvernement)	Centre des opérations du gouvernement

Comm. (Communications)	Communications
CS (Communications stratégiques)	Communications stratégiques
CSAM (Communications stratégiques et affaires ministérielles)	Communications stratégiques et affaires ministérielles, partie intégrante du Secrétariat du Conseil du Trésor du Canada
CST (Centre de la sécurité des télécommunications)	Centre de la sécurité des télécommunications
DG (Directeur général)	Directeur général
DI (Demande d'intervention)	Demande d'intervention
DPI (Dirigeant principal de l'information)	Dirigeant principal de l'information
DPS (Dirigeant principal de la sécurité)	Dirigeant principal de la sécurité
ECE (Équipe de coordination des événements)	Équipe de coordination des événements
EHD (Équipe de la haute direction)	Équipe de la haute direction
ÉRIC GC (Équipe de réponse aux incidents cybernétiques du gouvernement du Canada)	Équipe de réponse aux incidents cybernétiques du gouvernement du Canada
GC (Gouvernement du Canada)	Gouvernement du Canada
GICO (Gestion des incidents et coordination opérationnelle)	Gestion des incidents et coordination opérationnelle, partie intégrante du Centre canadien pour la cybersécurité
GRC (Gendarmerie royale du Canada)	Gendarmerie royale du Canada
MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes)	Ministère de la Défense nationale/Forces armées canadiennes
PFIU (Plan fédéral d'intervention d'urgence)	Plan fédéral d'intervention d'urgence
PGEC (Plan de gestion des événements de cybersécurité)	Plan de gestion des événements de cybersécurité
POCS (Principal organisme responsable de la sécurité)	Principal organisme responsable de la sécurité
RSSN (Réseaux, sécurité et services numériques)	Réseaux, sécurité et services numériques, partie intégrante de Services partagés Canada
S et R (Sécurité et renseignement)	Sécurité et renseignement
SCRS (Service canadien du renseignement de sécurité)	Service canadien du renseignement de sécurité

SCT (Secrétariat du Conseil du Trésor du Canada)	Secrétariat du Conseil du Trésor du Canada
SECTI (Sécurité de la technologie de l'information)	Sécurité de la technologie de l'information
SMA (Sous-ministre adjoint)	Sous-ministre adjoint
SNS (Systèmes nationaux de sécurité)	Systèmes nationaux de sécurité
SP (Sécurité publique Canada)	Sécurité publique Canada
SPC (Services partagés Canada)	Services partagés Canada
TI (Technologies de l'information)	Technologie de l'information

2.0 Introduction

▼ **Titres de la section**

2.1 Contexte

Les événements de cybersécurité s'appliquant aux systèmes d'information du gouvernement du Canada (GC) peuvent avoir une incidence considérable sur la qualité des programmes et services offerts aux Canadiens, et, par conséquent, sur la confiance qu'ils éprouvent à l'égard du gouvernement. Il est essentiel d'être en mesure d'intervenir rapidement et de manière cohérente et concertée en cas d'événement de cybersécurité à l'échelle du GC (Gouvernement du Canada) afin d'assurer la sécurité et la résilience des programmes et des services gouvernementaux.

2.2 Objet

Le présent document établit un cadre opérationnel pour la gestion des événements de cybersécurité (y compris les cybermenaces, les vulnérabilités et les incidents de sécurité) qui influent ou sont susceptibles d'influer sur la capacité du GC (Gouvernement du Canada) d'offrir des programmes et des services aux Canadiens. Il crée un contexte pour les plans et les procédures que les ministères et organismes ont mis en place pour gérer les événements de cybersécurité liés aux programmes et aux services dont ils sont responsables.

De plus, ce document vient compléter le plan « tous risques » et le mécanisme d'intervention du Plan fédéral d'intervention d'urgence (PFIU) en offrant un cadre cohérent permettant de gérer les conséquences des événements de cybersécurité qui affectent plusieurs organisations gouvernementales et qui minent la confiance dans le gouvernement.

2.3 Portée

La portée du Plan se limite aux événements de cybersécurité (y compris les menaces, vulnérabilités et incidents de sécurité) liés aux systèmes d'information du GC (Gouvernement du Canada) classés secret ou d'un niveau inférieur qui :

- soit influent ou risquent d'influer sur la qualité des programmes ou des services offerts aux Canadiens ou encore sur le fonctionnement du gouvernement, la sécurité ou la confidentialité de l'information ou la confiance à l'endroit du gouvernement;
- soit nécessite une solution intégrée dans l'ensemble du gouvernement afin d'en réduire au minimum les effets et de permettre une atténuation rapide et le rétablissement des programmes et des services.

Le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) ne traite :

- ni des événements de cybersécurité qui concernent les systèmes d'information classés très secret;
- ni de la coordination de la gestion des événements de cybersécurité faisant intervenir plusieurs autorités de compétence, par exemple, les provinces et territoires, les municipalités, d'autres pays ou des organismes non gouvernementaux.

2.4 Objectifs

Le Plan de gestion des événements de cybersécurité a pour but :

- de sensibiliser l'ensemble du GC (Gouvernement du Canada) à l'existence des cybermenaces et des risques de vulnérabilité ainsi que des incidents de cybersécurité confirmés;
- d'améliorer la coordination et la gestion des événements de cybersécurité dans le GC (Gouvernement du Canada);
- d'atténuer les menaces et les vulnérabilités avant l'éventualité d'une compromission;
- d'appuyer les méthodes d'évaluation du cyberrisque et les efforts de priorisation des mesures de redressement du GC (Gouvernement du Canada);
- de réduire au minimum les effets des événements de cybersécurité sur la confidentialité, la disponibilité ou l'intégrité des programmes et services du GC (Gouvernement du Canada) ou de son information et de son fonctionnement;
- d'améliorer la prise de décisions à tous les niveaux nécessaires;
- de renforcer l'échange des connaissances et le savoir-faire au sein du gouvernement;

- de renforcer la confiance de la population dans la capacité du GC (Gouvernement du Canada) de gérer les événements de cybersécurité.

2.5 Hypothèses

La construction du Plan repose sur les hypothèses suivantes :

- tous les ministères et organismes ont mis en place des processus de gestion des événements et des plans de continuité des activités, comme le prévoit la Politique sur la sécurité du gouvernement;
- les responsabilités des divers intervenants du GC (Gouvernement du Canada) responsables de la cybersécurité sont établies conformément aux mandats actuels des ministères;
- les événements de cybersécurité ayant trait à la divulgation des renseignements personnels ou des communications privées seront traités selon les protocoles privés établis;
- les événements de cybersécurité qui concernent plusieurs autorités de compétence (au Canada ou à l'étranger) sont coordonnés selon les plans nationaux de Sécurité publique Canada.

3.0 Gestion des événements de cybersécurité du gouvernement du Canada

▼ **Titres de la section**

La sécurité dans le gouvernement et la continuité des programmes et des services du GC (Gouvernement du Canada) dépendent de la capacité des ministères et organismes, et du gouvernement dans son ensemble, à gérer les événements de cybersécurité. Les ministères et organismes connaissent des événements qui influent ou risquent d'influer sur la qualité des programmes et des services publics. Étant donné que le GC (Gouvernement du Canada) recourt de

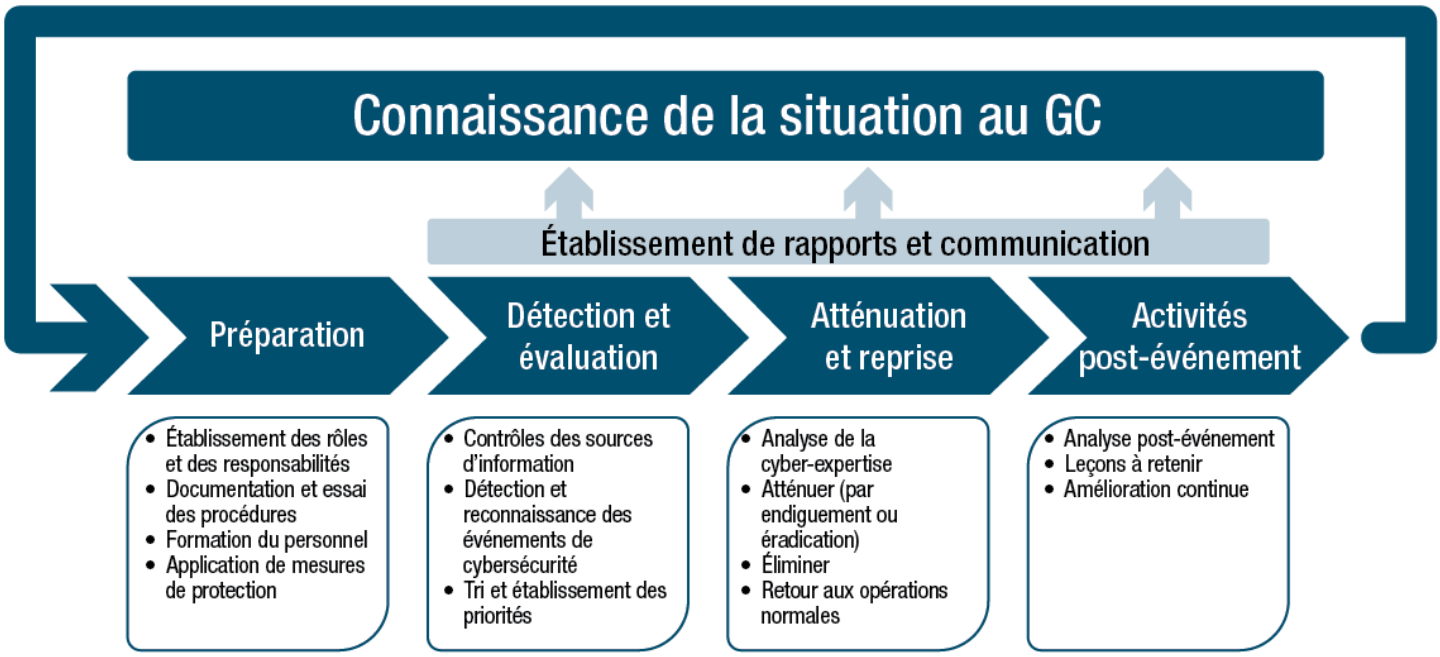
plus en plus à la TI (Technologies de l'information) pour dispenser ses services aux Canadiens et réaliser ses activités, il doit être prêt à réagir vite et efficacement lorsqu'un événement est susceptible de nuire à ses activités ou à la qualité des services qu'il offre aux Canadiens, ou de miner la confiance dans le gouvernement.

Le Plan de gestion des événements de cybersécurité (PGEC GC) identifie les intervenants et les actions à accomplir pour assurer une gestion cohérente, concertée et rapide des événements dans l'ensemble du GC. La présente section expose le processus de gestion des événements de cybersécurité, identifie les intervenants concernés, définit les niveaux d'intervention et décrit les éléments déclencheurs de la signalisation progressive.

3.1 Vue d'ensemble du processus

Le processus global de gestion des événements de cybersécurité comporte plusieurs phases, comme l'indique la figure 2.

Figure 2 : Processus de gestion des événements de cybersécurité



▼ Figure 2 - Version textuelle

La figure 2 représente le processus global de gestion des événements de cybersécurité et ses multiples phases, comme défini dans le présent document. Les quatre phases (Préparation, Détection et évaluation, Atténuation et reprise, et Activité après l'événement) sont illustrées au milieu, avec une flèche pointant de la phase finale (Activité après l'événement) vers la première (Préparation) pour indiquer une boucle de rétroaction continue. Chaque phase clé est décrite brièvement. Les descriptions sont les suivantes :

1. Préparation
    a. Établir les rôles et les responsabilités
    b. Documenter et tester les procédures

c. Former le personnel
d. Appliquer des mesures de protection

2. Détection et évaluation
    a. Surveiller les sources d'information
    b. Détecter et reconnaître les événements de cybersécurité
    c. Trier et établir les priorités
3. Atténuation et reprise
    a. Effectuer des analyses judiciaires
    b. Atténuation (par le confinement et l'éradication)
    c. Rétablir les activités normales
4. Activité après l'événement
    a. Effectuer une analyse après l'événement
    b. Tirer des leçons
    c. Amélioration continue

Au-dessus des phases 2 à 4 se trouve une boîte qui contient les mots « Établissement de rapports et communication ». Cela indique que l'établissement de rapports est une activité continue tout au long de ces phases. Cette case comporte des flèches pointant vers une boîte qui contient les mots « Connaissance situationnelle dans l'ensemble du GC » pour représenter le concept central de la connaissance continue de la situation à l'échelle du GC à chaque point du cycle de vie de gestion des événements.

La première phase, Préparation, se compose des activités générales de préparation permettant au GC (Gouvernement du Canada) de faire face à un large éventail de cyberévénements. C'est à ce stade-ci que les rôles et responsabilités en la matière sont établis, que les plans et procédures sont consignés (ou revus à la lumière des leçons apprises) et mis à exécution, et que le personnel reçoit de la formation. L'une des principales activités de cette phase consiste à mettre en place des mesures de protection et de prévention au niveau de l'hôte, de l'application et du réseau. Les mesures de protection comprennent aussi la mise en œuvre des processus de gestion des vulnérabilités et des rustines ainsi que d'autres processus.

La deuxième phase, Détection et évaluation, consiste à détecter les événements de cybersécurité potentiels, y compris les incidents de cybersécurité confirmés, par le contrôle des diverses sources d'information (ce qui comprend les solutions logicielles et le matériel des ministères et du reste du GC (Gouvernement du Canada)) et par l'établissement de rapports par les ministères et organismes concernés. Cette phase comporte aussi l'évaluation initiale du niveau d'incidence de l'événement qui influe dans la détermination de l'intervention à apporter appropriée du GC (Gouvernement du Canada).

La troisième phase, Atténuation et reprise, se compose de toutes les interventions requises pour réduire au minimum l'incidence de l'événement sur la confidentialité, la disponibilité et l'intégrité des programmes et services, et pour conduire à la reprise des activités normales. Le confinement et l'éradication jouent ici un rôle clé et consistent, entre autres choses, à éteindre les systèmes, à débrancher les systèmes des réseaux, à désactiver les fonctionnalités et à atténuer les vulnérabilités par l'installation de rustines. Les mesures de reprise peuvent consister notamment à mettre en application le PCA ou le plan RS ou toute autre mesure qui permettra de réduire l'incidence sur les systèmes d'information concernés et de reprendre les activités normales. Cette phase prévoit aussi une analyse de la cause première et une enquête, qui comprennent des activités telles que la collecte de preuves, l'analyse judiciaire, la recherche et d'autres processus pouvant influer sur les mesures de reprise.

La dernière phase, Activité après l'événement, joue un rôle crucial dans l'amélioration continue du processus global de gestion des événements de cybersécurité et, à ce titre, elle permet de tirer des leçons qui seront prises en compte à la prochaine phase de préparation, bouclant ainsi le cycle de gestion de l'événement. Cette phase consiste à effectuer une analyse après l'événement, à faire la synthèse des leçons apprises et à la réviser, et à recommander des modifications à apporter aux processus ou aux procédures afin de constamment peaufiner la capacité de gestion des événements de cybersécurité du GC (Gouvernement du Canada).

À partir de la détection d'un événement jusqu'à la clôture des activités qui lui sont postérieures, l'établissement de rapports et la communication entre les divers intervenants sont constants, permettant ainsi de sensibiliser l'ensemble du gouvernement à la situation. Il faut absolument intégrer ces activités dans le cycle de gestion des événements de cybersécurité pour veiller à ce que les conseils d'atténuation et les rapports sur la situation soient promptement communiqués aussi bien aux parties non concernées qu'à celles qui le sont afin d'améliorer la conscience situationnelle et la prise de décisions.

3.2 Intervenants

Outre les ministères et organismes, qui jouent un rôle important dans l'information et la prise de mesures concernant les activités de gestion des événements de cybersécurité, plusieurs autres intervenants participent au PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada). Voici un résumé des intervenants répartis entre trois grandes catégories. Les rôles et les responsabilités de chacun d'entre eux sont détaillés à l'annexe A.

