Guide du processus de gestion des risques pour la sécurité matérielle

GSMGC-018 (2024)

Préparé par :
La Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
73, promenade Leikin Ottawa (Ontario) K1A 0R2
Publication publiée : 2024-03-15
Mise à jour :

Avant-propos

Guide du processus de gestion des risques pour la sécurité matérielle est une publication NON CLASSIFIÉE, publiée sous l'autorité du Principal Organisme Responsable de la Sécurité Matérielle (POSM) de la GRC.

Il s'agit d'une publication du gouvernement du Canada qui sert de ligne directrice sur les considérations propres à l'élaboration de processus de gestion des risques, y compris la gestion des risques liés à la sécurité matérielle, et la création de procédures opérationnelles normalisées (PON) connexes pour les ministères, organismes et employés du gouvernement du Canada (GC).

Les suggestions de modifications et d'autres renseignements peuvent être envoyés au principal organisme de la sécurité matérielle de la GRC RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Date d'entrée en vigueur

La date d'entrée en vigueur du Guide du processus de gestion des risques pour la sécurité matérielle GSMGC-018 est 2024-03-15.

Registre des modifications

Amendement no.	Date	Entrée par	Résumé de la modification

Remarque : Le pouvoir de modification ou de dérogation est conféré au principal organisme responsable de la sécurité matérielle de la GRC (PORS de la GRC).

Contenu

1. Introduction

La GRC, Principal Organisme Responsable de la Sécurité Matérielle pour le gouvernement du Canada, est chargée de fournir des conseils et des directives sur toutes les questions liées à la sécurité matérielle.

1.1. But

Le présent guide a pour but d'aider les employés du GC qui ont des responsabilités en matière de gestion des risques liés à la sécurité matérielle à élaborer leurs propres processus liés à la gestion des risques liés à la sécurité matérielle, à la délégation de la prise de décisions en matière de risque et à la documentation et à la surveillance des risques résiduels. La Politique sur la sécurité du gouvernement (PSG) exige que des mesures de sécurité matérielle soient mises en œuvre, surveillées et maintenues. Ces processus doivent être officiellement documentés à toutes les étapes du cycle de vie d'une mesure. Le présent document établit un lien entre les outils existants et leurs utilisations afin de décrire des façons efficaces et claires pour les ministères de respecter leurs exigences en matière de sécurité énoncées dans la PSG et la Directive sur la gestion de la sécurité (DGS).

Le guide contient à la fois les mesures de contrôle de sécurité requises, indiquées par l'utilisation du mot « doit », et les mesures de contrôle de sécurité ou les lignes directrices recommandées, indiquées par l'utilisation du mot « devrait ». L'utilisation du mot « doit » indique une référence à une politique ou à une norme établie du gouvernement du Canada, tandis que l'utilisation du mot « devrait » renvoie à des conseils, à des directives ou à une pratique exemplaire.

1.2. Applicabilité

Le présent guide s'applique à tous les employés du GC ayant le pouvoir décisionnel en matière de gestion des risques liés à la sécurité matérielle. Le présent guide s'adresse aux chefs de service et aux dirigeants principaux de la sécurité., les gestionnaires et les praticiens de la sécurité matérielle à qui on a délégué le pouvoir de gestion des risques liés à la sécurité matérielle ou qui sont responsables de déterminer les risques liés à la sécurité matérielle aux cadres supérieurs qui ont ce pouvoir délégué. Ce document peut être appliqué aux processus d'évaluation et d'acceptation des risques liés à la sécurité physique et peut être utilisé pour créer ou mettre à jour les politiques, directives et programmes ministériels liés à la gestion des risques liés à la sécurité matérielle.

1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle

Tous les employés du gouvernement du Canada (GC) ont la responsabilité de protéger les personnes, les renseignements et les biens du GC. Il est important que les politiques et les pratiques en matière de sécurité ne servent pas d'obstacles à l'inclusion, mais soutiennent et respectent plutôt tout le personnel du GC tout en veillant à ce que les mesures de sécurité appropriées soient maintenues pour protéger le personnel, les biens et l'information du GC.

Les initiatives visant à promouvoir l'égalité et l'inclusion entre les diverses communautés et patrimoines au sein du GC devraient être respectées dans le développement et la maintenance des systèmes de sécurité matérielle. Les ministères et organismes devraient respecter toutes les lois, politiques et directives du GC sur l'équité, la diversité et l'inclusion (EDI) dans la promotion d'un milieu de travail juste et équitable pour toutes les personnes, tout en s'assurant qu'elles s'acquittent de leurs responsabilités en matière de sécurité.

Les ministères et organismes devraient mener un exercice de gestion des risques pour veiller à ce que, même si la dignité de tous est respectée, la protection des renseignements, des biens et du personnel du GC soit maintenue. Toutes les questions sur les politiques et les directives de l'EDI doivent d'abord être adressées à l'autorité ministérielle responsable.

1.4. Considérations aux technologies de l'information

Suite aux menaces qui évoluent constamment et l'intégration de la sécurité matérielle et de la technologie de l'information (TI), il est essentiel d'évaluer le risque de toute application et/ou de tout logiciel connecté à un réseau pour faire fonctionner et soutenir l'équipement dans les bâtiments contrôlés par le gouvernement du Canada.

Avant de mettre en œuvre des applications et/ou des logiciels qui contrôleront et/ou automatiseront certaines fonctions de l'immeuble, votre service de sécurité ministériel exige la réalisation d'une évaluation et d'une autorisation de sécurité (SA&A). Cela permettra de s'assurer que l'intégrité et la disponibilité des composants que les applications et/ou logiciels contrôlent sont maintenues et que tout risque mis en évidence sera atténué. Il est fortement recommandé de commencer le processus SA&A tôt afin de s'assurer que les calendriers de livraison des projets ne sont pas affectés. Pour plus d'informations sur le processus SA&A, veuillez consulter votre service de sécurité ministériel.

