Guide d'Évaluation des Menaces et des Risques

GSMGC-022 (2025)

Préparé par :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
DG, 73, promenade Leikin, Ottawa (Ontario) K1A 0R2

Date de publication : 2025-01-15
Date de mise à jour :

Avant-propos

GSMGC-022 - Guide d'évaluation des menaces et des risques, est une publication NON CLASSIFIÉE, publiée sous l'autorité de la Direction de la sécurité matérielle de la Gendarmerie royale du Canada (GRC).

Il s'agit d'une publication du gouvernement du Canada et sert comme guide complémentaire pour le cours de développement professionnel en Évaluation des Menaces et des Risques (EMR) du POSM de la GRC, mais il peut également être utilisé pour débuter l'initiation et l'achèvement d'un EMR pour les organismes et les employés du gouvernement du Canada.

Les suggestions de modifications et autres renseignements peuvent être envoyés par courriel au POSM-GRC à l'addresse : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Date d'entrée en vigueur

La date d'entrée GSMGC-022 - Guide d'Évaluation des Menaces et des Risques est 2025-01-15

Registre des modifications

N° de modification	Date	Auteur	Sommaire des modifications

Remarque : Le responsable des modifications est le Principal Organisme Responsable de la Sécurité Matérielle de la Gendarmerie royale du Canada (POSM GRC).

Table des matières

1. Introduction

La GRC, en tant que principal organisme responsable de la sécurité matérielle (POSM) pour le gouvernement du Canada (GC), est chargée de fournir des conseils et des orientations sur toutes les questions concernant la sécurité matérielle.

1.1. Objectif

Ce document a pour objet de servir comme guide complémentaire au cours d'Évaluation des Menaces et des Risques (EMR) des agents de la GRC et de fournir aux employés du GC des conseils sur l'exécution d'une EMR en matière de sécurité matérielle. Ce document est designé aux employés qui dirigent ou participe à une équipe d'EMR, et il explique les sept phases principales du processus d'EMR. Ce guide fournira des connaissances de base sur le processus d'EMR, habilitera les employés à effectuer des évaluations approfondies et complètes et fournira des rapports complets aux décideurs.

1.2. Application

Ce guide s'applique aux employés du GC et s'applique aux membres chargés de diriger ou de participer à une EMR. Le guide couvre les concepts de base des sept phases d'une EMR. Des exemples sont donnés dans ce document pour des études de méthodologies d'EMR spécifiques, mais peuvent être remplacés par l'équipe d'EMR à sa discrétion. Ce guide est conçu pour être un document de soutien au cours de dévlopement professionnel de l'EMR du PORS de la GRC, mais il peut être utilisé pour appuyer une compréhension fonctionnelle du processus d'EMR.

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 départements 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 départments 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 Liées à la Technologie 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. Quelques examples de ces systèmes de contrôle peuvent inclure mais ne se limite pas à l'éclairage de sécurité, des portes périphériques, système HVAC, etc.

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 au niveau de département exige la réalisation d'une Évaluation et d'une Autorisation de Sécurité (E&AS). 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 E&AS tôt afin de s'assurer que les calendriers de livraison des projets ne sont pas affectés. Pour plus d'informations sur le processus E&AS, 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. Acronyms

Acronym	Définition
AC	Autorité compétente
CIDV	Confidentiaqlité, intégrité, disponibilité et valeur
DGS	Directive sur la gestion de la sécurité
DPS	Dirigeant principal de la sécurité
E&AS	Évaluation et d'une autorisation de sécurité
EDI	Équité, diversité et inclusion
EMR	Évaluation des menaces et des risques
GC	Gouvernement du Canada
GR	Gravité du résultat
MFC	Menace fondé sur la conception
PC	Probabilité de compromis

PDIR	Protection, détection, intervention et récupération
PSG	Politique sur la sécurité du gouvernment
SCT	Secrétariat du conseil du trésor du Canada

4. Glossaire

Terme	Définition
Acteur de la Menace	Une personne ou un groupe qui portent intentionnellement atteinte, directement ou indirectement, au personnel, aux départements ou aux organismes du GC. L'example primaire s'agit d'une intrusion ou d'une activité criminelle, mais cela peut aussi être des actes allant jusqu'à la terreur ou à la violence parrainée par l'État.
Actif	Actifs corporels ou incorporels du GC. Ce terme s'applique, sans 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 Incorporel	Tout actif qui manque de forme physique et peut être difficile à identifier. Ces facteurs comprennent, sans s'y limiter, la confiance des employés, la confiance du public, la crédibilité personnelle ou organisationnelle et la réputation internationale.
Actif Tangible	Tout actif qui a une forme physique et est facile à identifier. Il peut s'agir, sans s'y limiter, d'information sous toutes ses formes et sur tous les supports, réseaux, systèmes, matériel, biens immobiliers ou ressources financières.
Actifs Essentiels	Les actifs dont la compromission en termes de disponibilité ou d'intégrité entraînerait un degré élevé de blessures à la santé, à la sécurité, à la sûreté ou au bien-être économique des Canadiens, ou au fonctionnement efficace du GC.
Blessure	Dommage ou conséquence en cas de compromis.
Criticité	Le degré de la blessure ou l'importance d'un bien, d'une personne, d'une fonction, d'un service ou d'une réputation s'il est perdu ou indisponible.
Gravité	Mesure utilisée pour déterminer la gravité d'un résultat.
Gravité de la Menace	La gravité de toute menace affectant un actif. Cette évaluation est effectuée à l'aide de renseignements sur les capacités d'un agent de menace et/ou sur l'ampleur d'un accident potentiel ou d'une menace naturelle.
Interdépendants	Relation entre des actifs, services ou systèmes qui en dépendent.