Intervenants du PGEC

1. **Principaux intervenants**
    - Secrétariat du Conseil du Trésor du Canada (SCT)
        - Bureau du dirigeant principal de l'information (BDPI)
        - Communications stratégiques et affaires ministérielles (CSAM)

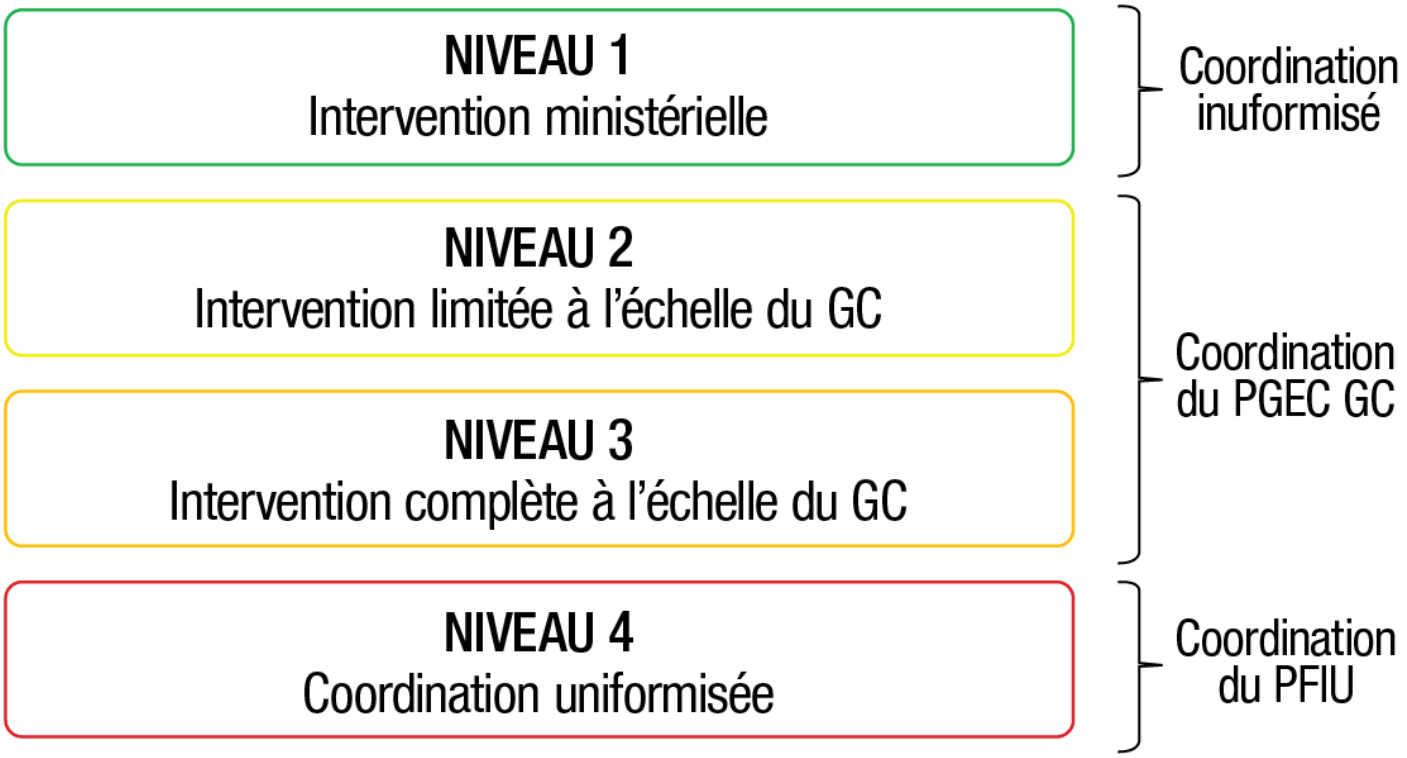
- Centre canadien pour la cybersécurité (CCC), partie intégrante du Centre de la sécurité des télécommunications (CST)
  - Gestion des incidents et coordination opérationnelle (GICO)
  - Communications (Comm.)

2. **Intervenants spécialisés**
   - Gendarmerie royale du Canada (GRC)
   - Service canadien du renseignement de sécurité (SCRS)
   - Ministère de la Défense nationale/Forces armées canadiennes (MDN-FAC)
   - Services partagés Canada (SPC)
     - Réseaux, sécurité et services numériques (RSSN)
     - Gestion de la prestation des services
     - Direction générale de la cybersécurité nationale (DGCN) de Sécurité publique Canada
3. **Autres intervenants**
   - Dirigeant principal de l'information du GC (Gouvernement du Canada) (DPI GC)
   - Centre des opérations du gouvernement (COG)
   - Bureau du Conseil privé (BCP)
     - Sécurité et renseignement (S et R)
     - Communications stratégiques (CS)
   - Comité canadien sur les systèmes nationaux de sécurité (CCSNS)
   - Comité d'intervention des directeurs généraux (CIDG)
   - Partenaires externes

3.3 Niveaux d'intervention du GC (Gouvernement du Canada)

Tel qu'il est indiqué à la figure 3, il existe quatre niveaux d'intervention qui déterminent les activités de gestion des événements de cybersécurité. Ces niveaux déterminent le niveau de coordination nécessaire à la bonne gestion de l'événement de cybersécurité, y compris le niveau hiérarchique, la participation des intervenants et l'établissement de rapports qui sont requis.

Figure 3 : Niveaux d'intervention du GC (Gouvernement du Canada)



▼ Figure 3 - Version textuelle

La figure 3 représente les quatre niveaux d'intervention du GC qui régissent les activités de gestion des événements de cybersécurité du GC et dictent la nécessité et le degré d'intervention organisationnelle requise. La figure illustre quatre boîtes superposées indiquant le niveau de coordination requis à droite des boîtes.

1. Niveau 1 – Réponse du ministère
    a. Nécessite une coordination standard
2. Niveau 2 – Réponse limitée à l'échelle du GC
    a. Nécessite la coordination du PGEC GC
3. Niveau 3 – Intervention globale à l'échelle du GC
    a. Nécessite la coordination du PGEC GC
4. Niveau 4 – Intervention en cas d'urgence (crise)
    a. Nécessite la coordination du PFIU

Le niveau 1 représente les activités quotidiennes du gouvernement. En raison du dynamisme de l'environnement des cybermenaces, et d'après la divulgation constante des nouvelles vulnérabilités de sécurité, le GC (Gouvernement du Canada) se situe, en moyenne, au niveau 1. Dans cet état, les ministères et organismes doivent coordonner leurs interventions conformément à leurs procédures ministérielles normalisées, continuer à appliquer des mesures préventives régulières et maintenir la communication avec le Groupe de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) pour obtenir des conseils et une orientation. Au niveau

du GC (Gouvernement du Canada) dans son ensemble, aucune coordination supplémentaire n'est requise entre les principaux intervenants ou les intervenants spécialisés, sinon l'échange habituel de renseignements entre eux pour se mettre au fait de la situation.

Le niveau 2 indique qu'il faut redoubler d'attention au niveau du GC (Gouvernement du Canada). L'atteinte de ce niveau déclenche le recours au palier intermédiaire de gouvernance prévu dans le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (énoncé à la section 3.4.4) et entraîne éventuellement une coordination limitée dans l'ensemble du gouvernement. À ce niveau, tous les principaux intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (et les intervenants spécialisés, au besoin), sont sur le pied d'alerte, et ils surveillent la cyberactivité par le contrôle des niveaux de risque dans l'ensemble du GC (Gouvernement du Canada) et par le confinement et l'atténuation des incidences, réelles ou éventuelles. Des conseils supplémentaires sont donnés à certains ministères ou organismes sur la façon d'intervenir, ce qui pourrait inclure le recours aux procédés de gestion des rustines d'urgence.

Le niveau 3 indique que l'ensemble du GC (Gouvernement du Canada) doit se mobiliser et être sur un pied alerte. L'atteinte de ce niveau déclenche le recours au palier supérieur de gouvernance prévu dans le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (énoncé au paragraphe 3.4.4) et entraîne éventuellement une coordination centralisée dans l'ensemble du gouvernement. À ce niveau, les interventions sont entièrement coordonnées selon la structure de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), et les ministères et organismes reçoivent des conseils et des consignes sur la façon d'intervenir, qui peut aller du recours aux procédés de gestion des rustines d'urgence jusqu'au débranchement des systèmes des réseaux du GC (Gouvernement du Canada). Les événements à ce niveau déclenchent aussi le recours au cadre des communications relatives à la cybersécurité du SCT (Secrétariat du Conseil du Trésor du Canada) [1].

Le niveau 4 est réservé aux événements graves ou catastrophiques qui concernent plusieurs ministères ou organismes publics, qui minent la confiance dans le gouvernement ou qui concernent d'autres aspects d'intérêt national. Les événements correspondant à ce niveau entraînent la mise en application immédiate du PFIU (Plan fédéral d'intervention d'urgence) et de sa structure de gouvernance, coordonnée par le COG (Centre des opérations du gouvernement) conformément au PFIU, afin d'assurer l'harmonisation des interventions.

3.3.1 Détermination des niveaux d'intervention globaux

La détermination des niveaux d'intervention globaux repose sur l'analyse de deux facteurs : l'évaluation des incidences sur les ministères et la portée de l'événement de cybersécurité en question.

Les évaluations des incidences sur les ministères se déroulent conformément au processus décrit à l'annexe B. Ce processus, valable pour tous les cyberévénements visés par le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), s'appuie sur un test de préjudice normalisé qui a pour but d'évaluer le degré de préjudice subi ou que l'on pourrait raisonnablement s'attendre à subir à la suite d'une compromission. Cette évaluation prend en compte la gravité et la portée de l'événement. Une fois évalué le degré de préjudice, on y applique un modificateur pour tenir compte de la probabilité de survenance du préjudice lorsqu'aucun incident ne s'est encore produit (p. ex., les cybermenaces latentes et les vulnérabilités non exploitées).

On cumule ensuite les résultats des évaluations des incidences sur tous les ministères concernés, puis la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), en collaboration avec le Bureau du dirigeant principal de l'information (BDPI) du SCT (Secrétariat du Conseil du Trésor du Canada) et d'autres partenaires, s'appuie sur l'annexe C pour évaluer le degré d'urgence dans l'ensemble du gouvernement et pour établir le niveau d'intervention global appropriée.

Remarque : Dans certains cas, comme dans celui de la divulgation d'une nouvelle vulnérabilité de sécurité pour laquelle le préjudice est difficile à établir, il pourrait s'avérer nécessaire de procéder à une évaluation plus approfondie des incidences sur les ministères pour pouvoir déterminer le niveau d'intervention adéquat. Dans ces cas, la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) demande aux ministères, par l'entremise d'une demande d'intervention (DI), d'effectuer une évaluation approfondie et de lui transmettre les résultats pour qu'il détermine le niveau d'intervention global adéquat.

3.4 Gouvernance

Durant un événement de cybersécurité, la mobilisation rapide des organes de gouvernance compétents fait en sorte que les responsables de la gestion et des opérations sont en mesure de prévenir ou de détecter les événements en fonction des priorités et d'assurer la reprise des activités.

La structure de gouvernance prévue par le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) comporte trois importants organes de gouvernance qui gèrent la signalisation progression d'un événement de cybersécurité, à savoir l'Équipe de coordination des événements (ECE), l'Équipe de la haute direction (EHD), et le Comité tripartite sur la sécurité de la TI (Technologies de l'information) des sous-ministres adjoints (SMA CTSTI). Lorsqu'il répond à un cyberévénement, le ministre responsable sera déterminé au cas par cas en tenant compte du contexte unique de chaque cyberévénement.

3.4.1 Équipe de coordination des événements

L'Équipe de coordination des événements (ECE) est un groupe d'intervenants de niveau opérationnel qui se mettent en action lorsque le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) l'exige (événements de niveau 2) ou lorsque l'Équipe de la haute direction (EHD) (événements de niveau 3) ou le Comité d'intervention des directeurs généraux (CIDG) (événements de niveau 4) fait appel à leurs services. L'ECE (Équipe de coordination des événements) a pour objet de collaborer avec les intervenants à la formulation de recommandations sur les mesures à prendre pour l'ensemble du gouvernement. Elle doit aussi veiller à tenir les directeurs généraux au fait de ce qui se passe en informant périodiquement les membres de l'EHD (Équipe de la haute direction) des progrès réalisés dans la gestion des événements de cybersécurité.

L'ECE (Équipe de coordination des événements) est coprésidée par le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), et la représentation des parties varie selon la nature de l'événement. À titre d'intervenant principal, l'équipe des CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada), en plus des coprésidents, participera à tous les types d'événements de cybersécurité (cybermenaces, vulnérabilités et incidents de sécurité).

Lorsqu'un incident de cybersécurité est confirmé ou lorsqu'une cybermenace entre dans le champ d'autres mandats, l'ECE (Équipe de coordination des événements) s'agrandit et fait appel aux services des intervenants spécialisés suivants, selon les besoins de la situation :

- SPC (Services partagés Canada) (Réseaux, sécurité et services numériques.);
- Sécurité publique (Direction de la cybersécurité nationale);
- la GRC (Gendarmerie royale du Canada) (Services d'enquêtes techniques et police fédérale);
- le SCRS (Service canadien du renseignement de sécurité) (Cyberactivité);
- MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes) (Gestion de l'information).

Les directement concernés par des menaces ou des incidents précis sont aussi invités à participer à l'ECE (Équipe de coordination des événements). Les invités sont choisis par les coprésidents, qui peuvent restreindre le nombre d'invités afin d'assurer le fonctionnement optimal de l'ECE.

Durant les événements de niveau 4, les coprésidents de l'ECE (Équipe de coordination des événements) veillent à ce que le COG (Centre des opérations du gouvernement) ait à sa disposition un expert technique pour donner des conseils et des consignes et tenir les parties au fait de la situation.

3.4.2 Équipe de la haute direction

L'Équipe de la haute direction (EHD) se compose de directeurs généraux qui se mettent en action lorsque l'exige le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (événements de niveau 3). Elle définit l'orientation stratégique de l'ECE (Équipe de coordination des événements) et lui donne des conseils et une orientation stratégiques, et elle présente des produits aux hauts fonctionnaires du gouvernement (comme des comptes rendus de décisions ou des projets de plans d'atténuation s'appliquant à l'ensemble du gouvernement qui requièrent l'approbation du SMA (Sous-ministre adjoint)). L'EHD (Équipe de la haute direction) doit aussi veiller à tenir les parties au niveau supérieur au courant de la situation en informant souvent les comités concernés du SMA (Sous-ministre adjoint). Durant les événements de niveau 4, l'EHD (Équipe de la haute direction) est intégrée au CIDG (Comité d'intervention des directeurs généraux) du PFIU (Plan fédéral d'intervention d'urgence).

L'EHD (Équipe de la haute direction) est coprésidée par le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), et la représentation des parties varie selon la nature de l'événement. À titre d'intervenant principal, l'équipe des CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada), en plus des coprésidents, participera à tous les types d'événements de cybersécurité (cybermenaces, vulnérabilités et incidents de sécurité). Lorsqu'un incident de cybersécurité est confirmé ou lorsqu'une cybermenace entre dans le champ d'autres mandats, l'ECE (Équipe de coordination des événements) s'agrandit et fait appel aux services des intervenants spécialisés suivants, selon les besoins de la situation :

- Centre des opérations du gouvernement (COG);
- Sécurité publique (DGCN);
- la GRC (Gendarmerie royale du Canada) (Services d'enquêtes techniques et police fédérale);
- le SCRS (Service canadien du renseignement de sécurité) (Cyberactivité);
- SPC (Services partagés Canada) (RSSN (Réseaux, sécurité et services numériques));
- MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes) (Gestion de l'information)

Les ministères directement concernés par des menaces ou des incidents précis sont aussi invités à participer à l'EHD (Équipe de la haute direction). Les invités sont choisis par les coprésidents, qui peuvent restreindre le nombre d'invités afin d'assurer le fonctionnement optimal de l'EHD (Équipe de la haute direction).

3.4.3 Comité tripartite sur la sécurité de la TI (Technologies de l'information) des SMA (Sous-ministre adjoint)

Le Comité tripartite sur la sécurité de la TI (Technologies de l'information) des SMA (Sous-ministre adjoint) (SMA CTSTI) est un comité au niveau des SMA qui sert d'organe de prise de décisions appuyant la conception, la livraison et la gestion efficaces des initiatives prioritaires de sécurité de la

TI (Technologies de l'information) touchant les systèmes internes du GC et les activités dans l'ensemble du GC (Gouvernement du Canada). Dans le cadre de la gestion des événements de cybersécurité, son activation peut être déclenchée par le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (événements de niveau 3). Le SMA (Sous-ministre adjoint) CTSTI fournit des directives et une orientation en matière d'atténuation à l'EHD (Équipe de la haute direction) en réponse à un événement de cybersécurité. Le SMA (Sous-ministre adjoint) CTSTI doit aussi veiller à tenir les parties très au courant de la situation en informant souvent les sous-ministres (SM) concernés. Pendant les événements de niveau 4, le SMA (Sous-ministre adjoint) CTSTI appuiera le Comité des sous-ministres adjoints du PFIU (Plan fédéral d'intervention d'urgence), au besoin.