2. Coordonnées

Pour plus d'informations, contacter :

Gendarmerie royale du Canada
Principale organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ontario)
K1A 0R2
Courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronymes

Acronyme	Signifiant
CATV	Distribution de télévision par câble
CCSM	Comité consultatif sur la sécurité matérielle
DGS	Directive sur la gestion de la sécurité

DPS	Dirigeant principal de la sécurité
EMR	Évaluation de la menace et des risques
GSMGC	Guide de sécurité matérielle du gouvernement du Canada
PSG	Politique sur la sécurité du gouvernement
SA&A	Évaluation et autorisation de sécurité
SCT	Secrétariat du Conseil du Trésor du Canada
SMA	Sous-ministre adjoint

4. Glossaire

Terme	Définition
Accès non autorisé	Accès à des renseignements ou à des biens par un particulier qui n'a pas fait l'objet d'une enquête de sécurité du personnel exigée ou ne satisfait pas aux critères du « besoin de connaître », ou les deux.
Actif	Actifs matériels ou immatériels du gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.
Actif protégé	Actifs dont la compromission risquerait vraisemblablement de porter préjudice autre que l'intérêt national.
Incident de sécurité	Tout acte de violence en milieu de travail manifesté à l'endroit d'un employé ou tout acte, événement ou omission pouvant entraîner la compromission d'informations, de biens ou de services.
Besoin de connaître	Le principe selon lequel il est nécessaire pour une personne d'avoir accès à des renseignements et de les connaître afin de pouvoir exécuter ses tâches.
Compromis	Divulgation, destruction, suppression, modification, interruption d'accès ou utilisation de renseignements ou de biens non autorisée.
Disponibilité	Se dit de l'information utilisable sur demande au soutien des opérations, des programmes et des services.
Divulgation non autorisée	Événement donnant lieu à l'exposition d'un matériel ou à la divulgation de renseignements à des personnes non autorisées à y accéder.
Installation	Lieu physique utilisé dans un but particulier. On entend par installation une partie ou la totalité d'un immeuble, soit un immeuble, son emplacement et ses alentours, ou encore une construction qui n'est pas un immeuble. Le terme désigne non seulement l'objet même, mais aussi son usage (p. ex. champs de tir, terres agricoles).
Intégrité	L'exactitude et l'intégralité des biens, et l'authenticité des transactions.

Intérêt national	Concerne la défense et le maintien de la stabilité sociale, politique et économique du Canada.
Menace	Événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services.
Procédures Opérationnelles Normalisées	Un ensemble d'instructions écrites décrivant les mesures étape par étape à prendre pour accomplir une ou des tâches ou intervenir en cas d'incident. Les PON visent à normaliser le rendement et à compenser tout manque de connaissances ou d'expérience.
Risque résiduel	Niveau restant de risque lié à la sécurité après la mise en œuvre de mesures de sécurité et d'autres mesures d'atténuation des risques.
Risque résiduel projeté	Le risque prévu après la mise en œuvre complète des recommandations et des mesures de protection proposées.
Surveillance	Pour surveiller ou détecter une faille de sécurité.
Surveillance continue	Surveillance sur une base continue pour confirmer qu'il n'y a pas eu infraction à la sécurité.
Vulnérabilité	Insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou au préjudice.
Énoncé des risques	Description un événement et ses répercussions potentielles (positives ou négatives) sur la réalisation des objectifs de l'organisation.
Évaluation de la sécurité	Le processus d'évaluation des pratiques et des contrôles de sécurité ayant pour but d'établir la mesure dans laquelle ils sont mis en œuvre correctement, fonctionnent comme prévu et produisent les résultats souhaités en ce qui concerne le respect des exigences établies en matière de sécurité.
Évaluation des menaces et des risques	Processus d'évaluation des biens d'une installation, des menaces qui pèsent sur eux et du rendement des mesures de protection contre ces menaces, visant à définir les risques.
Évaluation et autorisation de sécurité	La composante d'évaluation de la sécurité de l'ESA vise à vérifier si les exigences de sécurité établies pour un système ou un service particulier sont respectées et si les contrôles et les mesures de protection fonctionnent comme prévu. L'objectif de la composante d'autorisation de l'ESA est de signifier que la direction a accepté le risque résiduel d'exploitation du système ou du service et a autorisé son utilisation en s'appuyant sur la preuve.

5. Processus décisionnel fondé sur le risque

La connaissance du risque consiste à comprendre la relation entre la probabilité qu'un événement se produise, les niveaux possibles de dommages associés à chaque événement et le préjudice causé aux biens, au personnel et/ou aux produits livrables en cas d'événement. Il est essentiel que les décideurs comprennent parfaitement ces facteurs lorsqu'ils prennent des décisions qui pourraient avoir une incidence sur la sécurité matérielle des biens et des fonctions essentielles de leur ministère ou organisme. Avoir des processus formalisés et documentés, liés à la gestion du

risque, est essentiel pour atteindre cet objectif de sécurité matérielle ; les décideurs à tous les niveaux n'auront pas le temps d'examiner et d'analyser les données, dans leur intégralité, lors d'un événement ou d'une crise. Cela permettra également de mieux cerner les vulnérabilités dans l'appareil de sécurité physique d'un ministère ou d'un organisme et d'accélérer les mesures correctives.

Conformément à la section 4.6.3 du DGS, les personnes désignées par l'administrateur général doivent également communiquer aux ministères clients les pratiques et les contrôles de sécurité qui ont été mis en œuvre pour répondre aux exigences de sécurité définies, les conditions de sécurité qui doivent être en place dans l'environnement du client, les risques résiduels restants et les mesures d'atténuation recommandées.