Le SMA (Sous-ministre adjoint) CTSTI est présidé par le dirigeant principal de la technologie (DPT) au BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada), et ses principaux membres sont l'adjoint au dirigeant du CST (Centre de la sécurité des télécommunications) au CCC (Centre canadien pour la cybersécurité) et le SMA (Sous-ministre adjoint) à RSSN (Réseaux, sécurité et services numériques) de SPC (Services partagés Canada). La représentation des autres parties au SMA CTSTI variera selon la nature de l'événement. À titre d'intervenant principal, l'équipe des CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada), en plus des coprésidents, participera à tous les types d'événements de cybersécurité (cybermenaces, vulnérabilités et incidents de sécurité).

Lorsqu'un incident de cybersécurité est confirmé ou lorsqu'une cybermenace entre dans le champ d'autres mandats, l'ECE (Équipe de coordination des événements) s'agrandit et fait appel aux services des intervenants spécialisés suivants, selon les besoins de la situation :

- Centre des opérations du gouvernement (COG);
- Sécurité publique (Direction générale de la cybersécurité nationale).
- SPC (Services partagés Canada) (Gestion de la prestation des services);
- la GRC (Gendarmerie royale du Canada) (Services d'enquêtes techniques et police fédérale);
- MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes) (Chef du personnel, Groupe de la gestion de l'information);
- le SCRS (Service canadien du renseignement de sécurité);
- les ministères ou les organismes touchés.

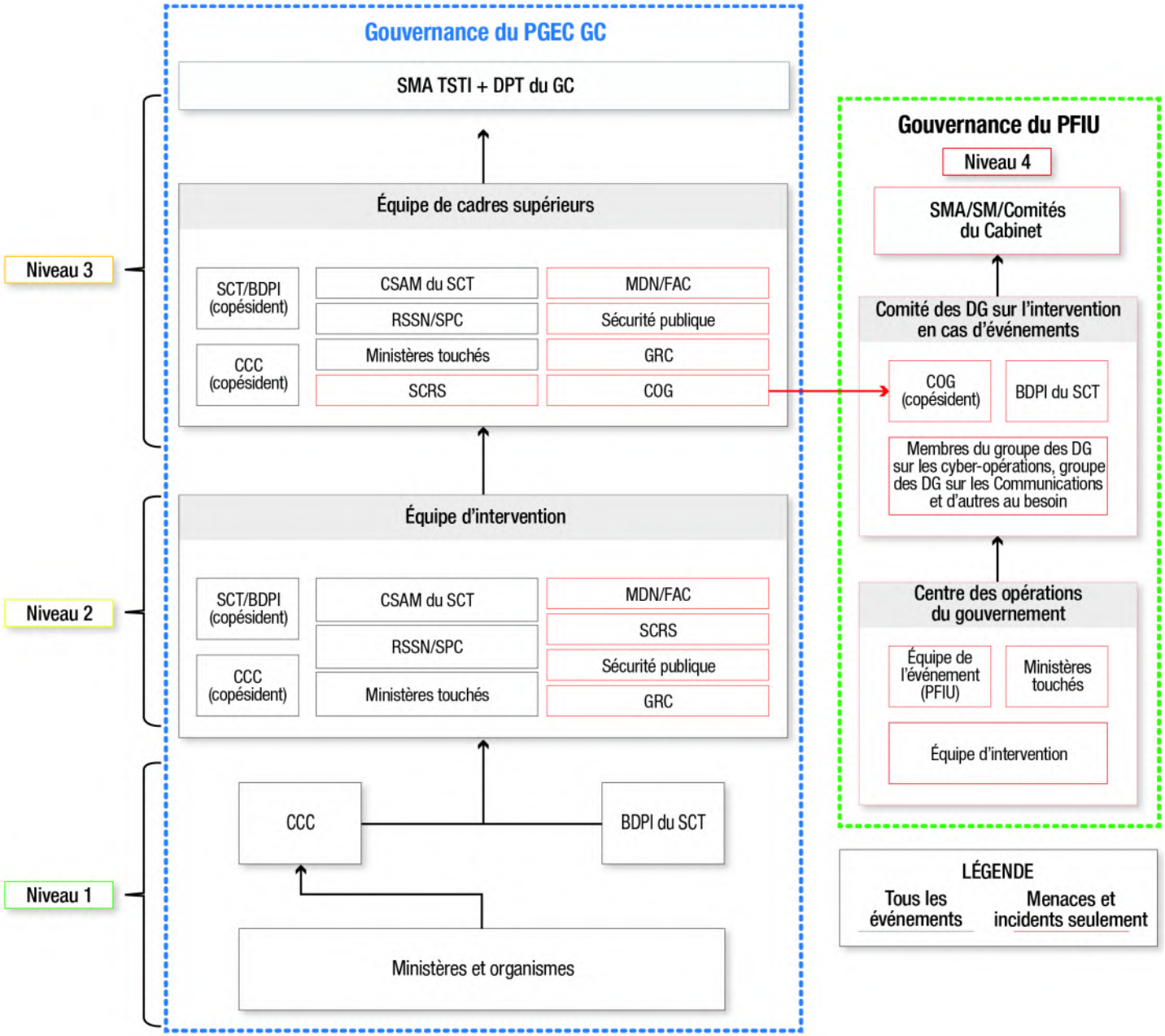
3.4.4 Modèle de signalisation progressive

Le modèle de signalisation progressive prévu dans le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), illustré à la figure 4 indique les intervenants de niveau opérationnel et les intervenants du niveau supérieur et établit une distinction entre les principaux intervenants et les intervenants spécialisés qui varie selon le type d'événements (illustrée au moyen de carrés rouges et noirs). Après l'analyse des données obtenues des organisations concernées, les intervenants demanderont aux organes de gouvernance compétents (c'est-à-dire l'ECE (Équipe de

coordination des événements), l'EHD (Équipe de la haute direction) ou les deux) d'intervenir, selon les besoins de la situation. À noter que ce modèle identifie le sous-ensemble minimum d'intervenants qui doivent intervenir dans le processus de signalisation progressive; les coprésidents de chacun des organes de gouvernance peuvent inviter d'autres organisations du GC (Gouvernement du Canada) s'il y a lieu, par exemple, l'intervenant spécialisé qui a fourni l'information.

En raison des brefs délais au cours desquelles les événements de cybersécurité peuvent provoquer des dommages importants, il est essentiel d'avoir recours rapidement à l'organe de gouvernance compétent. À ce titre, le choix initial de l'organe de gouvernance à contacter dépend du niveau d'intervention global établi pour cet événement particulier. Par exemple, dans le cas d'un événement classé dès le début de niveau 3, la gouvernance est immédiatement assurée par l'EHD (Équipe de la haute direction).

Figure 4 : Modèle de signalisation progressive prévu par le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)



▼ Figure 4 - Version textuelle

La figure 4 représente le modèle d'escalation du PGEC GC. Cette figure indique la gouvernance requise en fonction du niveau d'intervention indiqué à la figure 3. La figure 4 indique le niveau de travail et les intervenants de la haute direction requis, en différenciant les membres principaux et les membres spécialisés, lesquels varient selon le type d'événement. Les voici :

1. Niveau 1 – Réponse du ministère
    a. Ce niveau relève de la gouvernance du PGEC GC.
    b. Les ministères et organismes fournissent des renseignements au CCC pour tous les événements.
    c. Le CCC transmettra ensuite cette information au BDPI du SCT.
2. Niveau 2 – Réponse limitée à l'échelle du GC
    a. Ce niveau relève de la gouvernance du PGEC GC.

b. Un événement de ce niveau fait appel à l'Équipe de coordination des événements (invoquée par le CCC ou le BDPI du SCT). Cette équipe comprend les intervenants opérationnels suivants :
    i. BDPI du SCT (coprésident)
    ii. CCC (coprésident)
    iii. Sécurité publique (Direction de la cybersécurité nationale)
    iv. CSAM du SCT (communications du SCT)
c. Dans les scénarios où une menace ou un incident a été identifié, les membres suivants se joindront à l'Équipe de gestion des événements de cybersécurité :
    i. GRC
    ii. MDN-FAC
    iii. SCRS
    iv. le(s) ministère(s) touché(s)

3. Niveau 3 – Intervention globale à l'échelle du GC
    a. Ce niveau relève de la gouvernance du PGEC GC./li>
    b. Un événement de ce niveau fait appel à l'Équipe de la haute direction, qui se compose des membres suivants du niveau de la DG :
        i. BDPI du SCT (coprésident)
        ii. CCC (coprésident)
        iii. Sécurité publique
        iv. CSAM du SCT (communications du SCT)
    c. Dans les scénarios où une menace ou un incident a été identifié, les membres suivants se joindront à l'Équipe de gestion des événements de la haute direction :
        i. GRC
        ii. MDN-FAC
        iii. COG (qui agit à titre d'agent de liaison entre l'Équipe de gestion des événements de la haute direction et la structure de gouvernance du PFIU si l'incident nécessite un recours hiérarchique supplémentaire)
        iv. SCRS
        v. le(s) ministère(s) touché(s)
    d. Au niveau 3, le DPI du GC et d'autres comités au niveau des SMA (qui sont intentionnellement flexibles étant donné que l'engagement variera selon le type d'événement) sont désignés comme des intervenants et recevront de l'information de l'Équipe de gestion des événements de la haute direction
4. Niveau 4 – Intervention en cas d'urgence (crise)
    a. Ce niveau relève de la gouvernance du PFIU.
    b. Ce niveau est actif en cas de menaces et d'incidents seulement.

c. Il y a trois organismes de gouvernance désignés à ce niveau, qui informent à partir de la base dans l'ordre suivant :
    i. Centre des opérations du Gouvernement (niveau opérationnel)
        1. Équipe de gestion des événements de cybersécurité
        2. Équipe de l'événement (PFIU)
        3. Ministères concernés
    ii. Comité d'intervention en cas d'incident des DG (niveau des DG)
        1. COG (coprésidence)
        2. BDPI du SCT (coprésident)
        3. Membres du groupe des DG sur les cyberopérations, groupe des DG sur les communications et d'autres au besoin
    iii. SMA, SM, comités du Cabinet

Voici quelques remarques à propos du modèle de signalisation progressive :

- **Quel que soit** le type d'événements :
    - les intervenants des niveaux inférieurs du modèle sont mobilisés (ou demeurent actifs, s'ils participent déjà) lorsque les niveaux supérieurs sont mobilisés durant un événement;
    - les intervenants des niveaux supérieurs du modèle, même s'ils ne sont pas formellement mobilisés, sont constamment informés de la situation tout au long du cycle de vie de l'événement.
- En ce qui concerne les événements de **niveau 2** :
    - le recours à l'ECE (Équipe de coordination des événements) signifie que les intervenants concernés sont simplement en communication entre eux et que les membres ne sont pas forcément tenus de se réunir en personne;
    - l'ECE (Équipe de coordination des événements) s'en remet à l'autorité supérieure s'il faut accentuer les mesures d'atténuation, si l'incidence de l'événement est plus grande qu'anticipée ou que les circonstances nécessitent une intervention du GC (Gouvernement du Canada).
- En ce qui concerne les événements de **niveau 3** :
    - le recours à l'EHD (Équipe de la haute direction) signifie que les intervenants concernés se réunissent formellement en personne;
    - la décision de s'en remettre à l'autorité supérieure et de passer au mode de coordination prévu dans le PFIU (Plan fédéral d'intervention d'urgence) est prise par le COG (Centre des opérations du gouvernement) DG (Directeur général), en consultation avec l'EHD (Équipe de la haute direction).
- En ce qui concerne les événements de **niveau 4** :
    - les intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) restent mobilisés auprès des équipes de gestion des

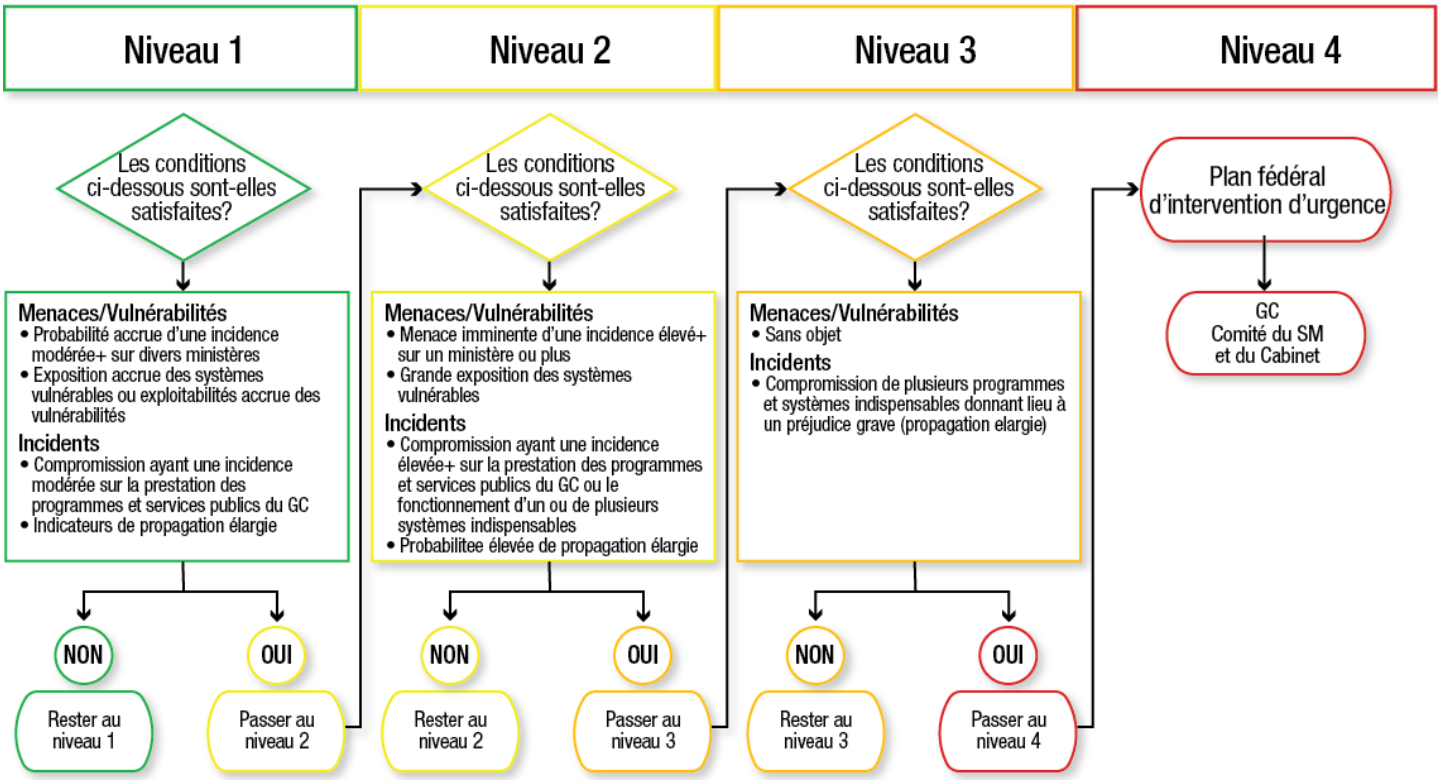
événements du PFIU (Plan fédéral d'intervention d'urgence) et continuent d'accomplir leurs mandats respectifs au sein du gouvernement, conformément à l'orientation donnée par les organes de gouvernance du PFIU (Plan fédéral d'intervention d'urgence);
- les mécanismes en place d'échange de renseignements sont utilisés autant que possible pour des raisons d'efficacité.

3.4.5 Signalisation progressive et niveaux d'intervention

Les intervenants doivent aussi savoir que le niveau d'intervention global du GC (Gouvernement du Canada) peut changer pendant le déroulement d'un événement, si certains critères sont remplis. La figure 5 illustre les éléments qui peuvent être utilisés durant un événement afin de faire intervenir les bons intervenants au moment opportun. La décision du passage d'un niveau à l'autre est prise conjointement par les intervenants concernés, en se fondant sur le préjudice subi (ou potentiellement subi) par le GC (Gouvernement du Canada) comme élément déclencheur (le préjudice se fonde sur les résultats du test de préjudice exposé à l'annexe B). D'autres facteurs de signalisation progressive peuvent entrer en ligne de compte, selon les circonstances de l'événement en question.

Selon la nature de l'événement, le test de préjudice peut être réévalué afin de pouvoir établir avec précision quel palier d'autorité doit intervenir. Dans le cas des cybermenaces ou des vulnérabilités, la signalisation progressive est enclenchée lorsque le risque de préjudice augmente (p. ex., probabilité accrue d'occurrence, utilisation ou exposition accrue de systèmes vulnérables, diminution de l'efficacité des contrôles de sécurité). Dans le cas d'incidents confirmés, la signalisation progressive est enclenchée lorsqu'il y a aggravation du préjudice ou que son étendue augmente.

Figure 5 : Signalisation progressive et niveaux d'intervention



▼ Figure 5 - Version textuelle

La figure 5 présente les intervenants pertinents et les éléments déclencheurs connexes de recours hiérarchique pour les divers niveaux d'intervention du gouvernement définis à la figure 2 au moyen de cercles concentriques et d'un tableau ci-joint. Voici les éléments déclencheurs pour l'acheminement à l'ordre hiérarchique pertinent :

1. Niveau 1 – Réponse du ministère
    a. Intervenants
        i. Activités quotidiennes :
            1. Des ministères et organismes
            2. CCC
    b. Éléments déclencheurs de recours à un niveau hiérarchique supérieur
        i. Menaces et vulnérabilités
            1. Probabilité accrue de répercussions de gravité moyenne ou plus élevée pour de nombreux ministères
            2. Exposition accrue des systèmes vulnérables ou exploitabilité accrue des vulnérabilités
        ii. Incidents
            1. Compromission à incidence moyenne ayant une incidence sur la prestation d'un ou de plusieurs programmes et services du GC destinés au public
            2. Indicateurs de propagation
2. Niveau 2 – Réponse limitée à l'échelle du GC
    a. Intervenants

        i. Équipe de coordination des événements
    b. Éléments déclencheurs de recours à un niveau hiérarchique supérieur
        i. Menaces et vulnérabilités
            1. Menace imminente de répercussions importantes ou plus pour un ou plusieurs ministères
            2. Exposition élevée des systèmes vulnérables
        ii. Incidents
            1. Incidence élevée ou supérieure d'une compromission ayant une incidence sur la prestation d'un programme ou de services du GC destinés au public ou sur l'exploitation d'un ou de plusieurs systèmes essentiels à la mission
            2. Probabilité élevée de propagation
3. Niveau 3 – Intervention globale à l'échelle du GC
    a. Intervenants
        i. Équipe de la haute direction
        ii. Comités des SMA (au besoin)
        iii. DPI du GC
    b. Éléments déclencheurs de recours à un niveau hiérarchique supérieur
        i. Menaces et vulnérabilités
            1. S. O.
        ii. Incidents
            1. Compromission ayant une incidence sur la prestation de nombreux programmes et services essentiels à la mission et entraînant des blessures graves (propagation généralisée)
4. Niveau 4 – Intervention en cas d'urgence (crise)
    a. Intervenants
        i. Plan fédéral d'intervention d'urgence
            1. COG
            2. Comités du SM et du Cabinet
    b. Éléments déclencheurs de recours à un niveau hiérarchique supérieur
        i. S. O.

3.4.6 Désescalade

Le niveau d'intervention global peut changer pendant le déroulement d'un événement, en fonction de l'efficacité des mesures d'atténuation, si l'on détermine qu'un incident est moins grave qu'on ne le pensait, si la menace est réduite ou si la vulnérabilité des systèmes du gouvernement est jugée comme amoindrie. La décision de désescalade d'un niveau à un autre est prise par les coprésidents du Comité, en consultation avec les intervenants concernés, en se fondant sur le préjudice subi par

le GC (Gouvernement du Canada) comme élément déclencheur (le préjudice se fonde sur les résultats du test de préjudice exposé à l'annexe B). D'autres facteurs de désescalade peuvent entrer en ligne de compte, selon les circonstances de l'événement en question.

Selon la nature de l'événement, le test de préjudice peut être réévalué afin de pouvoir établir avec précision le niveau d'intervention nécessaire. Dans le cas des cybermenaces ou des vulnérabilités, la désescalade est enclenchée lorsque le risque de préjudice baisse (p. ex., faible probabilité d'occurrence, faible utilisation ou exposition de systèmes vulnérables, efficacité accrue des mesures de sécurité). Dans le cas d'incidents de cybersécurité confirmés, la désescalade sera enclenchée lorsqu'il y a diminution de la gravité du préjudice ou que son étendue diminue.

4.0 Concept des opérations

▼ **Titres de la section**

Les paragraphes qui suivent donnent une vue d'ensemble des attentes pour chaque phase du cycle de gestion des événements de cybersécurité. Elles décrivent la mise en application du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) et les principaux éléments d'entrée et de sortie de chaque phase.

Tous les intervenants doivent élaborer leurs propres procédures normalisées d'exploitation ou leurs propres processus internes menant à l'obtention des produits attendus.

4.1 Préparation

▼ Figure Préparation - Version textuelle

Il s’agit d’une reproduction de la figure 2, avec une flèche en gris indiquant la phase de Préparation. La flèche de Préparation est surlignée en bleu et cette image est une représentation visuelle de la phase décrite pour le lecteur dans cette section.

La phase Préparation est une phase permanente au cours de laquelle le gouvernement exécute une série de processus continus afin de se préparer à des événements précis ou inattendus; ce qui nécessite la tenue à jour, l’amélioration et la création de mécanismes qui permettent de définir les priorités, d’intégrer plusieurs organisations et plusieurs fonctions, et de veiller à ce que des moyens efficaces soient disponibles pour répondre à l’ensemble des exigences qu’entraîne la gestion des événements de cybersécurité. Cette phase englobe aussi la mise en application anticipée de mesures de protection et de prévention avant un cyberévénement.

Au cours de cette phase :

- **tous les intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (y compris les ministères et organismes)** mettent en œuvre les mesures de protection et de prévention dans leurs secteurs de responsabilité respectifs, conformément aux conseils et aux consignes des principaux organismes chargés de la sécurité (POCS);
- le **SCT (Secrétariat du Conseil du Trésor du Canada)** élabore et tient à jour le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), coordonne des exercices réguliers auxquels participent tous les intervenants concernés et veille à la mise en application des leçons apprises;
- le **SCT (Secrétariat du Conseil du Trésor du Canada)** examine les rapports portant sur les analyses prospectives et les leçons tirées d’événements passés et, au besoin, préconise des changements dans la politique de sécurité ou dans les architectures de référence relatives à la sécurité organisationnelle;
- la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** tient à jour des listes de diffusion opérationnelles qui s’étendent à l’ensemble du gouvernement, et veille à ce que les ministères et organismes reçoivent continuellement les conseils et les consignes dont ils ont besoin pour atténuer les cybermenaces et les vulnérabilités afin de prévenir l’occurrence d’incidents de cybersécurité;
- les **ministères et organismes, y compris les fournisseurs de services comme SPC (Services partagés Canada)**, harmonisent leurs plans, leurs processus et leurs procédures sur le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), participent aux exercices au besoin et veillent à la mise en application en interne des leçons apprises;
- les **ministères et les organismes, y compris les fournisseurs de services comme SPC (Services partagés Canada)**, tiendront constamment à jour une liste de leurs systèmes d’information qui sont essentiels à la réalisation de la mission.

Voici les éléments d'entrée et de sortie de cette phase :

- **Éléments d'entrée**
  - Leçons tirées d'événements passés, stratégies d'atténuation, exercices, scénarios de tests.
  - Recommandations périodiques des POCS (Principal organisme responsable de la sécurité).
  - Pratiques exemplaires dans l'industrie.
- **Extrants**
  - Mise en pratique des leçons apprises.
  - Révision des plans, processus, directives et outils de gestion des événements de cybersécurité dans l'ensemble du GC (Gouvernement du Canada).
  - Exercices, scénarios et tests afin de valider l'efficacité du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada).
  - Révision des plans, des processus et des procédures des ministères, afin qu'ils concordent avec le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada).
  - Connaissance des systèmes de l'ensemble du GC (Gouvernement du Canada) qui sont jugés essentiels.

4.2 Détection et évaluation

▼ Figure Détection et évaluation - Version textuelle

Il s'agit d'une reproduction de la figure 2, avec toutes les flèches en gris, sauf celle qui représente la phase de Détection et d'évaluation. La flèche Détection et évaluation est surlignée en bleu et cette image est une représentation visuelle de la phase décrite pour le lecteur dans cette section.

La phase Détection et évaluation consiste en un contrôle continu des sources d'information afin de repérer les signes avant-coureurs des événements de cybersécurité et d'évaluer leurs incidences, réelles ou éventuelles, sur la qualité des services offerts aux Canadiens, sur le fonctionnement du gouvernement ou sur la confiance que l'on a envers le gouvernement.

Le volet détection de cette phase reste le même quel que soit le type d'événement de cybersécurité (menace, vulnérabilité ou incident de sécurité), et il comprend aussi la notification des parties concernées. La détection étant un produit direct de l'activité de contrôle, si la composante de contrôle est inadéquate ou incomplète, le processus de détection peut passer à côté d'anomalies ou d'événements qui pourraient nuire au GC (Gouvernement du Canada).

En ce qui concerne le volet détection de cette phase :

- **Les principaux intervenants et les intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)** contrôlent leurs sources d'information respectives afin de détecter des signes précurseurs de cybermenaces ou de vulnérabilité ou des indicateurs d'incidents de cybersécurité confirmés ou éventuels, et ils **informent immédiatement la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** de toute activité malveillante pouvant compromettre l'intégrité des systèmes d'information du GC (Gouvernement du Canada). Plus particulièrement :
  - La GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) surveillera :
    - les sources techniques, ainsi que les renseignements déclarés par d'autres intervenants;
    - le périmètre du GC (Gouvernement du Canada) et tous les points d'extrémité dont ils ont une visibilité;
    - les environnements d'informatique en nuage gérés par le ministère, y compris les points d'extrémité ou les services relevant de leur compétence;
    - les réseaux du gouvernement et les sources de renseignements;
    - les renseignements provenant de sources nationales ou internationales.
  - la **GRC (Gendarmerie royale du Canada)** contrôle l'information provenant de sources de surveillance de la criminalité;
  - le **SCRS (Service canadien du renseignement de sécurité)** contrôle l'information provenant de sources de renseignement;
  - le **MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes)** contrôlent tous les réseaux du MND, de même que les réseaux des sources alliées (comme l'OTAN), déployés dans le cadre des activités.
- **Les principaux intervenants et les intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)**, lorsqu'ils détectent un événement de cybersécurité, déclarent l'événement aux organismes concernés conformément au paragraphe 5.1 du Plan.
- **Les ministères et les organismes, y compris les fournisseurs de services comme SPC (Services partagés Canada)**, mettent en œuvre les mesures générales de sécurité établies en vertu de la *Politique sur la sécurité du gouvernement* sur l'infrastructure informatique dont ils

sont responsables, et ils informent la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) lorsqu'ils détectent un événement de cybersécurité, conformément aux exigences d'information énoncées au paragraphe 5.2 du Plan.
- **Les ministères et organismes, y compris les fournisseurs de services comme SPC (Services partagés Canada)**, informent les autorités compétentes en matière d'application de la loi ou de sécurité nationale lorsqu'ils reçoivent de l'information indiquant qu'un événement relève de ces domaines particuliers, et ce, conformément au paragraphe 5.2.3 du Plan.

Le volet évaluation de cette phase s'enclenche dès la réception d'une information indiquant l'existence, réelle ou éventuelle, d'un événement de cybersécurité. Cette phase a pour but d'établir le niveau d'intervention global et de déterminer s'il faut recourir aux organes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) ou du PFIU (Plan fédéral d'intervention d'urgence).

En ce qui concerne le volet évaluation de cette phase :

- **La GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** établit le niveau initial d'intervention global, en consultation avec le BDPI (Bureau du dirigeant principal de l'information) du SCT et d'autres partenaires, en se fondant sur une compilation de l'information produite par les ministères, et elle a recours aux organes de gouvernance compétents prévus par le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) pour le niveau d'intervention établi.
    - **Lorsqu'il faut plus de renseignements pour pouvoir apprécier le niveau de risque dans l'ensemble du gouvernement :**
        - la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** tirera parti, dans la mesure du possible, des outils automatisés pour recueillir les renseignements nécessaires à l'appui d'une évaluation d'incidence;
        - la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** envoie une DI (Demande d'intervention) aux ministères et organismes, en consultation et en accord avec le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada), afin qu'ils procèdent à une évaluation de l'incidence interne;
        - les **ministères et organismes** effectuent une évaluation de l'incidence interne et envoient les résultats à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) dans le délai imparti.

Voici les éléments d'entrée et de sortie de cette phase :

- **Éléments d'entrée**

- Rapports de menaces et de renseignements obtenus des intervenants de la gestion des événements du GC (Gouvernement du Canada) ou de sources externes (fournisseurs, code source libre, entre autres).
- Rapports d'incidents obtenus des intervenants de la gestion des événements du GC (Gouvernement du Canada), des ministères ou de sources externes.

- **Extrants**
  - Rapports d'évaluation de l'incidence sur les ministères et sur le gouvernement dans son ensemble.
  - Établissement d'un niveau d'intervention global.
  - Recensement des événements qui nécessitent une intervention coordonnée dans l'ensemble du gouvernement.
  - Recours aux organes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) ou du PFIU (Plan fédéral d'intervention d'urgence), s'il y a lieu.

4.3 Atténuation et reprise

▼ Figure Atténuation et reprise - Version textuelle

Il s'agit d'une reproduction de la figure 2, avec toutes les flèches en gris, sauf celle qui représente la phase d'Atténuation et de reprise. La flèche Atténuation et reprise est surlignée en bleu et cette image est une représentation visuelle de la phase décrite pour le lecteur dans cette section.

La phase Atténuation et reprise a pour but d'atténuer les menaces et les vulnérabilités avant qu'elles ne provoquent d'incident, ou de circonscrire et d'atténuer les effets des incidents survenus. Si les activités de cette phase varient en fonction de la nature de l'événement, elles pourraient comprendre, entre autres choses, l'installation de rustines, la mise en place de mesures préventives, le confinement et l'éradication d'un incident confirmé (qui peuvent comporter une analyse judiciaire), le recours au plan de continuité des activités et au plan de reprise après sinistre

(RS) ou encore l'interruption temporaire des services vulnérables. Quel que soit le type d'événement, le but ultime de cette phase est de réduire au minimum les incidences et d'assurer la reprise rapide des activités normales.

Au cours de cette phase, pour tous les événements concernés (à noter que le degré de participation varie en fonction du niveau d'intervention global établi) :

- le **BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada)** assure la coordination stratégique, ce qui peut comprendre l'envoi de conseils stratégiques aux ministères et organismes afin de réduire au minimum l'incidence des événements de cybersécurité sur l'ensemble du gouvernement (p. ex., mise hors service des systèmes d'information vulnérables accessibles au grand public, le recours aux plans RS) (dans le cas des événements de niveau 3 ou lorsque des événements de niveau 2 le nécessitent);
- le **COG (Centre des opérations du gouvernement)** assure la coordination stratégique, ce qui peut comprendre l'envoi (par l'intermédiaire du BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada)) de conseils stratégiques aux ministères et organismes qui préconisent l'adoption de mesures permettant de réduire au minimum l'incidence des événements de cybersécurité sur l'ensemble du gouvernement (dans le cas uniquement des événements de niveau 4);
- la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**, à titre de fournisseur de services de défense, assure la coordination opérationnelle, ce qui comprend l'envoi de conseils techniques et d'avis aux ministères et organismes qui préconisent l'adoption de mesures permettant d'atténuer ou de circonscrire l'incidence sur les systèmes des ministères (p. ex., installation de rustines, blocage des adresses IP) et le suivi de ces mesures et l'établissement de rapports connexes (tous les événements);
- **tous les principaux intervenants et les intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)** prodiguent conseils et avis à la lumière des informations obtenues de leurs sources respectives;
- les **ministères et les organismes, y compris les fournisseurs de services comme SPC (Services partagés Canada)**, mettent en œuvre l'orientation fournie par la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) et du BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) dans les délais établis (sur les appareils et l'infrastructure dont ils sont responsables). Les fournisseurs de services, comme SPC (Services partagés Canada), établissent des liens avec leurs ministères clients pour coordonner l'application de correctifs sur l'infrastructure (tous les événements).