Cadre stratégique de gestion du risque fournie des directives aux administrateurs généraux sur la mise en œuvre de pratiques efficaces de gestion du risque à tous les niveaux de leur organisation, assurant ainsi la conformité au DGS. Cela appuie l'établissement de priorités stratégiques et des décisions éclairées en matière de tolérance au risque.

Une gestion efficace des risques au gouvernement fédéral devrait :

- Appuyer les priorités pangouvernementales;
- Être adaptés au mandat, aux priorités, à la culture du risque et aux intérêts des intervenants du ministère ou des organismes;
- Atteindre un équilibre entre la réponse aux risques/les contrôles établis et le soutien de la flexibilité/innovation pour améliorer les résultats;
- Être transparent, intégré et systématique;
- Améliorer continuellement la culture, la capacité et la capacité de gestion des risques; et
- Ces principes devraient influencer et guider le processus décisionnel lors de l'élaboration et de la mise en œuvre des procédures opérationnelles normalisées (PON) et des politiques du ministère et de l'organisme.

Lorsqu'il est correctement mis en œuvre, le Cadre stratégique de gestion du risque aide à s'assurer que les mesures de sécurité matérielle sont correctement évaluées, mises en œuvre, surveillées et maintenues conformément à la politique et aux directives du SCT. Le cadre donne aux administrateurs généraux le pouvoir d'intégrer la sécurité de manière à s'assurer que les biens dont ils ont la garde sont entièrement protégés et permettent une culture d'amélioration continue et de vigilance à l'égard de tous les aspects de la sécurité, y compris la sécurité matérielle.

Une culture axée sur le risque consiste à faire en sorte qu'un ministère ou un organisme, dans son ensemble, comprenne l'importance de toutes les activités de gestion du risque et permette aux employés de participer ouvertement au processus de gestion du risque. Les dirigeants ministériels sont encouragés à favoriser ce développement culturel en collaborant régulièrement avec le personnel, en étant disponibles pour former et encadrer leurs équipes et en donnant l'exemple par leurs propres mesures de sécurité et de sensibilisation aux risques. Le soutien de la responsabilisation favorise également une culture axée sur le risque, encourage la diligence raisonnable dans toutes les tâches de gestion du risque et, lorsqu'il encourage les employés à améliorer ces compétences, peut promouvoir un engagement à l'égard de la sensibilisation au

risque dans leur perfectionnement professionnel.

Il existe des cours obligatoires sur la sécurité pour tous les employés du gouvernement, mais il est préférable d'élargir ces possibilités d'apprentissage. Ceci peut être réalisé par :

- Programmes de mentorat;
- Tables rondes;
- Formation propre au ministère ou à l'organisme; et
- Intégration de la sensibilisation à la sécurité dans les séances de perfectionnement et d'intégration régulières.

Le Guide de gestion intégrée du risque couvre un large éventail de sujets liés à la gestion des risques, y compris des domaines qui correspondent directement aux processus de gestion des risques propres à la sécurité physique et qui les renforcent. Consultez ce guide pour un examen plus approfondi du processus de gestion intégrée du risque.

6. Processus d'évaluation et d'acceptation des risques

L'environnement de sécurité matérielle d'un ministère ou d'un organisme doit faire l'objet d'une évaluation officielle, périodique, par un membre auquel est délégué le pouvoir de prendre des décisions concernant les risques pour la sécurité matérielle (voir 8.1.1. Exemple de matrice de délégation). Dans les cas où ce risque dépasse son pouvoir d'acceptation, la décision doit être transmise à l'échelon supérieur (voir 8.2.1. Exemple d'organigramme de transmission hiérarchique).

Il y aura des occasions où une base de référence établie ne peut être raisonnablement atteinte. Ces circonstances peuvent découler de contraintes de temps, de complications géographiques ou d'obstacles juridiques ou législatifs. La décision d'accepter tout risque, y compris les risques pour la sécurité physique, ne doit pas être prise à la légère et, dans l'exercice de la diligence raisonnable, l'enquête sur toutes les solutions de rechange pour atténuer le risque doit d'abord être terminée.

Il est recommandé que chaque ministère élabore une approche normalisée pour évaluer et accepter le risque lié à la sécurité matérielle qui s'harmonise avec ses processus existants. Chacune des sept phases d'une EMR, décrites ci-dessous, doit être comprise et prise en compte par le responsable du risque lorsqu'il évalue et accepte tout risque pour la sécurité matérielle. Il y a sept phases à une EMR qu'une autorité d'acceptation des risques doit comprendre avant d'affecter une équipe à une EMR.

6.1. Préparation

La phase de préparation déterminera la portée de l'évaluation et le niveau acceptable de risque résiduel. La portée de l'évaluation devrait être déterminée par un employé ayant le pouvoir de gérer les risques pour la sécurité matérielle afin de déterminer quels biens seront évalués dans l'EMR. L'autorité de gestion des risques liés à la sécurité matérielle devrait également attribuer l'évaluation à une équipe qualifiée de praticiens de la sécurité. Au cours de cette phase, le chef d'équipe de l'EMR devrait recevoir suffisamment de renseignements pour créer un plan de travail décrivant les principaux produits livrables à chaque étape ainsi que les ressources

nécessaires pour effectuer une EMR. Une fois qu'un plan de travail est terminé, il doit être examiné pour s'assurer qu'il respecte le budget, qu'il respecte les délais et que le personnel demandé peut être affecté au projet. Si le plan de travail de l'EMR est acceptable, la direction doit documenter son approbation et demander à l'équipe de commencer l'évaluation.

6.2. Identification et évaluation des actifs

La phase d'identification et d'évaluation des biens identifiera tous les biens visés par l'EMR (biens classifiés, armes à feu, biens pour un projet particulier). Le temps et les ressources ne devraient pas être consacrés aux biens qui ne font pas partie de l'EMR, à moins qu'il y ait des interdépendances liées aux biens pertinents. Tous les biens qui respectent les paramètres désignés à la phase de préparation doivent être clairement énumérés et une valeur doit leur être attribuée. Il y a plusieurs catégories que chaque actif peut avoir notées de très faible à très élevée; la catégorie de notation la plus élevée doit être identifiée dans la liste. Les catégories sont les suivantes.

6.2.1. Confidentialité

Dans quelle mesure cette information serait-elle compromise? L'agrégation de données moins sensibles pourrait augmenter la valeur de ce score.

6.2.2. Disponibilité

Combien de dommages seraient causés si ce bien était rendu inaccessible au personnel ou aux clients?

6.2.3. Intégrité

Combien de dommages pourraient être causés si l'actif était modifié et rendu inexact, frauduleux ou incomplet?

6.2.4. Coût de remplacement

Combien en coûterait-il pour remplacer l'actif? Cette valeur devrait être indiquée à côté de la valeur la plus élevée ci-dessus.

Le livrable pour cette phase est un tableau d'évaluation de l'actif/État de sensibilité.

6.3. Évaluation de la menace

La phase d'évaluation des menaces identifiera et énumérera toutes les menaces réelles et potentielles auxquelles le bien peut être confronté de manière réaliste dans le cadre de l'EMR (agence de renseignement hostile, crime organisé, accidents, catastrophes naturelles). Les menaces doivent être répertoriées et associées à un niveau de menace allant de très faible à très élevé. Cette valeur est déterminée par la probabilité d'un événement et la gravité de la menace. Lors de la détermination de la gravité de la menace, des calculs doivent être effectués pour les catégories suivantes :

6.3.1. Pertes de vie potentielles

Y a-t-il un risque pour la vie? Combien de victimes pourrait-on s'attendre à un événement?

6.3.2. Disponibilité opérationnelle

Cette menace aura-t-elle pour effet de réduire ou de cesser la capacité du ministère ou de l'organisme d'accomplir sa mission? Dans quelle mesure la mission est-elle essentielle? Combien de temps faudra-t-il pour retrouver la capacité opérationnelle?

6.3.3. Coût économique

Combien d'argent faudra-t-il pour récupérer de l'événement (main-d'œuvre, réparation/remplacement, perte de revenus)? Combien de titres pourraient être irrémédiablement perdus (espèces, métaux précieux, obligations au porteur)?

6.3.4. Réputation

Un événement aura-t-il une incidence négative sur la confiance des intervenants envers le ministère ou l'organisme? Un événement nuirait-il à la réputation d'un client en raison des biens qu'il a confiés au ministère ou à l'organisme?

Une fois que les niveaux de menace ont été calculés, selon la méthodologie utilisée, ils doivent être utilisés pour créer le livrable de cette phase : une liste des menaces prioritaires.

6.4. Évaluation de la vulnérabilité

À la phase d'évaluation de la vulnérabilité, l'équipe d'EMR évaluera les mesures de protection existantes, ou leur absence, et déterminera la vulnérabilité du bien par rapport à la menace identifiée, en fonction de paramètres prédéterminés définis pour tous les membres de l'équipe qui effectuent l'évaluation. L'équipe d'EMR mesurera la probabilité de compromission et la gravité du résultat de faible à élever. L'absence de mesures de protection est une cote élevée automatique, qui sert ensuite à calculer le niveau de vulnérabilité de très faible à très élevé. Une fois que toutes les vulnérabilités du champ d'application de l'EMR ont été évaluées, elles peuvent être compilées dans une liste de vulnérabilités prioritaires pour le livrable de cette phase.

6.5. Simulation des risques résiduels

Les résultats des trois phases précédentes peuvent ensuite être utilisés pour calculer le risque résiduel. Il peut y avoir plus d'un score de risque résiduel pour chaque actif, car certains sont soumis à de multiples menaces et vulnérabilités. Ils seront tous calculés individuellement et se verront attribuer leur propre côté de risque résiduel. Le risque résiduel est un calcul numérique qui donnera un score de très faible à très élevé. Cette cote correspond au niveau de risque acceptable indiqué à la phase un de l'EMR. Les résultats seront identiques, peu importe la méthode utilisée. Le livrable de cette phase est terminé lorsque l'équipe compile les noyaux de risques résiduels dans une liste des risques résiduels prioritaires.

6.6. Recommandations

La phase de recommandation contient la comparaison effectuée par l'équipe d'EMR des risques calculés par rapport au niveau de risque acceptable, déterminé à la phase de préparation. Pour les risques résiduels qui se situent au niveau cible ou en deçà de celui-ci,

l'équipe recommandera soit de maintenir le statu quo, soit d'ajuster les mesures de protection en fonction de la tolérance au risque. Dans le cas où ils recommandent de réduire ou de supprimer la garantie, ils doivent recalculer le risque résiduel pour la proposition pour l'autorité désignée. Dans tous les cas où le risque résiduel dépasse le niveau acceptable, l'équipe d'EMR proposera d'autres mesures pour ramener le risque résiduel au niveau acceptable. L'autorité désignée peut alors examiner toutes les mesures de protection proposées et le coût de leurs ressources et déterminer si elle mettra en œuvre une ou plusieurs mesures, ou refuser et accepter officiellement le risque résiduel de base ci-dessus.

6.7. Conclusion

La phase finale de conclusion est celle où l'équipe de l'EMR résumera toutes les données contenues dans le rapport, comme un résumé. Les DPS, ou leurs délégués devraient disposer de suffisamment d'informations pour comprendre l'intégralité du rapport et pouvoir trouver des informations supplémentaires pour tout calcul de suivi. Seront également incluses les décisions de la direction d'accepter ou de refuser les mesures de protection recommandées, de maintenir, d'augmenter ou de réduire les mesures de protection existantes, ainsi qu'une signature officielle reconnaissant ces décisions et l'authenticité du rapport. Ce processus sera terminé seulement après que l'DPS ou son délégué aura signé le rapport d'EMR.