De plus, dans le cas d'incidents confirmés (tous les événements de niveau 3+ et certains événements de niveau 2) :

- La GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) :
  - dirige l'élaboration d'un plan de confinement dans l'ensemble du gouvernement, en collaboration avec les intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada);
  - tire parti de ses capacités de collecte pour faciliter une intervention ciblée;
  - aider à mettre en œuvre le plan de prévention ou de confinement dans leurs domaines de compétence respectifs;
  - en collaboration avec les ministères et organismes et les POCS (Principal organisme responsable de la sécurité) concernés, dirige l'investigation et l'analyse judiciaires (y compris la collecte des preuves) des systèmes informatiques dont elle a la charge.
- **les fournisseurs de services concernés et les ministères et organismes concernés** aident à la mise en œuvre du plan de prévention ou de confinement dans leurs secteurs de responsabilité respectifs;
- l'équipe des **RSSN (Réseaux, sécurité et services numériques) de SPC (Services partagés Canada)** aidera à identifier et à rendre compte des systèmes touchés ou vulnérables afin de faciliter une approche ciblée des activités d'atténuation, en collaboration avec les ministères et organismes.

Voici les éléments d'entrée et de sortie de cette phase :

- **Éléments d'entrée**
  - Rapports d'incidents et de situation
  - Renseignements de sécurité
  - Résultats de l'analyse judiciaire
  - Autres éléments (politiques, légaux, etc.)
  - Rapports d'évaluations des incidences
  - PCA et plan de RS
- **Extrants**
  - Plan d'intervention
  - Atténuation de la menace ou de la vulnérabilité (s'il y a lieu)
  - Confinement et éradication de l'incident (s'il y a lieu)
  - Reprise des activités normales
  - Confirmation de la fin de la menace, de la vulnérabilité ou de la menace.

4.4 Activité après l'événement

▼ Figure Activité après l'événement - Version textuelle

Il s'agit d'une reproduction de la figure 2, avec toutes les flèches en gris, sauf celle qui représente la phase d'Activité après l'événement et rétroaction. Les flèches d'Activité après l'événement et de rétroaction sont surlignées en bleu et cette image est une représentation visuelle de la phase décrite pour le lecteur dans cette section.

La phase Activité après l'événement consiste à tirer parti des leçons tirées de chaque événement de cybersécurité afin d'améliorer continuellement le processus de gestion des événements et, par extension, le niveau de sécurité de l'infrastructure du GC (Gouvernement du Canada) dans son ensemble. Cette phase a pour but de clore officiellement la gestion de l'événement de cybersécurité en procédant à une analyse après l'événement, en recensant les leçons apprises (le cas échéant) et en préconisant des changements dans la politique de sécurité ou des améliorations dans l'architecture de sécurité, selon les besoins.

L'importance des efforts et des ressources à consacrer à cette phase varie d'un événement à l'autre. Les événements graves, y compris les incidents confirmés, nécessitent une analyse plus approfondie que ceux d'une gravité moindre. Les événements répétitifs peuvent faire l'objet d'une analyse d'ensemble.

Durant cette phase, pour tous les événements concernés (ou sur demande) :

- les **ministères et organismes concernés** établissent leur propre rapport des leçons apprises et leur propre plan d'action et, au besoin, participent aux activités après événement qui se déroulent dans l'ensemble du GC (Gouvernement du Canada);
- la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** recueille les résultats des ministères et établit un rapport, ce qui comprend la chronologie des événements et une analyse de la cause première;
- le **BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada)** établit un rapport des leçons apprises, de même qu'un plan d'action pour le compte du GC (Gouvernement du Canada) et elle contrôle la mise en œuvre des recommandations (dans le cas des événements de niveau 3 ou lorsque les événements de niveau 2 le justifient);

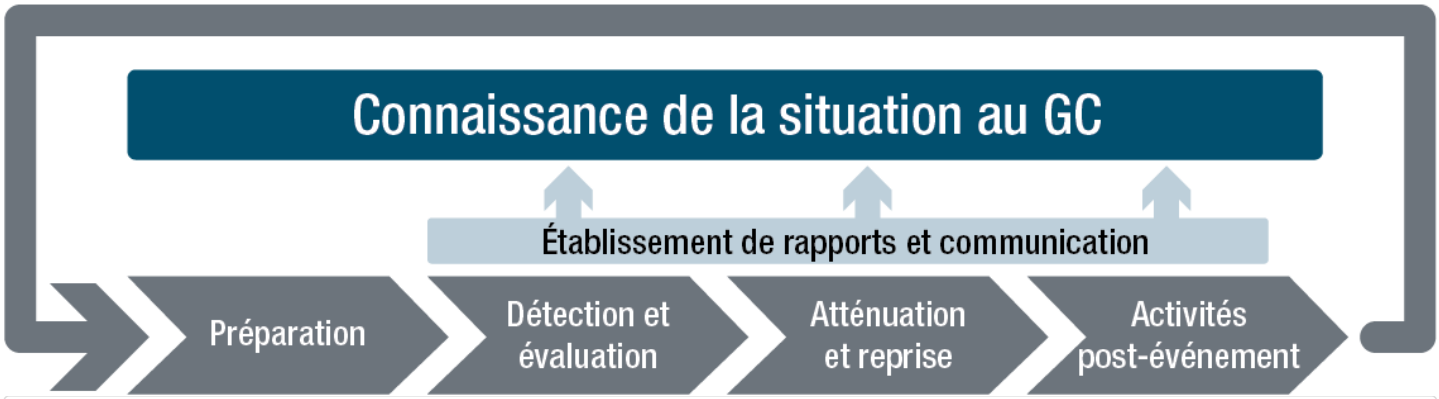
- le **COG (Centre des opérations du gouvernement)** établit un rapport des leçons apprises, assure la coordination de la production des plans d'action des ministères et contrôle la mise en œuvre des recommandations (dans le cas uniquement des événements de niveau 4);
- **tous les autres intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)** produisent l'information nécessaire à l'établissement de rapports sur les leçons apprises dans l'ensemble du GC (Gouvernement du Canada), et ils participent à la mise en œuvre des mesures à prendre dans leur secteur de responsabilité.tous les autres intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) produisent l'information nécessaire à l'établissement de rapports sur les leçons apprises dans l'ensemble du GC (Gouvernement du Canada), et ils participent à la mise en œuvre des mesures à prendre dans leur secteur de responsabilité.

Voici les éléments d'entrée et de sortie de cette phase :

- **Éléments d'entrée**
  - Examen de la chronologie des événements.
  - Examen des procédures d'établissement de rapports et de communication, et de la possibilité qu'offrent les produits.
  - Analyse de la cause première.
  - Autres éléments importants obtenus des intervenants concernés du PGEC (Plan de gestion des événements de cybersécurité).
- **Extrants**
  - Rapport des leçons apprises produit par les ministères.
  - Rapports du GC (Gouvernement du Canada) donnant suite à un événement.
  - Leçons apprises et plan d'action pour l'ensemble du GC (Gouvernement du Canada) (s'il y a lieu).
  - Recommandations visant à améliorer des instruments de politique ou l'architecture de sécurité de l'organisation.

5.0 Établissement de rapports et communication

▼ **Titres de la section**



▼ Figure Établissement de rapports et communication - Version textuelle

Il s'agit d'une reproduction de la figure 2, avec toutes les flèches en gris, sauf celle qui représente la boîte « Connaissance situationnelle dans l'ensemble du GC » et « Établissement de rapports et communication ». Les boîtes « Connaissance situationnelle dans l'ensemble du GC » et « Établissement de rapports et communication » sont surlignées en bleu et cette image est une représentation visuelle de la phase décrite pour le lecteur dans cette section.

Une fois l'événement de cybersécurité détecté, il faut en informer certains intervenants du GC (Gouvernement du Canada). Il peut s'agir d'acteurs œuvrant au sein même de la structure de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) ou bien à l'extérieur de cette structure, mais au sein du gouvernement du Canada (ce qui comprend les communications entre ministères ou avec les employés), ou d'interlocuteurs de l'extérieur du gouvernement du Canada, notamment les médias et le grand public. L'établissement de rapports et la communication continue (que ce soit sur une base périodique ou ponctuelle) jouent un rôle crucial dans le processus de gestion des événements de cybersécurité, car elles permettent de tenir au fait de la situation les intervenants concernés pour qu'ils prennent des décisions en toute connaissance de cause et qu'ils soient au courant des incidences possibles sur les programmes et services du GC (Gouvernement du Canada).

Sont décrits ci-après les produits liés à l'établissement de rapports et à la communication à diffuser pendant le cycle de gestion des événements du GC (Gouvernement du Canada), et les obligations particulières en matière d'établissement de rapports par les ministères et les organismes.

5.1 Établissement de rapports et communication dans l'ensemble du gouvernement

L'établissement de rapports et la communication dans l'ensemble du gouvernement s'effectuent comme suit :

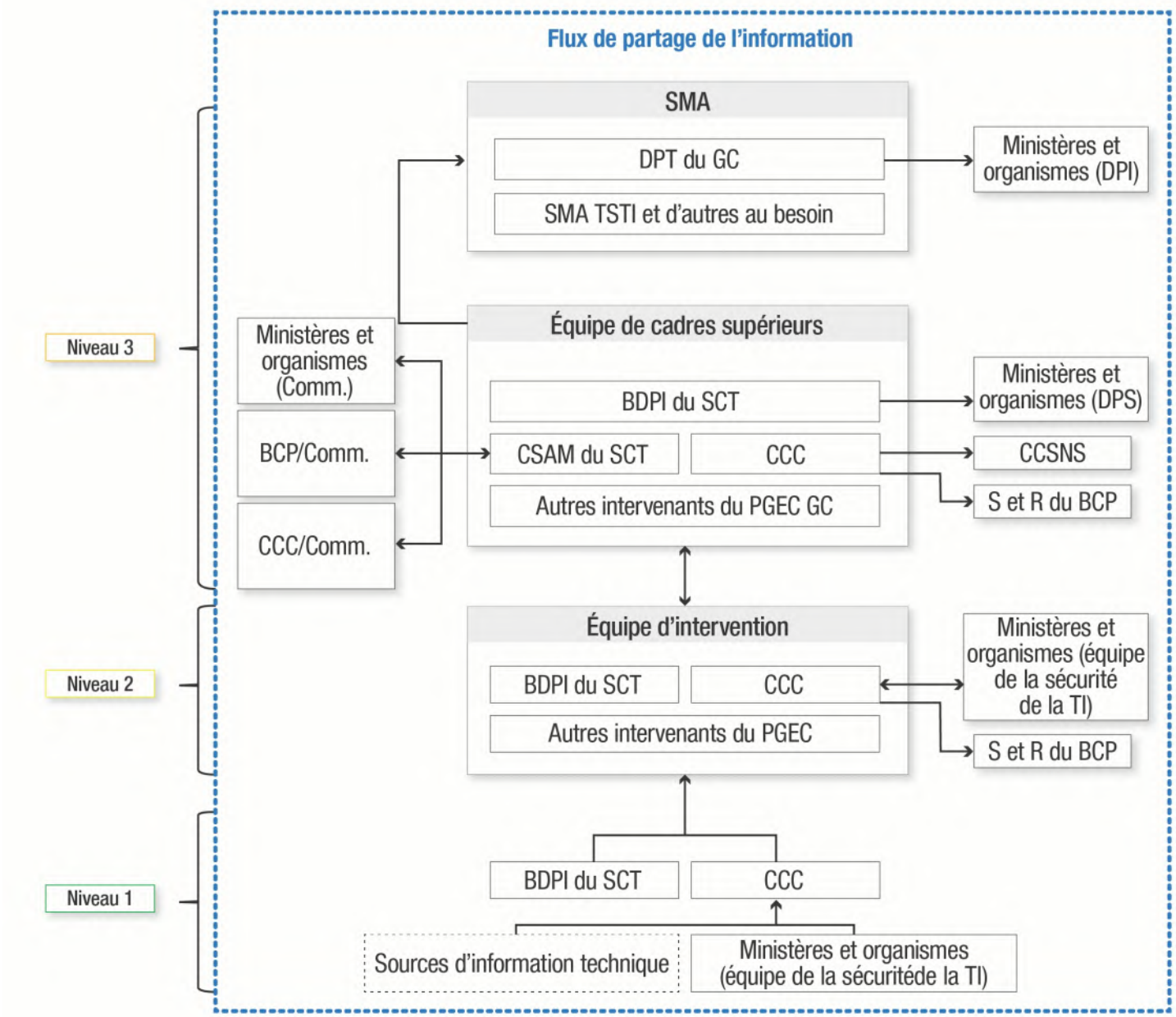
- la division **CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada)** coordonne la préparation de la stratégie de communication, et il prépare et publie les documents de communication externe (conformément au cadre des communications relatives à la cybersécurité du SCT (Secrétariat du Conseil du Trésor du Canada) [1]) qui sont requis durant le cycle de gestion des événements de cybersécurité, en collaboration avec les Comm. (Communications) du CCC (Centre canadien pour la cybersécurité) et avec la division CS (Communications stratégiques) du BCP (Bureau du Conseil privé) (pour tous les événements qui exigent des communications externes ou une coordination des messages);
- les **ministères et organismes concernés** élaborent leurs propres produits de communication destinés aux clients/intervenants ou au grand public (tous les événements, mais avec l'approbation de CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada) et de la CS (Communications stratégiques) du BCP (Bureau du Conseil privé) dans le cas des événements de niveau 3 ou 4, conformément au cadre des communications relatives à la cybersécurité du SCT (Secrétariat du Conseil du Trésor du Canada) [1]);
- le **BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada)** coordonne la correspondance publiée à la collectivité des DPI (Dirigeant principal de l'information) et la collectivité des DPS (Dirigeant principal de la sécurité), et elle publie au besoin les rapports destinés à la haute direction tout au long du processus de gestion des événements de cybersécurité (dans le cas des événements de niveau 3 ou 4 ou lorsqu'il faut tenir les intervenants concernés au fait de la situation durant les événements de niveau 2);
- la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** communique au COG (Centre des opérations du gouvernement) et à la division S et R (Sécurité et renseignement) du BCP (Bureau du Conseil privé) les résultats de l'évaluation des incidences sur les opérations dans l'ensemble du gouvernement (dans le cas des événements de niveau 2 ou 3);
- Sur demande, tout au long du processus de gestion des événements de cybersécurité, le **COG (Centre des opérations du gouvernement)** publie les rapports, les documents dressant l'état de la situation ainsi que les notes de breffage produites par les organes de gouvernance du PFIU (Plan fédéral d'intervention d'urgence) (dans le cas des événements de niveau 3 ou 4 ou lorsqu'il faut tenir au fait de la situation les intervenants concernés durant les événements de niveau 2);
- Tout au long du processus de gestion des événements de cybersécurité, la **GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)** coordonne la correspondance publiée auprès de la collectivité opérationnelle (Sécurité de la TI (Technologies de l'information)), et elle publie, au besoin, des produits d'information technique (bulletins sur les incidents de cybersécurité, avis, alertes, etc.) et des rapports d'étape et de

situation liés au niveau d'intervention aux intervenants concernés (tous les événements), en collaboration avec le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et les autres partenaires applicables);

- les **principaux intervenants et les intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)** veillent à ce que les organismes compétents soient informés de la détection d'une cyberactivité criminelle, terroriste ou militaire (respectivement la GRC (Gendarmerie royale du Canada), le SCRS (Service canadien du renseignement de sécurité) et le MDN (Ministère de la Défense nationale));
    - la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) s'occupe d'informer la GRC (Gendarmerie royale du Canada), le SCRS (Service canadien du renseignement de sécurité) et/ou le MDN (Ministère de la Défense nationale) si l'activité liée à leur mandat respectif est découverte durant la gestion d'un événement.

La figure 6 illustre le flux d'échange de renseignements. À noter que l'échange de renseignements aux niveaux inférieurs se poursuit en parallèle à l'échange de renseignements au niveau supérieur.

Figure 6 : Flux d'échange de renseignements selon le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)



▼ Figure 6 - Version textuelle

La figure 6 présente le flux d'échange d'information du PGEC GC, séparé par les différents niveaux d'intervention du GC décrits à la figure 2. La figure 6 ne s'applique qu'aux trois premiers niveaux d'intervention et ne traite pas de l'échange d'information au niveau 4 (intervention en cas d'urgence ou de crise).