Pour obtenir de plus amples renseignements sur l'EMR dans le contexte du gouvernement du Canada, consultez le GSMGC-022 Guide d'évaluation de la menace et des risques.

7. Intégration des contre-mesures

Après avoir déterminé les mesures de protection et la posture de sécurité matérielle appropriées pour un ministère ou un organisme, ces fonctions devront être intégrées aux tâches quotidiennes du personnel pour s'assurer qu'elles sont les plus efficaces. Il est contre-productif d'avoir des systèmes de sécurité matérielle mis en place en tant qu'entité distincte des opérations quotidiennes; la protection des actifs est une fonction essentielle des opérations et elle devrait être priorisée en tant que telle. La nécessité de documenter, d'examiner et de mettre à jour les mesures de sécurité matérielle devrait être liée aux fonctions opérationnelles de l'actif ou du service. Dans la mesure du possible, l'intégration de l'examen de la garantie de sécurité matérielle dans les fonctions opérationnelles répétées, comme les vérifications trimestrielles, améliorera la synergie des deux fonctions. Un autre avantage d'une stratégie d'intégration bien planifiée est de s'assurer que l'examen a le temps nécessaire pour être fait complètement et avec une diligence raisonnable, ce qui réduit le risque qu'il soit précipité à l'approche des échéances.

7.1. Élaboration de normes et de procédures

Les normes de sécurité des ministères et des organismes doivent appuyer l'adoption de processus intégrés, en veillant à ce qu'il y ait une surveillance et une documentation décrivant clairement les attentes de la haute direction, ainsi qu'en normalisant la façon dont les données sont recueillies, analysées et tenues à jour. Il y a plusieurs considérations qui devraient être incluses dans une norme; bien que la version finale varie considérablement d'un cas à l'autre. Il est conseillé que ces normes indiquent clairement quels postes sont responsables de quels

processus et comment les données seront enregistrées et respectées. Par exemple, le personnel de bureau peut être tenu de signaler l'état des verrous de câble qui fixent les ordinateurs portables lors de la signature de l'équipement. Le gestionnaire de l'unité peut ensuite examiner les registres et vérifier l'inventaire tous les trimestres; compiler un rapport sur l'efficacité et l'état des mesures de protection (Exemple : Aucun inventaire non comptabilisé, usure mineure de trois serrures nécessitant une attention, mesure de sauvegarde jugée efficace sans changement conseillé).

Il est conseillé que les rapports finaux de toutes les mesures de contrôle et de sauvegarde atteignent un point unique, tels que le DPS ou le membre d'équipe délégué. L'intégration de cette méthode serait plus efficace si elle suivait une chaîne de possession préétablie, comme le modèle interne d'escalade/délégation. Plus il y a de cohérence entre les processus, plus il sera facile pour le personnel de les parcourir tous. Cela augmenterait l'efficacité des contre-mesures utilisées, tout en favorisant un processus reconnu et une culture positive des risques pour la sécurité physique.

8. Délégation des responsabilités en matière de gestion des risques

Les personnes désignées ayant des rôles et des responsabilités clés en matière de sécurité en vertu de la section 4 du DGS peuvent, avec l'approbation de l'administrateur général, déléguer ces rôles, à condition que la diligence raisonnable et la surveillance soient exercées dans chaque fonction et tâche. Cela peut améliorer l'efficacité lorsque des tâches déléguées sont assignées aux membres appropriés qui ont une compréhension de niveau opérationnel des mesures de sécurité matérielle et des biens impliqués dans leur domaine de responsabilité. Une stratégie de délégation mal mise en œuvre, ou un manque de surveillance peuvent avoir l'effet inverse; laissant des lacunes dans les rapports, l'escalade et exposant les ministères et organismes à des vulnérabilités et des responsabilités inutiles. Une stratégie de délégation claire et propice aide le personnel à s'acquitter de ses responsabilités en matière de gestion des risques pour la sécurité matérielle. Voici les pratiques exemplaires pour la stratégie et la culture en matière de sécurité matérielle d'un ministère ou d'un organisme.

8.1. Normalisation de la délégation des responsabilités

Une stratégie de délégation normalisée est prescrite par la PSG et appuie la communication des données essentielles à la haute direction pour éclairer ses décisions en matière de gestion des risques liés à la sécurité matérielle. Les ministères et organismes sont autorisés à élaborer un processus de délégation pour tous les rôles de gestion des risques pour la sécurité qui conviennent à leur environnement opérationnel unique au sein du GC. L'élaboration d'un profil de risque ministériel fournira un aperçu stratégique des biens et des fonctions qui nécessitent une protection et déterminera quelles responsabilités en matière de gestion des risques pour la sécurité physique peuvent être déléguées.

Idéalement, la délégation de la surveillance de la gestion des risques liés à la sécurité matérielle devrait être accordée en priorité aux personnes qui participent déjà à la supervision de la

gouvernance de la sécurité du Ministère. Avec une préférence accordée aux membres du personnel qui ont une expérience ou une formation antérieure en sécurité matérielle. Un niveau de formation de base devrait être fourni à tous les membres du personnel qui ont été délégués pour assumer des responsabilités en matière de gestion des risques afin de s'assurer qu'ils peuvent exécuter correctement les fonctions requises. Il faut également tenir compte de la structure organisationnelle préexistante et, si possible, les tâches déléguées devraient utiliser la même configuration. Cela permet d'intégrer le processus global de délégation de la gestion des risques liés à la sécurité matérielle dans la structure du ministère ou de l'organisme et de s'assurer que le personnel connaît les voies de communication appropriées pour l'approbation des différentes demandes et tâches.

8.1.1. Exemple de matrice de délégation

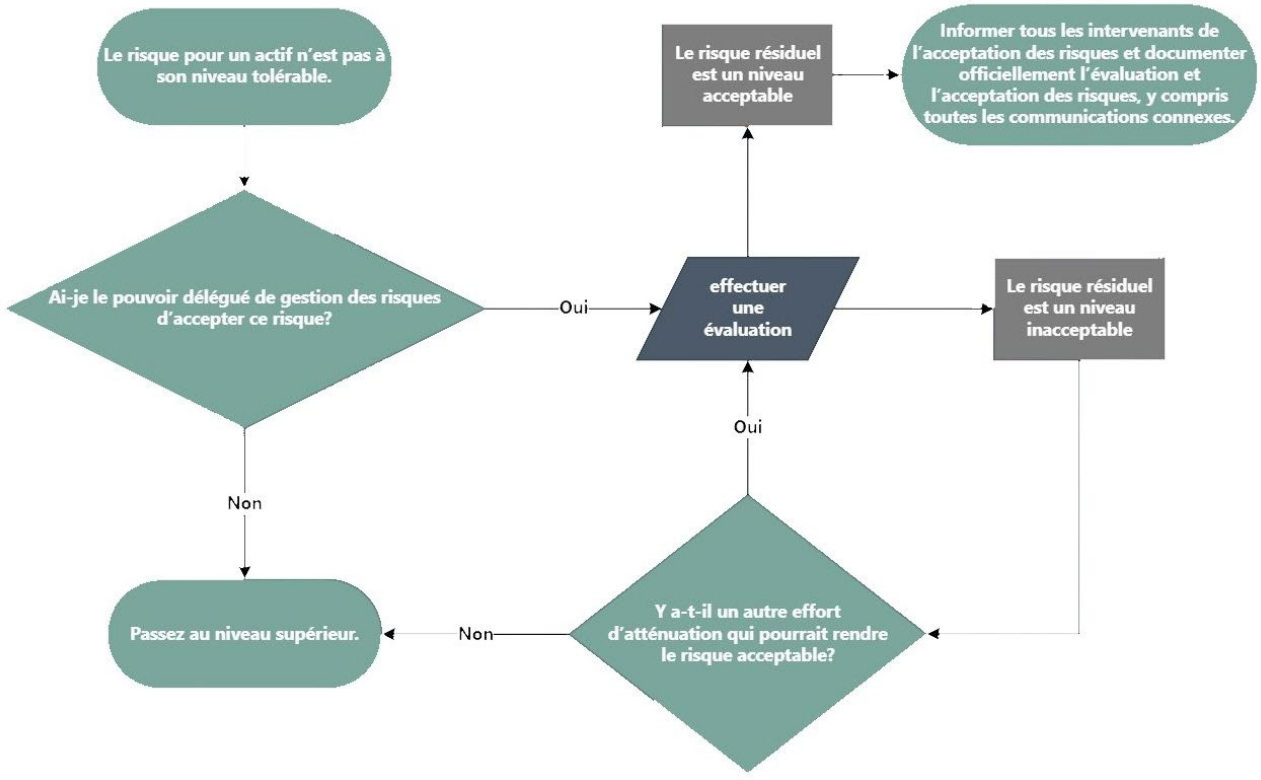
Exemple actions de tache	Niveaux de Gestion (NG)					
	NG 0	NG 1	NG 2	NG 3	NG 4	NG 5
Administrateur général/commissaire	**NG 0**	**NG 1**	**NG 2**	**NG 3**	**NG 4**	**NG 5**
Dirigeant principal de la sécurité (DPS)	**NG 0**					
Approuver les directives et les normes liées à la sécurité	**NG 0**	**NG 1**	**NG 2**			
Approuver la délégation des risques (NG 2- NG 5)	**NG 0**	**NG 1**	**NG 2**			
Approuver les procédures et les lignes directrices liées à la sécurité	**NG 0**	**NG 1**	**NG 2**	**NG 3**		
Approuver les contrôles de sécurité physique (contrôle d'accès, CCTV)	**NG 0**	**NG 1**	**NG 2**	**NG 3**		
Approuver les écarts à risque élevé par rapport aux normes de sécurité matérielle	**NG0**	**NG 1**				
Approuver les écarts à risque moyen par rapport aux normes de sécurité matérielle	**NG 0**	**NG 1**	**NG 2**	**NG 3**		
Approuver les écarts à fiable risque élevé par rapport aux normes de sécurité matérielle	**NG 0**	**NG1**	**NG 2**	**NG 3**	**NG 4**	
Approuver les exigences, les pratiques et les plans de sensibilisation à la sécurité et de formation	**NG 0**	**NG 1**	**NG 2**	**NG 3**	**NG 4**	
Soumettre une demande pour accepter un risque		**NG 1**	**NG 2**	**NG 3**	**NG 4**	**NG 5**

Level	Employee Positions
NG 0	Administrateur général/commissaire
NG 1	SMA, directeur général, DPS (relevant de l'administrateur général)
NG 2	Directeurs régionaux, DPS/ADPS, gestionnaires régionaux (relevant du niveau un)
NG 3	Gestionnaires régionaux, gestionnaires (relevant d'un niveau deux)
NG 4	Gestionnaires ou superviseurs (relevant d'un niveau trois)
NG 5	Gestionnaires ou superviseurs (relevant d'un niveau quatre)