1. Niveau 1 – Réponse du ministère
    a. Le CCC est l'agent central de la collecte d'information
    b. Le CCC obtiendra et fournira des renseignements aux sources suivantes :
        i. BDPI du SCT
        ii. Ministères et organismes (équipe de la sécurité de la TI)
        iii. Sources d'information technique
    c. Le BDPI du SCT doit recevoir de l'information uniquement du CCC.

2. Niveau 2 – Réponse limitée à l'échelle du GC
    a. L'Équipe de coordination des événements est désignée comme la source centrale d'échange d'information.
    b. L'Équipe de coordination des événements est composée des agents suivants :
        i. BDPI du SCT
        ii. CCC
        iii. autres intervenants du PGEC GC
    c. L'Équipe de coordination des événements fournira et recevra des renseignements des intervenants suivants :
        i. ministères et organismes (équipe de la sécurité de la TI) (par l'entremise du CCC)
        ii. S et R du BCP (par l'entremise du CCC)
        iii. autres intervenants du PGEC GC
3. Niveau 3 – Intervention globale à l'échelle du GC
    a. Deux organes de gouvernance sont désignés comme des sources centrales pour l'échange de renseignements.
    b. La première est l'Équipe de la haute direction composée des agents suivants :
        i. BDPI du SCT
        ii. CSAM du SCT
        iii. CCC
        iv. autres intervenants du PGEC GC
    c. L'Équipe de la haute direction (par l'entremise du BDPI du SCT) fournira de l'information aux ministères et organismes (DPS).
    d. L'EDH fournira et recevra des renseignements du CCSNS en tant que comité.
    e. L'EHD (par l'entremise du CSAM du SCT) fournira et recevra des renseignements des ministères et organismes (Communications), des Communications du BCP.
    f. L'EHD (par l'entremise du BDPI du SCT) informera le deuxième niveau de gouvernance au niveau du SMA.
    g. Le deuxième niveau de gouvernance est le suivant :
        i. Comités des SMA désignés
        ii. DPT du GC
    h. Le DPT du GC fournira des renseignements aux ministères et organismes au niveau du DPI.

5.1.1 Résumé de l'établissement de rapports et de communication

Voici un résume les types de produits d'information et de communication qui sont diffusés au sein du GC (Gouvernement du Canada) au cours d'un cyberévénement, selon le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada). L'échange de renseignements entre les principaux intervenants et les intervenants spécialisés s'effectue

conformément aux procédures normales d'exploitation établies. À noter que ce tableau ne tient pas compte de l'échange de renseignements qui se poursuit au moyen des processus ou des mécanismes existants.

Tableau 1A : Résumé de l'établissement de rapports et de communication entre les principaux intervenants et les intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)

Type	Expéditeur(s)	Destinataire(s)	Moment de la production
Conscience situationnelle (événements de gravité de niveau 2+)	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada)**	Au fur et à mesure de la disponibilité de nouvelles informations (depuis la détection jusqu'à la clôture de l'événement, en passant l'atténuation et les rapports sur la situation générale).
Établissement de rapports sur les événements de cybersécurité	**GRC (Gendarmerie royale du Canada)** **SCRS (Service canadien du renseignement de sécurité)** **MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes)**	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	À la détection d'un événement malveillant menaçant la sécurité d'un système du GC (Gouvernement du Canada)
Établissement de rapports spécifiques au mandat	**Principaux intervenants et intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)**	**GRC (Gendarmerie royale du Canada)**	Dès qu'on soupçonne ou détecte un événement de cybersécurité lié à une activité criminelle.
		SCRS (Service canadien du renseignement de sécurité)	Dès qu'on soupçonne ou détecte un événement de cybersécurité lié à une activité terroriste.
		MDN (Ministère de la Défense nationale)	Dès qu'on soupçonne ou détecte un événement de cybersécurité lié à la défense nationale.

Type	Expéditeur(s)	Destinataire(s)	Moment de la production
Mises à jour sur les incidences sur la qualité des programmes et des services du GC (Gouvernement du Canada)	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**S et R (Sécurité et renseignement) du BCP (Bureau du Conseil privé)**	Au fur et à mesure de la disponibilité de nouveaux renseignements.
Conscience situationnelle (événements de gravité de niveau 2 seulement)	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**COG (Centre des opérations du gouvernement)**	Au fur et à mesure de la disponibilité de nouvelles informations (depuis la détection jusqu'à la clôture de l'événement, en passant l'atténuation et les rapports sur la situation générale).
Documents de communication externe	**CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada)**	**Principaux intervenants et intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada)**	Au besoin

Tableau 1B : Résumé de l'établissement de rapports et de communication des principaux intervenants et intervenants spécialisés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) aux ministères

Type	Expéditeur(s)	Destinataire(s)	Moment de la production
Notification d'incident	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**Ministère concerné (Équipe de sécurité de la TI (Technologies de l'information))**	Dès la détection ou la notification d'un événement de cybersécurité malveillant.

Type	Expéditeur(s)	Destinataire(s)	Moment de la production
Bulletins sur les incidents de cybersécurité, alertes, avis	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**Tous les ministères (Équipe de sécurité de la TI (Technologies de l'information))**	**Gravité élevée :** Dans les 8 heures de la divulgation **Gravité moyenne :** Dans les 24 heures de la divulgation **Gravité faible :** Dans les 72 heures de la divulgation
Demande d'intervention (DI)	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**Tous les ministères (Équipe de sécurité de la TI (Technologies de l'information))**	Au besoin (habituellement lorsque les vulnérabilités sont importantes+ et que l'exposition à l'ensemble du gouvernement est inconnue).
Rapports de situation techniques	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**Tous les ministères (Équipe de sécurité de la TI (Technologies de l'information))**	**Événements de niveau 2, 3, et 4 :** Au besoin
Rapports à la haute direction	**BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada)**	**Tous les ministères (DPI (Dirigeant principal de l'information), DPS (Dirigeant principal de la sécurité))**	**Événements de niveau 2, 3, et 4 :** Au besoin
Orientation stratégique générale visant à réduire au minimum l'incidence d'un événement de cybersécurité	**BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) (par l'intermédiaire du DPI (Dirigeant principal de l'information) du GC (Gouvernement du Canada))**	**Tous les ministères (DPI (Dirigeant principal de l'information))**	**Événements de niveau 4 :** Sur ordre des organes de gouvernance du PFIU (Plan fédéral d'intervention d'urgence) **Événements de niveau 2 et 3 :** Au besoin

Type	Expéditeur(s)	Destinataire(s)	Moment de la production
Documents de communication externe	**CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada)**	**Ministère concerné (Équipe Comm. (Communications))**	Au besoin
Tous les produits d'information nécessaires	**GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)**	**CCSNS (Comité canadien sur les systèmes nationaux de sécurité)**	Au besoin

5.2 Exigences relatives à l'établissement de rapports ministériels

5.2.1 Menaces et vulnérabilités

Lorsque la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) émet une DI (Demande d'intervention), le ministère visé doit établir un rapport sur la menace ou la vulnérabilité en question (se reporter au paragraphe 4.2). Le délai pour une réponse variera selon la nature de la DI (Demande d'intervention). Par conséquent, la DI précisera le délai imparti pour une réponse. D'ordinaire, on accorde un délai de 24 à 48 heures, selon la nature de l'événement.

Les DI (Demande d'intervention) sont toujours envoyées à la boîte aux lettres générale des Opérations de sécurité. Les ministères doivent veiller à ce qu'une procédure soit en place pour assurer la lecture du courrier afin que l'on réponde aux DI dans les plus brefs délais.

5.2.2 Incidents

Tous les incidents de cybersécurité qui sont visés par le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (veuillez consulter le paragraphe 2.3) doivent être déclarés à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) conformément aux exigences du tableau 2. Les mécanismes et les délais d'établissement de rapports varient en fonction de l'importance de l'incidence sur le ministère, calculée selon le procédé décrit à l'annexe B. La GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) veille au stockage sécurisé de ces rapports d'incident et ne communique aux autres ministères et organismes que l'information portant sur les techniques de détection ou d'atténuation (p. ex., indicateurs de compromission, identification de sites malveillants). L'information sensible qui porte sur un ministère particulier n'est pas partagée à l'ensemble du gouvernement.

Tableau 2 : Exigences relatives à l'établissement de rapports liés aux incidents

Importance de l'incidence	Rapport d'incident initial	Rapport d'incident détaillé	Rapport sur les leçons retenues	Sommaire des incidents
Élevée/Très élevée	**Immédiatement** après la détection	Dans les 24 heures après la détection	Dans les 30 jours après la résolution	Tous les trimestres
Moyenne	Dans l'heure après la détection	Dans les 48 heures après la détection	Dans les 30 jours après la résolution	Tous les trimestres
Faible	S. O.	S. O.	S. O.	Tous les trimestres

5.2.3 Exemples d'événements à déclarer

La GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) gère le registre central pour le signalement des événements de cybersécurité au sein du GC (Gouvernement du Canada). Bien que les infractions mineures puissent être gérées à l'échelle du ministère, la majorité des événements de cybersécurité doivent être signalés à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) sans tarder. Les exemples qui suivent, bien qu'incomplets, donnent une indication des types d'événements à déclarer :

- des messages de courriel suspects ou ciblés avec liens ou pièces jointes que n'ont pu détecter les systèmes de contrôle en place;
- une activité réseau suspecte ou non autorisée qui s'écarte de la norme;
- la violation de données ou la compromission ou corruption de l'information;
- l'introduction intentionnelle ou accidentelle d'un logiciel malveillant dans un réseau;
- des attaques par déni de service;
- la défiguration ou la compromission de pages Web ou en ligne, y compris l'utilisation non autorisée de comptes de médias sociaux du GC (Gouvernement du Canada).

Il faut aussi s'interroger pour savoir si l'événement peut avoir des incidences sur d'autres organisations du GC (Gouvernement du Canada). Dans le doute, il vaut mieux le déclarer que de prendre des risques.

5.2.4 Autre

Si des éléments de preuve laissent présumer l'existence d'une activité criminelle selon le *Code criminel*, les ministères et organismes doivent le faire savoir non seulement à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), mais aussi **directement** à la GRC (Gendarmerie royale du Canada) ou à la police militaire, selon le cas.

Les ministères doivent aussi le faire savoir à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) dès qu'ils constatent qu'ils ont besoin d'une aide supplémentaire à la phase Atténuation et reprise du fait de l'occurrence d'un

événement de cybersécurité (p. ex., l'aide de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), de la GRC (Gendarmerie royale du Canada), de l'équipe des RSSN (Réseaux, sécurité et services numériques) de SPC (Services partagés Canada), de fournisseurs de services) ou qu'ils ne sont pas en mesure de mettre à exécution les consignes dans le délai imparti.

Les ministères et organismes qui assurent des services à d'autres organisations du GC (Gouvernement du Canada) doivent informer ces bénéficiaires (en plus de l'établissement de rapports réguliers à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité)) lorsqu'un événement de cybersécurité compromet la qualité de l'information ou du service qu'il leur dispense.

Les équipes Communications des ministères et organismes concernés coordonnent la préparation des produits de communication destinés aux clients/intervenants ou au grand public en collaboration avec la division CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada), conformément au cadre des communications relatives à la cybersécurité du SCT [1].

En cas d'atteinte réelle ou soupçonnée à la vie privée, les ministères et les organismes interviendront conformément à la *Directive sur les pratiques relatives à la protection de la vie privée*. Les ministères et les organismes devraient se renseigner sur les *Lignes directrices sur les atteintes à la vie privée du SCT (Secrétariat du Conseil du Trésor du Canada)* et la boîte à outil de gestion des atteintes à la vie privée. Ces instruments en matière de protection des renseignements personnels indiquent les causes des cas de violation et donnent des conseils sur la façon d'intervenir et de circonscrire et de gérer les cas de violation de la vie privée, en plus de définir les rôles et responsabilités et de fournir des liens à des documents de référence. Les ministères et organismes doivent consulter les conseillers juridiques au besoin.

5.3 Sécurisation des communications

Durant le cycle de gestion des événements de cybersécurité (plus particulièrement, durant les phases Détection et évaluation et Atténuation et reprise), des intervenants ont à s'échanger des informations. Lorsqu'il s'agit d'informations sensibles, qui concernent, par exemple, la vulnérabilité de systèmes informatiques ou l'exfiltration de données, ces intervenants doivent recourir à des méthodes de communication sûres pour transmettre ces informations.

C'est pourquoi tous les intervenants doivent être prêts à envoyer et à recevoir des informations sensibles. Ils doivent également veiller au bon fonctionnement des outils de communication sécurisés (c'est-à-dire, l'infrastructure de données et de technologies vocales sécurisées) et veiller à ce qu'une procédure soit en place avec laquelle le personnel est familiarisé. Les intervenants qui

n’ont pas à leur disposition suffisamment d’outils doivent veiller à ce qu’un procédé manuel soit en place pour envoyer et recevoir ces informations et reconnaître que ce procédé peut retarder leur réception.

Annexe A : Rôles et responsabilités

▼ **Titres de la section**

Sont décrits ici les rôles et les responsabilités des intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada). Ces rôles et responsabilités varient en fonction du type d’événement (menace, vulnérabilité ou incident de sécurité) et de son niveau de priorité.

1. Principaux intervenants de la gestion des événements de cybersécurité

Voici la liste des principaux intervenants du processus de gestion des événements de cybersécurité (y compris les menaces et vulnérabilités et les incidents confirmés) et qui répondent aux critères préétablis. Le degré de participation de chaque intervenant est fonction de l’incidence ou de la gravité de l’événement.

Secrétariat du Conseil du Trésor du Canada

Le Secrétariat du Conseil du Trésor Canada (SCT) assure la surveillance et l’orientation stratégiques du processus de gestion des événements de cybersécurité, veillant à la bonne coordination des événements afin de faciliter la prise de décisions et de réduire au minimum les incidences sur le gouvernement et les pertes pour le GC (Gouvernement du Canada).

Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), les responsabilités du SCT (Secrétariat du Conseil du Trésor du Canada) en matière de surveillance stratégique, déléguées au BDPI (Bureau du dirigeant principal de l’information), consistent à :

- établir, tenir à jour et tester le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) et les procédures connexes;
- assurer la coordination stratégique des interventions du GC (Gouvernement du Canada) en réponse aux événements de cybersécurité prioritaires (habituellement les événements de niveau 3, ou lorsque des événements de niveau 2 le nécessitent), ce qui comprend :

    - la fonction de coprésident et de secrétaire de toutes les équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (y compris les décisions d'acheminement au palier supérieur et de désamorçage en collaboration avec la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité));
    - l'évaluation, en collaboration avec la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) et d'autres partenaires, de l'incidence des cybermenaces, des vulnérabilités et des incidents de sécurité sur l'ensemble des programmes et services du GC (Gouvernement du Canada), afin de faciliter l'établissement de rapports et l'établissement des priorités dans l'ensemble du gouvernement;
    - la prestation de conseils aux ministères et organismes (par l'entremise du DPI (Dirigeant principal de l'information) du GC (Gouvernement du Canada)) qui préconisent l'adoption de mesures permettant de réduire au minimum l'incidence des événements de cybersécurité importants sur l'ensemble du gouvernement;
- prodiguer des conseils stratégiques au CIDG (Comité d'intervention des directeurs généraux) durant les événements de cybersécurité de niveau 4;
- veiller à ce que la division CSAM (Communications stratégiques et affaires ministérielles) obtienne à temps les informations dont elle a besoin pour élaborer des produits de communication;
- analyser les rapports après événement que produit la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), et recenser les leçons apprises dans l'ensemble du gouvernement, s'il y a lieu, afin d'améliorer la politique de sécurité ou l'architecture s'y rapportant.

La division CSAM (Communications stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada) joue un rôle dans le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) en ce qui a trait à la communication stratégique, habituellement dans le cas des événements de niveau 3 (ou dans le cas d'autres événements qui le nécessitent). En sa qualité de porte-parole du GC (Gouvernement du Canada) relativement à tous les événements de cybersécurité qui compromettent l'intégrité des programmes et services publics, la CSAM (Communications stratégiques et affaires ministérielles) est responsable :

- de préparer, en collaboration avec la Direction générale des communications de CST (Centre de la sécurité des télécommunications) et la division CS (Communications stratégiques) du BCP (Bureau du Conseil privé), et en consultation avec les équipes Communications des intervenants concernés du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), des documents de communication interne (publiés dans l'ensemble du gouvernement) et externe;

- de déterminer s'il est nécessaire de faire des déclarations publiques (proactives et réactives), et le cas échéant, de choisir le moment;
- d'approuver tous les plans de communication (communication interne ou destinée aux clients/intervenants ou au grand public), en collaboration avec les organisations concernées et la division CS (Communications stratégiques) du BCP (Bureau du Conseil privé).

Centre de la sécurité des télécommunications

Le Centre de la sécurité des télécommunications abrite le Centre canadien pour la cybersécurité (CCC). Il joue plusieurs rôles dans la gestion des événements de cybersécurité du GC (Gouvernement du Canada).

Coordination

L'équipe de la Gestion des incidents et coordination opérationnelle (GICO) coordonne toutes les phases opérationnelles de la gestion des événements pour les événements de cybersécurité qui ont eu ou pourraient avoir des incidences sur le GC (Gouvernement du Canada). Les activités de coordination comprennent notamment :

- surveiller le périmètre du GC (Gouvernement du Canada) et de tous les points d'extrémité pour lesquels ils ont de la visibilité, intervenir dans les événements de cybersécurité, et mettre en œuvre des mesures préventives et d'atténuation au besoin;
- servir de contact central pour les opérations de cybersécurité, qu'il s'agisse de la diffusion des produits d'information technique ou de la collecte des rapports que les organisations du GC (Gouvernement du Canada) envoient au sujet des événements;
- assurer la coordination opérationnelle des réponses du GC (Gouvernement du Canada) en réponse à la totalité des événements de cybersécurité, y compris :
    - le contrôle des sources d'information technique (incluant les POCS (Principal organisme responsable de la sécurité), les ministères et organismes concernés, les fournisseurs) afin de détecter les signes précurseurs de cybermenaces, de vulnérabilités ou d'incidents de cybersécurité confirmés;
    - l'émission quotidienne de produits d'information en matière de sécurité qui renferment des conseils techniques d'atténuation des menaces (p. ex., alertes, avis) et des DI (Demande d'intervention) à l'intention des ministères et organismes;
    - la collation, le suivi et l'établissement de rapports sur les événements et les réponses aux événements, et la mise en œuvre des moyens techniques d'atténuation;
    - l'évaluation, en collaboration avec le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et d'autres partenaires, de l'incidence des cybermenaces, des vulnérabilités et des incidents de sécurité sur l'ensemble des programmes et services du GC (Gouvernement du Canada), afin de faciliter l'établissement de rapports et l'établissement des priorités dans l'ensemble du gouvernement;

    - la coordination des efforts en matière de prévention, d'atténuation et de reprise des activités, et la livraison opportune de rapports aux divers acteurs du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) pour les tenir au fait de la situation;
    - la coprésidence de toutes les équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) (y compris les décisions d'acheminement au palier supérieur et de désescalade en collaboration avec le SCT (Secrétariat du Conseil du Trésor du Canada)).
- établir des rapports après événement qui comprennent la chronologie des événements et une analyse de la cause première (d'après les analyses et les rapports sur les leçons apprises produits par les ministères) et les soumettre au BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et autres organisations concernées, au besoin (p. ex., BCP (Bureau du Conseil privé));
- communiquer avec le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) tout au long du cycle de gestion des événements de cybersécurité;
- vérifier la clôture des événements et en informer les intervenants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) concernés;
- communiquer le cyberrenseignement lié aux enquêtes et fournir des activités de sensibilisation liées aux cybermenaces, aux vulnérabilités et aux techniques d'attaque.

Parmi les autres services offerts par le CCC (Centre canadien pour la cybersécurité) pour aider les ministères et organismes à se remettre d'événements liés à la cybersécurité et à reprendre des activités normales, mentionnons, entre autres, les suivants :

- l'enquête et l'analyse judiciaires, y compris la collecte des preuves et un soutien aux enquêtes;
- l'analyse de vulnérabilité et la réponse;
- l'analyse des logiciels malveillants et la réponse.

La prestation de ces services est généralement gérée par le CCC (Centre canadien pour la cybersécurité), mais, s'il y a lieu, les priorités peuvent être établies conformément à la structure de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada).

Capacité consultative technique

Le CCC (Centre canadien pour la cybersécurité) élabore, fournit et exploite des moyens et des outils pour la gestion des événements de cybersécurité, et il prodigue des conseils techniques au sein du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada). Son rôle comprend les responsabilités suivantes :

- détecter, bloquer ou atténuer les cybermenaces visant les réseaux ou les données du GC (Gouvernement du Canada);
- établir des rapports et concevoir d'autres produits d'information à l'intention des autres intervenants importants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada);
- participer à l'identification des événements de cybersécurité et à leur atténuation, à l'évaluation des risques, à la reprise des activités et aux analyses après événement;
- fournir une connaissance situationnelle des événements de cybersécurité (sur les systèmes du GC (Gouvernement du Canada) qui sont secrets ou inférieurs) au CCSNS (Comité canadien sur les systèmes nationaux de sécurité).

Centre national de coordination

Le CCC (Centre canadien pour la cybersécurité) est le centre national de coordination en matière de prévention, d'atténuation, de préparation, d'intervention et de reprise des activités après un événement de cybersécurité.

De concert avec des partenaires nationaux ou internationaux, le CCC (Centre canadien pour la cybersécurité) s'emploient à répondre aux graves préoccupations en matière de cybersécurité, qui concernent notamment les organisations et les infrastructures essentielles et les administrations publiques provinciales, territoriales ou municipales. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), le CCC (Centre canadien pour la cybersécurité) est responsable :

- de communiquer au COG (Centre des opérations du gouvernement) les renseignements et les avertissements qu'il reçoit de la part de partenaires nationaux ou internationaux au sujet de cybermenaces, de vulnérabilités ou d'incidents;
- d'échanger avec les partenaires nationaux et internationaux les données non classées de partenaires du GC (Gouvernement du Canada) (menaces, vulnérabilités, indicateurs, etc.);
- de communiquer des renseignements sur la portée et l'incidence possibles d'un événement donné du point de vue des propriétaires et des exploitants d'infrastructures essentielles du Canada en vue d'assurer une compréhension complète des incidences qui n'affectent pas directement les systèmes du GC (Gouvernement du Canada), mais qui touchent l'intérêt du GC (Gouvernement du Canada).

Communications

L'équipe Communications (Comm.) du CST (Centre de la sécurité des télécommunications) joue elle aussi un rôle durant les événements de cybersécurité d'importance. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), cette équipe responsable, durant un événement de cybersécurité, d'assister la CSAM (Communications

stratégiques et affaires ministérielles) du SCT (Secrétariat du Conseil du Trésor du Canada) dans la coordination de l'ensemble des activités de communication publique du GC (Gouvernement du Canada).

2. Intervenants spécialisés de la gestion des événements de cybersécurité

Voici la liste des intervenants spécialisés du processus de gestion des événements de cybersécurité et à qui on fait appel lorsque des cybermenaces ou des incidents confirmés nécessitent une attention spécialisée liée à leur mandat respectif.

Services partagés Canada

Services partagés Canada (SPC) est responsable de l'infrastructure de réseau de 43 partenaires, des services fournis à d'autres ministères et organismes du GC (Gouvernement du Canada) et de la gestion du périmètre au moyen des passerelles et de l'infrastructure secrète.

Dans le cas d'un événement de cybersécurité, SPC (Services partagés Canada) coordonnera ses activités avec les partenaires afin de déterminer si l'infrastructure gérée par SPC doit être fermée ou isolée du réseau et répondre aux recommandations de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) et aux directives du BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada).

De plus, SPC (Services partagés Canada) développe, fournit et exploite des capacités et des outils pour la défense préventive de l'infrastructure de réseau pour les 43 partenaires. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), SPC (Services partagés Canada) est responsable de :

- détecter et d'atténuer les cybermenaces visant les réseaux ou les données gérés par SPC (Services partagés Canada);
- répondre aux recommandations de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) et du BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et du BDPI, et veiller à ce que les mises à jour et les mesures d'atténuation soient appliquées en temps opportun;
- mettre en œuvre des efforts en matière de prévention, d'atténuation et de reprise des activités, et la livraison opportune de rapports aux principaux acteurs du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) pour les tenir au fait de la situation;
- établir des rapports et concevoir d'autres produits d'information à l'intention des intervenants importants du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada);

- participer à l'identification des événements de cybersécurité et à leur atténuation, à l'évaluation des risques, à la reprise des activités et aux analyses après événement;
- l'évaluation de l'incidence des cybermenaces, des vulnérabilités et des incidents de sécurité sur l'ensemble des programmes et services du GC (Gouvernement du Canada), afin de faciliter l'établissement de rapports dans l'ensemble du gouvernement à remettre à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) et au BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada);
- établir des rapports après événement, y compris la chronologie des événements et une analyse de la cause première et les soumettre à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), au BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) et autres organisations concernées, au besoin (p. ex., BCP (Bureau du Conseil privé)).

Sécurité publique Canada

Sécurité publique Canada (SP) dirige la politique et la stratégie nationales en matière de cybersécurité notamment en coordonnant l'intervention globale en cas de cyberévénements d'envergure nationale par l'entremise du COG (Centre des opérations du gouvernement).

Gendarmerie royale du Canada

La Gendarmerie royale du Canada (GRC) est le principal service d'enquête des incidents de cybersécurité de toutes sortes, s'occupant des cybercrimes, réels ou présumés, d'origine non étatique qui touchent à l'infrastructure informatique du GC (Gouvernement du Canada).

Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), la GRC (Gendarmerie royale du Canada) est chargée de :

- diriger les enquêtes criminelles dans le cas d'incidents de cybersécurité liés à une activité criminelle non étatique, y compris une activité terroriste;
- participer aux équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) à titre de guide et de conseiller, lorsque l'incident de cybersécurité ou la cybermenace le nécessite.

Service canadien du renseignement de sécurité

Le Service canadien du renseignement de sécurité (SCRS) est le principal service chargé d'enquêter sur les menaces visant les systèmes d'information et les infrastructures essentielles de la part d'intervenants ou de terroristes vivant à l'étranger.

Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), le SCRS (Service canadien du renseignement de sécurité) est responsable de :

- diriger les enquêtes dans le cas d'incidents de cybersécurité qui posent une menace pour la sécurité du Canada, d'après la définition qu'en donne la Loi sur le SCRS (Service canadien du renseignement de sécurité) (comprend le terrorisme et l'espionnage);
- participer aux équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) à titre de guide et de conseiller, lorsque l'incident de cybersécurité ou la cybermenace le nécessite.

Ministère de la Défense nationale/Forces armées canadiennes

Le ministère de la Défense nationale/Forces armées canadiennes (MDN-FAC) est le principal ministère chargé d'intervenir en cas de cybermenaces, de vulnérabilités ou d'incidents de sécurité visant les systèmes militaires. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), MDN-FAC (Ministère de la Défense nationale/Forces armées canadiennes) est responsable de :

- diriger les enquêtes dans le cas de tous les incidents de cybersécurité (au Canada ou à l'étranger) liés à des activités menaçant l'intégrité des systèmes militaires (soit les systèmes qui appuient directement les opérations, de même que les systèmes d'armes);
- apporter éventuellement de l'aide et de l'assistance à d'autres ministères publics, sur demande;
- participer aux équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) à titre de guide et de conseiller, lorsque l'incident de cybersécurité ou la cybermenace le nécessite.

3. Autres intervenants

Dirigeant principal de l'information du gouvernement du Canada

Le dirigeant principal de l'information du gouvernement du Canada (DPI du GC) défend les intérêts de l'ensemble du gouvernement durant les événements de cybersécurité qui touchent, ou peuvent toucher, l'exécution des programmes et la prestation des services, en abordant des sujets qui comprennent la réponse globale du GC (Gouvernement du Canada) aux événements de cybersécurité et les mesures prises à l'échelle de l'organisation en vue de protéger les systèmes d'information du GC (Gouvernement du Canada). Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), le DPI (Dirigeant principal de l'information) du GC (Gouvernement du Canada) est responsable des suivants :

- de donner suite aux décisions de gestion des risques de cybersécurité en répondant à l'émission de directives obligatoires aux ministères en réponse aux événements de cybersécurité (p. ex., appliquer des mesures de sécurité ou de déconnecter des systèmes du réseau ayant mis le GC (Gouvernement du Canada) à risque, au besoin);

- renseigner le bureau du sous-ministre délégué et les niveaux supérieurs, au besoin, en plus de conseiller les CSMA sur les questions liées aux événements, comme la sécurité et les opérations des systèmes et réseaux de la TI (Technologies de l'information) du GC (Gouvernement du Canada), la prestation des services et la confiance dans le gouvernement;
- présider un comité composé des DPI (Dirigeant principal de l'information) des ministères, le CDPI; par l'entremise de ce dernier, le DPI du DC peut émettre des directives à l'intention des DPI des ministères en ce qui concerne les activités de gestion des événements de cybersécurité, en particulier les activités qui favorisent l'atténuation des événements ou la reprise des activités.

Centre des opérations du gouvernement

Le Centre des opérations du gouvernement (COG), au nom du GC (Gouvernement du Canada), dirige et appuie la coordination des interventions en réponse à tout type d'événement qui menace les intérêts nationaux. Son rôle ne concerne pas uniquement les événements de cybersécurité. En tout temps, il assure la surveillance, établit des rapports, offre une connaissance de la situation à l'échelle nationale, élabore des évaluations intégrées du risque et de produits d'avertissement, effectue la planification à l'échelle nationale et coordonne une gestion pangouvernementale des interventions. Lors des périodes nécessitant des interventions accrues, d'autres ministères et organismes du gouvernement et des organisations non gouvernementales travaillent de concert avec le COG (Centre des opérations du gouvernement), sur place ou à distance.

Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), le COG (Centre des opérations du gouvernement) est responsable de :

- contrôler le déroulement des événements de cybersécurité de niveau 3 au cas où il faudrait consulter l'autorité supérieure; pour ce faire, il doit notamment :
  - préparer, à l'intention des centres des opérations de l'ensemble du gouvernement, des produits d'avertissement et des documents dressant l'état de la situation;
  - établir des plans et procéder à des évaluations des risques;
  - informer les organes de gouvernance du PFIU (Plan fédéral d'intervention d'urgence).
- coordonner l'intervention globale du GC (Gouvernement du Canada) au cours des événements de niveau 4, conformément au PFIU (Plan fédéral d'intervention d'urgence).

Bureau du Conseil privé

En sa qualité de principal prestataire de conseils impartiaux au premier ministre et au Cabinet, le Bureau du Conseil privé (BCP), dans son rôle d'organisme central, participe à la formulation et à la mise en œuvre du programme politique du GC (Gouvernement du Canada) et à la coordination des solutions opportunes aux problèmes d'importance nationale, internationale ou intergouvernementale auxquels le GC (Gouvernement du Canada) est confronté. À ce titre, l'équipe S et R (Sécurité et renseignement) du BCP (Bureau du Conseil privé) joue un rôle de premier plan

dans la coordination des interventions générales du gouvernement en réponse aux urgences sécuritaires nationales. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), la S et R (Sécurité et renseignement) du BCP (Bureau du Conseil privé) :

- appuie le processus décisionnel en veillant à ce que les hauts fonctionnaires soient rapidement informés des incidents de cybersécurité pouvant avoir une importance nationale ou des implications sécuritaires nationales;
- participe aux équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) à titre de guide et de conseiller, lorsque l'incident national ou la menace le nécessite.

Du point de vue des communications, l'équipe des Communications stratégiques (CS) du BCP (Bureau du Conseil privé) joue elle aussi un rôle durant les événements de cybersécurité d'importance. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), elle est responsable, durant un événement de cybersécurité, de conseiller le Cabinet et les hauts fonctionnaires du BCP (Bureau du Conseil privé) et de coordonner les activités de communication dans l'ensemble du gouvernement en collaboration avec l'équipe Communications de SP (Sécurité publique Canada) et du CST (Centre de la sécurité des télécommunications), ce qui comprend la gestion des crises.

Comité canadien sur les systèmes nationaux de sécurité

Le Comité canadien sur les systèmes nationaux de sécurité (CCSNS), dont la présidence est assurée par le chef adjoint du CCC (Centre canadien pour la cybersécurité), élabore et gère un plan de gestion global pour assurer la sécurité de ceux des systèmes du GC (Gouvernement du Canada) dont la fiabilité doit être à toute épreuve, à savoir les systèmes nationaux de sécurité. Le CCSNS (Comité canadien sur les systèmes nationaux de sécurité) gère en parallèle un plan de gestion des urgences qui s'applique à tous les systèmes nationaux de sécurité et il peut offrir de la visibilité aux organes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) dans des situations qui peuvent aussi avoir des incidences sur les systèmes qui ne font pas partie des systèmes nationaux de sécurité. Ces situations peuvent aussi survenir dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada); le CCSNS (Comité canadien sur les systèmes nationaux de sécurité) profite donc d'un triage bidirectionnel au niveau de la direction et reçoit certains types d'alertes du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada).