8.2. Normalisation de la transmission hiérarchique des rapports/ incidents de sécurité

Il incombe à tous les employés du GC de communiquer en temps opportun les incidents de sécurité aux décideurs responsables ou de les transmettre à un niveau supérieur. Le fait de ne pas remonter la situation correctement peut avoir des répercussions catastrophiques sur les objectifs opérationnels d'un ministère ou d'un organisme et nuire à leur image aux yeux des intervenants. Chaque ministère et organisme doit avoir des processus pour la transmission hiérarchique et la documentation des atteintes à la sécurité et des incidents, conformément à l'annexe G du DGS, lorsqu'une évaluation officielle des menaces et des risques peut ne pas être justifiée. Lors de la normalisation d'un processus d'escalade, il doit suivre les mêmes canaux que le processus de délégation, jusqu'au niveau qui a le pouvoir d'intervenir en cas d'incident. La personne pour qui le processus d'escalade prendra fin dépendra en grande partie de la gravité de l'incident et de l'autonomie accordée à chaque niveau par la direction. Une taxonomie des risques peut fournir une liste des menaces les plus probables ou les plus dommageables auxquelles chaque bien protégé peut faire face. Ces risques peuvent ensuite être liés à un poste dans l'organigramme de délégation qui a le pouvoir de donner suite à une intervention. Les incidents qui pourraient avoir des niveaux de gravité variables devraient clairement définir les seuils de transmission à un niveau supérieur au niveau standard établi par la matrice du ministère ou de l'organisme.

8.2.1. Exemple d'organigramme de transmission hiérarchique



Alt texte : L'image ci-dessus montre un exemple d'organigramme de processus d'escalade

9. Guides et outils

Divers ministères et organismes du GC ont élaboré des outils qui s'appliquent à la gestion des risques liés à la sécurité matérielle. Il est essentiel de comprendre les outils disponibles et leur applicabilité pour concevoir et maintenir un programme de sécurité matérielle efficace. Les publications suivantes peuvent être utilisées conjointement avec les conseils contenus dans ce guide.

9.1. Guide de gestion intégrée du risque

Le Guide de gestion intégrée du risque vise à aider les ministères et les organismes à renforcer leurs pratiques globales de gestion intégrée du risque. Le Guide de gestion intégrée du risque ne fournit pas de pratiques précises de gestion du risque lié à la sécurité matérielle, car celles-ci seront propres à chaque organisation selon son mandat unique, son exposition au risque, sa capacité de gestion du risque et d'autres facteurs. Il appuie une approche globale de la gestion de tous les risques, y compris les risques pour la sécurité matérielle, pour les ministères et les organismes.

9.2. Guide d'élaboration d'un profil de risque organisationnel

Un Guide des profils de risque ministériels permet aux ministères et organismes d'obtenir un aperçu de leurs principaux risques, y compris une compréhension du contexte opérationnel et des objectifs en matière de gestion des risques. Un profil de risque ministériel est un résultat du processus d'évaluation des risques qui améliore la capacité de la haute direction d'analyser, de hiérarchiser et de budgétiser sa stratégie de gestion des risques. Ils peuvent également servir à fournir un aperçu clair des principaux risques et des efforts d'atténuation du ministère ou des organismes au personnel, aux praticiens et aux intervenants. Un profil de risque ministériel appuie l'établissement de priorités stratégiques, permet une prise de décisions éclairée et démontre le niveau de tolérance au risque d'un ministère ou d'un organisme.

9.3. Guide sur les taxonomies des risques

Le Guide de taxonomie des risques est un ensemble complet, commun et stable de catégories de risque utilisées au sein des ministères et organismes. Ce document comprend des considérations pour l'élaboration et l'utilisation d'une taxonomie des risques. Il décrit une approche de catégorisation et de regroupement des risques qui peut être adaptée aux besoins particuliers d'un ministère ou d'un organisme. Les taxonomies des risques appuient la normalisation des systèmes et contribuent à favoriser une culture de sensibilisation aux risques. Les taxonomies des risques et leurs tâches complémentaires sont importantes pour développer une culture de « sensibilisation aux risques » en permettant une terminologie et une compréhension standard par les employés.

9.4. Guide sur les énoncés de risque

Le Guide des énoncés de risque vise à renforcer les pratiques de gestion des risques en élaborant des énoncés de risque. Les énoncés de risque sont une composante essentielle de la définition des menaces et des possibilités identifiées, qui sont fondamentales pour appuyer le

processus de gestion des risques. Une présentation normalisée des énoncés de risque améliore l'intégration des processus de sécurité dans l'ensemble d'un ministère ou d'un organisme.

9.5. Modèle de la capacité en matière de gestion des risques

Le modèle de capacité de gestion du risque est un outil de diagnostic qui permet aux ministères et aux organismes de comparer leur capacité actuelle de gestion du risque. Cet outil peut servir à lancer une discussion éclairée sur la question de savoir si des ressources doivent être affectées ou détournées pour combler les lacunes en matière de gestion des risques ou pour améliorer la capacité dans des secteurs clés des priorités de gestion des risques du ministère ou de l'organisme.

9.6. Publications des Principal organisme responsable de la sécurité matérielle de la GRC

La POSM de la GRC, mandatée par le SCT, publie et gère un catalogue de documents d'orientation couvrant des domaines précis de la sécurité matérielle. Ces documents tirent parti des commentaires professionnels d'experts en la matière dans de nombreux domaines et sont examinés par les pairs par la collectivité de la sécurité matérielle du GC afin d'intégrer les leçons apprises et les pratiques exemplaires de l'ensemble du GC. Il vaut la peine d'examiner ces publications pour déterminer s'il y a des répercussions sur le risque pour la sécurité matérielle d'un ministère ou d'un organisme, surtout lorsqu'on envisage de modifier des installations existantes ou d'en aménager de nouvelles.