Comité d'intervention des directeurs généraux

Le Comité d'intervention des directeurs généraux (CIDG) est un comité fédéral composé de directeurs généraux qui gèrent les activités d'intervention opérationnelle et qui dirigent, appuient et améliorent la planification des interventions et la coordination des événements menaçant les

intérêts nationaux. Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), le CIDG (Comité d'intervention des directeurs généraux) assure l'interface entre les organes de gouvernance du PFIU (Plan fédéral d'intervention d'urgence) durant les événements de niveau 4, assurant au besoin la liaison avec les comités du SMA (Sous-ministre adjoint), du SM et du Cabinet.

Partenaires externes

Les ministères et organismes font souvent appel aux services de partenaires de l'extérieur du GC (Gouvernement du Canada) pour assurer la prestation des programmes et services, et notamment des fournisseurs du secteur privé et d'autres ordres de gouvernements. Les partenaires externes sont tenus de gérer les événements de cybersécurité et d'en rendre compte conformément aux stipulations des accords contractuels respectifs des propriétaires des services des ministères.

4. Ministères et organismes

Les ministères et organismes jouent un rôle clé dans la gestion des événements de cybersécurité dans l'ensemble du gouvernement, qu'ils soient ou non directement concernés par l'événement. Leurs rôles et leurs responsabilités en la matière sont exposés dans le détail dans leurs plans et leurs procédures de gouvernance, lesquels ont pour but d'appuyer la mise en application de la PSG et de ses directives et de ses normes d'application.

Dans le contexte du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), les ministères et organismes sont chargés :

- de déclarer les événements de cybersécurité conformément à la section 5.2 du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada);
- de contrôler les produits d'information technique de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) et d'évaluer leur applicabilité aux systèmes d'information que gèrent et possèdent les ministères;
- d'analyser l'incidence des cybermenaces, des vulnérabilités et des incidents de sécurité sur leurs programmes et leurs services;
- de répondre aux DI (Demande d'intervention) de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) dans les délais impartis;
- de mettre en œuvre les moyens d'atténuation selon les directives et les consignes des POCS (Principal organisme responsable de la sécurité) ou des organismes centraux;
- d'aviser la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) lorsqu'on a besoin d'aide supplémentaire pour exécuter des activités d'intervention;
- d'aviser l'autorité compétente chargée de l'application de la loi ou de la sécurité nationale lorsqu'un événement est de son ressort;

- de participer aux équipes de gouvernance du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada) lorsqu'un coprésident le leur demande (habituellement lorsqu'un événement de cybersécurité les concerne);
- de suivre le protocole prévu en cas de violation de la vie privée;
- de réaliser des analyses après événement et de préparer des rapports sur les leçons qu'ils ont apprises (valable pour les événements concernés), et d'en présenter les résultats de la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité);
- d'élaborer et de publier des produits de communication appropriés de gestion des intervenants et des clients (en consultation avec CSAM (Communications stratégiques et affaires ministérielles)/SCT (Secrétariat du Conseil du Trésor du Canada) et CS (Communications stratégiques)/BCP (Bureau du Conseil privé) ou sous leur direction, au besoin);
- de veiller à ce que les exigences de la direction et les exigences relatives à l'établissement de rapports liés aux événements de cybersécurité soient clairement stipulées dans les contrats, les protocoles d'entente et les autres accords officiels conclus avec des partenaires externes (p. ex., des fournisseurs du secteur privé et d'autres ordres de gouvernements) et à ce que ces contrats, protocoles et accords tiennent compte des exigences établies dans les instruments de politique applicables du GC (Gouvernement du Canada) et des ministères, ainsi que dans le PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement du Canada), entre autres instruments;
- d'élaborer, de tenir à jour et de mettre à l'essai des plans et des procédés de gestion des événements de cybersécurité, et d'en assurer l'harmonisation avec les directives, les plans et les procédés en place dans l'ensemble du gouvernement;
- de tenir à jour un répertoire des systèmes d'information essentiels à la réalisation de la mission ainsi qu'un fonds de données, afin de faciliter les interventions ou l'établissement des priorités;
- de tenir à jour et d'améliorer continuellement leur capacité d'intervention, y compris, notamment, la mise en application des leçons apprises (dans le ministère et dans l'ensemble du gouvernement), la mise en pratique périodique de leurs plans et procédures, la tenue à jour de listes de personnes-ressources internes, et la formation adéquate du personnel responsable d'intervenir en cas d'événement de cybersécurité.

Les ministères et organismes qui dispensent des services à d'autres organisations du GC (Gouvernement du Canada) doivent établir des mécanismes afin d'informer leurs bénéficiaires des événements de cybersécurité qui ont une incidence sur leurs systèmes ou leurs données. Les fournisseurs de service doivent aussi fournir aux bénéficiaires les données dont ils ont besoin pour répondre en temps voulu aux exigences relatives à l'établissement de rapports énoncées au paragraphe 5.2 du PGEC GC (Plan de gestion des événements de cybersécurité du gouvernement

du Canada) (plus précisément, pour appuyer la réalisation des rapports d'incidents et des réponses aux DI (Demande d'intervention)), ainsi que toutes autres données numériques nécessaires à la réalisation des activités d'atténuation ou de reprise ou des activités après événement.

Annexe B : Évaluation de l'incidence des événements sur les ministères

▼ **Titres de la section**

Le processus général qui suit sert à évaluer l'incidence d'un événement de cybersécurité sur un ministère; ce qui permettra en fin de compte au GC (Gouvernement du Canada) d'en déterminer l'incidence sur l'ensemble des ministères et ainsi être en mesure d'intervenir de manière adéquate dans l'ensemble du gouvernement.

Quel que soit le type d'événements de cybersécurité (menaces, vulnérabilités ou incidents confirmés), l'évaluation de leur incidence commence par un test de préjudice permettant de mesurer le degré de préjudice qui pourrait vraisemblablement découler d'une compromission (se reporter à l'étape 1). Dans le cas d'incidents de sécurité confirmés, le résultat de ce test représente l'incidence de l'incident, puisque le préjudice a été confirmé, et le processus s'arrête là.

Dans le cas de cybermenaces ou de vulnérabilités, il faut franchir une autre étape avant de pouvoir déterminer la probabilité d'occurrence d'un préjudice et ainsi obtenir une idée précise de l'éventuelle incidence sur un ministère (veuillez consulter l'étape 2).

Étape 1 (pour tous les types d'événements de cybersécurité) : Test de préjudice

Le test de préjudice, qui s'effectue selon le tableau 3, est fonction de la gravité et de l'étendue du préjudice qui pourrait vraisemblablement survenir.

Gravité : La gravité du préjudice réfère à l'importance des dommages ou des pertes (p. ex., depuis les dommages corporels jusqu'au décès, depuis les pertes financières négligeables jusqu'à la perte de viabilité, depuis les faibles ennuis jusqu'aux énormes difficultés). Elle peut être caractérisée de mineure, importante ou extrême, selon l'évaluation des types suivants de préjudices :

- nuisible à la santé ou à la sécurité des personnes;
- pertes financières ou difficultés économiques;
- incidences sur les programmes et les services publics;
- menace pour l'ordre public ou pour la souveraineté nationale;

- nuisible à la réputation ou aux relations.

Peuvent aussi entrer en ligne de compte d'autres facteurs particuliers au mandat du ministère ou de l'organisme ou au contexte opérationnel.

Étendue : L'étendue du préjudice réfère au nombre de personnes, d'organisations, d'installations ou de systèmes touchés, à la région géographique concernée (p. ex., préjudice localisé ou répandu) ou encore à la durée du préjudice (p. ex., de court ou de long terme). L'étendue peut être caractérisée de :

- Grande : Le préjudice est répandu; est national ou international; s'étale à plusieurs pays ou juridictions; affecte d'importants programmes ou secteurs publics.
- Moyenne : Le préjudice concerne une juridiction, un secteur d'activité, un programme public; un groupe ou une collectivité.
- Faible : Le préjudice concerne un particulier, une petite entreprise.

Tableau 3 : Test de préjudice

		Portée		
		Faible	**Moyenne**	**Grande**
Gravité	**Extrême**	Moyenne	Élevée	Très élevée
	Importante	Faible	Moyenne	Élevée
	Limitée	Faible	Faible	Moyenne
Niveau de l'incidence sur le ministère		[Resultat du test de préjudice]		

Le tableau 4 permet d'analyser les conséquences possibles d'une compromission et de valider les résultats du test de préjudice initial. Une fois confirmée, cette valeur peut être inscrite dans le rapport d'incident et soumise à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité).

Tableau 4 : Conséquences prévues d'une compromission

Incidence	**Conséquences d'une compromission**
Très élevée	• Nombreuses pertes de vie. • Lourde perte à long terme pour l'économie canadienne. • Atteinte majeure à la sécurité nationale (p. ex., compromet la capacité d'intervention des FAC ou les activités de renseignement nationales). • Très graves nuisances aux relations diplomatiques ou internationales. • Perte de confiance à long terme de la population dans le GC (Gouvernement du Canada), ce qui nuit à la stabilité du gouvernement.

Incidence	Conséquences d'une compromission
Élevée	• Blessés très graves ou décès parmi un groupe de personnes, ou nombreux blessés graves. • Perte financière grave qui nuit à l'économie canadienne, qui compromet la viabilité d'un programme public ou qui réduit la compétitivité à l'échelle internationale. • Sérieux obstacle à la réalisation d'un ou de plusieurs programmes et services essentiels à la réalisation de la mission, ou atteinte importante à la sécurité nationale. • Graves nuisances aux relations internationales qui pourraient être suivies d'une protestation ou d'une sanction officielle. • Perte de confiance à long terme de la population dans le GC (Gouvernement du Canada), ce qui nuit à la réalisation d'un objectif prioritaire du gouvernement.
Moyenne	• Menace pour la sécurité ou la vie d'une personne, ou blessés graves parmi un groupe de personnes. • Perte financière qui nuit au rendement de tout un secteur de l'économie, qui compromet la réalisation des objectifs d'un programme public ou qui nuit au bien-être d'un grand nombre de Canadiens. • Sérieux obstacle à la réalisation de programmes et de services accessibles au grand public, ou au bon fonctionnement d'un ministère, ce qui compromet gravement la réalisation des objectifs. • Nuisances aux relations fédérales-provinciales. • Importante perte de confiance de la population dans le GC (Gouvernement du Canada) ou embarras pour le GC.
Faible	• Dommage physique ou psychologique subi par une personne. • Stress financier ou difficultés financières subis par une personne. • Obstacle au bon fonctionnement d'un ministère qui pourrait avoir une faible incidence sur l'efficacité d'un programme. • Nuisance à la réputation d'un particulier ou d'une entreprise. • Légère perte de confiance de la population dans le GC (Gouvernement du Canada).

Étape 2 (dans le cas uniquement des cybermenaces ou des vulnérabilités) : Évaluation du risque

À la différence des incidents de sécurité confirmés, dont le préjudice a été constaté, les autres cyberévénements que sont les cybermenaces et les vulnérabilités représentent un préjudice qui est encore à l'état de potentialité. C'est pourquoi, lorsque l'on souhaite établir avec précision le niveau de l'incidence potentielle, il faut procéder à une évaluation du risque (à l'aide du tableau 5) afin de déterminer la probabilité d'occurrence du préjudice. En se fondant sur les résultats du test de préjudice réalisé à l'étape 1 (c'est-à-dire, le préjudice prévu), on détermine le niveau de l'incidence

sur le ministère, corrigé du risque, en fonction de facteurs tels que des indicateurs (probabilité de compromission), l'exploitabilité, l'exposition des systèmes d'information concernés et la mise en œuvre de mesures compensatoires.

Tableau 5 : Évaluation du risque

		Exposition			
		Faible	**Moyenne**	**Élevée**	**Très élevée**
		• Faible probabilité que la menace frappe le GC (Gouvernement du Canada). • Vulnérabilité très difficile à exploiter. • Les systèmes vulnérables ne sont pas directement exposés (p. ex., systèmes autonomes). • Les mesures de sécurité en place offrent une protection efficace contre la menace ou la vulnérabilité.	• Probabilité moyenne que la menace frappe le GC (Gouvernement du Canada). • Vulnérabilité exploitable avec d'importantes ressources. • Les systèmes vulnérables sont accessibles par un seul ministère (p. ex., au moyen de son intranet). • Les mesures de sécurité en place offrent une protection partielle contre la menace ou la vulnérabilité.	• Forte probabilité que la menace frappe le GC (Gouvernement du Canada). • Vulnérabilité exploitable avec des ressources en quantité modérée. • Les systèmes vulnérables sont accessibles par de nombreux ministères (p. ex., extranet du GC (Gouvernement du Canada)). • Les mesures de sécurité en place offrent peu de protection contre la menace ou la vulnérabilité.	• Menace ou compromission imminente. • Vulnérabilité facilement exploitable avec peu de ressources. • Les systèmes vulnérables sont fortement exposés (p. ex., par Internet). • Les mesures de sécurité en place n'offrent aucune protection contre la menace ou la vulnérabilité.
Importance de l'incidence (selon le test de l'étape 1)	**Très élevée**	Élevée	Élevée	Élevée	Très élevée
	Élevée	Moyenne	Moyenne	Élevée	Élevée
	Moyenne	Faible	Moyenne	Moyenne	Moyenne
	Faible	Faible	Faible	Faible	Faible
Niveau d'incidence sur le ministère, corrigé du risque		[Resultat de l'évaluation du risque]			

Le niveau d'incidence sur le ministère, après correction du risque, doit être communiqué à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité) (lorsque l'on a reçu une DI (Demande d'intervention)), qui s'en servira à des fins globales.

Les cybermenaces ou les vulnérabilités doivent être considérées comme des incidents de cybersécurité dès la constatation du préjudice. Lorsqu'un préjudice passe de l'état de potentialité à celui de réalité, le test de préjudice évoqué précédemment devra faire l'objet d'une réévaluation, et ses résultats communiqués de nouveau à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), qui devra déterminer s'il y a lieu d'intervenir autrement ou de s'en référer à l'autorité supérieure.

Annexe C : Matrice de calcul du niveau d'intervention (pour l'ensemble du gouvernement)

En se fondant sur la compilation des résultats des évaluations des incidences que les ministères font parvenir à la GICO (Gestion des incidents et coordination opérationnelle) du CCC (Centre canadien pour la cybersécurité), le calcul du niveau d'intervention tient compte du niveau d'urgence au sein du gouvernement du Canada en réponse à l'événement de cybersécurité, selon le tableau 6.

Tableau 6 : Niveaux d'intervention du GC (Gouvernement du Canada)

		Niveau d'urgence au sein du GC (Gouvernement du Canada)		
		Faible	**Moyenne**	**Élevée**
		• Concerne un programme ou service interne du GC (Gouvernement du Canada) • Peu probable que l'événement se propage	• Concerne un programme ou service externe du GC (Gouvernement du Canada) ou plusieurs programmes ou services internes • Possibilité de propagation	• Concerne un grand nombre de programmes ou services internes et externes • Propagation imminente ou confirmée
Niveau d'incidence sur le ministère (selon l'Annexe B)	**Très élevée**	Niveau 3	Niveau 3	Niveau 4
	Élevée	Niveau 2	Niveau 2	Niveau 3
	Moyenne	Niveau 1	Niveau 2	Niveau 2
	Faible	Niveau 1	Niveau 1	Niveau 1
Niveau d'intervention global		[Niveau d'intervention global calculé]		

Cette matrice se veut un guide de calcul. Au moment de déterminer le niveau d'intervention global, il faudra aussi considérer les incidences de l'événement et d'autres facteurs. C'est pourquoi le BDPI (Bureau du dirigeant principal de l'information) du SCT (Secrétariat du Conseil du Trésor du Canada) se réserve le droit de modifier ce niveau en fonction du contexte du scénario de l'événement de cybersécurité.

Notes en bas de page

1 Cadre des communications relatives à la cybersécurité du SCT (Secrétariat du Conseil du Trésor du Canada), 2015.

ISBN : 978-0-660-24006-0

Date de modification :
2020-04-09