10. Surveillance continue de l'atténuation des risques

Une surveillance adéquate et la production de rapports sur les mesures de protection sont des éléments essentiels d'une stratégie efficace de gestion des risques pour la sécurité matérielle et garantissent le respect des obligations législatives au sein du GC. Les plans de sécurité doivent être surveillés régulièrement pour déterminer si la stratégie d'atténuation des risques pour la sécurité matérielle maintient toujours un niveau acceptable de risques résiduels pour les biens dans un environnement de menace dynamique. Si l'efficacité des mesures d'atténuation utilisées devient douteuse, en raison d'un changement des facteurs de risque ou des ressources disponibles, une EMR officielle peut être justifiée pour déterminer les modifications nécessaires à la stratégie d'atténuation.

10.1. Importance de la surveillance continue

En plus de la surveillance obligatoire des stratégies d'atténuation des risques de sécurité matérielle et des mesures de protection de la sécurité matérielle, un système normalisé de surveillance continue permet au personnel de comprendre son rôle dans l'atténuation des risques de sécurité physique pour l'organisation. Une documentation claire et concise décrivant la stratégie de surveillance, ainsi que des données sur les résultats et des examens périodiques, fournit des informations précieuses dans une enquête post-compromission. Plus les données collectées seront claires, plus il sera facile d'identifier la panne du système qui a permis d'exploiter une vulnérabilité.

La surveillance continue facilite la réduction des méfaits et la capacité de cerner de façon proactive les possibilités d'accroître la sécurité physique du personnel et des biens. Lorsque cet examen comprend l'examen des nouvelles pratiques exemplaires des partenaires de l'industrie et d'autres ministères et organismes gouvernementaux, de nouvelles stratégies d'atténuation peuvent être adoptées pour les mesures de protection existantes. Cela peut entraîner une augmentation des mesures de sécurité physique, une amélioration de l'efficacité opérationnelle, des économies de coûts potentielles et une amélioration du recouvrement.

10.2. Évaluation périodique

Des normes d'évaluation devraient être établies avec des délais clairs pour que les données soient entièrement compilées, lorsque l'examen et l'analyse des données auront lieu, puis lorsque les résultats seront disponibles. Un examen annuel du plan de sécurité ministériel ou du plan de travail annuel sur la sécurité matérielle d'un ministère ou d'un organisme devrait être effectué; toutefois, les ministères et organismes auraient avantage à établir leurs propres cibles qui :

- Permettre que les données obligatoires soient prêtes à l'avance; et
- Examiner leurs propres politiques et procédures afin d'évaluer proactivement leurs initiatives et d'assurer leur conformité.

Bien que certains délais ne soient pas négociables, bon nombre de ceux qui permettent une certaine souplesse peuvent être liés à des délais opérationnels afin d'encourager l'efficacité opérationnelle et la synergie avec des jalons préétablis. Lorsque la sécurité matérielle est intégrée aux exigences opérationnelles, elle permet une évaluation efficace de l'ensemble de la posture de gestion des risques d'un ministère ou d'un organisme.

10.3. Élaboration de mesures du rendement en matière de sécurité physique

Le rendement en matière de sécurité physique devrait être mesuré dans le cadre de l'évaluation périodique pour s'assurer qu'ils demeurent efficaces et qu'ils atteignent toujours l'objectif. Les mesures de rendement varieront entre les garanties et devront être personnalisées en fonction des évaluations effectuées par les praticiens de la sécurité physique. Au moment de décider de la façon de mesurer l'efficacité d'une sauvegarde, plusieurs considérations clés devraient influencer la décision :

- Quel est l'objectif par la mesure de protection?
- Comment la sauvegarde s'intègre-t-elle dans les fonctions opérationnelles;
- La sauvegarde assure-t-elle le suivi des données ou produit-elle un enregistrement; et
- La mesure de protection est-elle excessive et risque-t-elle d'être contournée par le personnel?

D'autres indicateurs à surveiller peuvent comprendre des changements radicaux dans les données observées, ce qui pourrait indiquer ce qui suit :

- Sous-déclaration des incidents;
- Les nouvelles techniques d'exploitation utilisées contre les vulnérabilités; et
- Non-respect des procédures en vigueur.

Bien qu'il ne soit pas toujours négatif, l'absence d'incidents mineurs peut indiquer que la mesure de protection est inefficace; toutefois, cette seule mesure ne devrait pas être considérée comme une preuve, mais peut indiquer qu'une enquête pour confirmer les données est justifiée.

11. Références et documents connexes

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Directive sur l'obligation de prendre des mesures d'adaptation
- Instrument de délégation et de responsabilisation en matière de nomination
- Cadre stratégique de gestion du risque
- Guide de gestion intégrée du risque
- Cadre stratégique sur la gestion de la conformité
- Guide d'élaboration d'un profil de risque organisationnel
- Guide sur les taxonomies des risques
- Guide sur les énoncés de risque
- Méthodologie harmonisée d'EMR (TRA-1)
- Modèle de la capacité en matière de gestion des risques
- Guides sur la sécurité matérielle du gouvernement du Canada
- Ligne directrice à l'intention des employés fédéraux : Rudiments de la gestion de l'information
- Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale
- Guide à l'intention des employés deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale

12. Promulgation

Examiné et recommandé aux fins d'approbation.

J'ai examiné et recommande par la présente, GSMGC-018 (2024) Guide du processus de gestion des risqués pour la sécurité matérielle pour approbation.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2024.03.26 12:08:30 -04'00'

Shawn Nattress, Date
Gestionnaire
Principale Organisme Responsable de la Sécurité Matérielle, GRC

Approuvé

J'approuve par la présente GSMGC-018 (2024) Guide du processus de gestion des risqués pour la sécurité matérielle.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.03.26 15:20:04 -04'00'

André St-Pierre, Date
Directeur, Sécurité Matérielle
Gendarmerie royale du Canada