Menace	Événement ou acte délibéré ou accidentel qui pourrait porter de blessures aux personnes, à l'information, aux biens ou aux services.
Menace Accidentelle	Compromis sur la confidentialité, l'intégrité et la disponibilité d'un bien par suite d'une erreur humaine. Ces dommages peuvent inclure, sans s'y limiter, les dommages physiques accidentels, les dysfonctionnements de l'équipement, les erreurs opérationnelles ou la corruption des données.
Menace Délibérée	Tentative préméditée, causée par l'humain, d'interrompre la prestation de services et/ou de compromettre la confidentialité, l'intégrité, la disponibilité et la valeur d'un bien. Cela peut inclure, sans s'y limiter, le vol, le sabotage, l'espionnage ou la modification/exploitation non autorisée de renseignements et etc.
Menace Naturelle	Les perturbations environnementales et naturelles qui échappent au contrôle humain et peuvent avoir une incidence sur la prestation de services ou la disponibilité, la valeur d'un actif. Cela peut inclure, sans s'y limiter, les tornades, les ouragans, les inondations, les tempêtes de neige et etc.
Mesures de Protection	Actifs ou contrôles externes qui réduisent les risques aux employés, d'autres actifs ou la prestation de services en diminuant la probabilité d'un événement menaçant, en réduisant la probabilité de compromission, ou atténuer la gravité du résultat par une interaction directe ou indirecte avec les valeurs de l'actif, les menaces ou les vulnérabilités.
Niveau de la Blessure	Une estimation de ce qui pourrait se produire si l'actif est compromis et ne peut pas remplir sa fonction prescrite.
Probabilité	La probabilité, ou le hasard, que quelque chose se produit.
Probabilité de Menace	La probabilité qu'une menace compromette un actif.
Risque	Incertitude que peut engendrer l'exposition à des événements ou résultats non désirés. Il s'agit de l'expression de la probabilité et de l'incidence d'un événement susceptible de nuire à la réalisation des objectifs d'une organisation.
Risque Résiduel	Le risque résiduel représente la quantité de risque restant après une détermination des valeurs pour les données sur les actifs, les menaces et la vulnérabilité.
Tolérance au Risque	La volonté d'une organisation d'accepter ou de rejeter un niveau donné de risque résiduel (exposition). La tolérance au risque peut varier d'une organisation à l'autre, mais elle doit être clairement comprise par les personnes qui prennent des décisions liées au risque sur un sujet donné.
Vulnérabilité	Insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou aux blessures.

5. Aperçu d'une Évaluation des Menaces et des Risques

Les EMR sont un outil d'analyse utilisé pour identifier et déterminer objectivement le niveau de risque d'un actif ou d'un portfolio d'actifs particuliers. Utilisation des données recueillies sur la criticité d'un actif, les menaces auxquelles il peut être confronté et les vulnérabilités des mesures de protection actuellement en place; L'EMR utilise des calculs pour déterminer le niveau de risque de chaque actif. Le risque résiduel est ensuite comparé au niveau de tolérance du département ou de l'organisme pour déterminer les lacunes qui nécessitent des efforts d'atténuation supplémentaires. Ces renseignements servent ensuite à formuler des recommandations aux responsables de la protection de l'actif sur la façon de réduire le risque à des niveaux jugés acceptables. Il existe de nombreuses méthodologies qui pourraient être utilisées pour effectuer une EMR, mais chacune d'entre elles devrait suivre un ensemble similaire de concepts de base. Il y a sept parties principales d'un EMR, bien qu'elles puissent être décomposées ou combinées selon la méthodologie utilisée. Peu importe la structure de l'EMR, toutes les méthodes utilisées pour les EMR contiennent les processus décrits ci-dessous.

Il existe un quelques méthodes pour produire une EMR, à la fois manuellement ou avec l'aide d'un logiciel. Le cours d'Évaluation des Menaces et des Risques du POSM de la GRC utilise le logiciel automatisé d'Évaluation des Menaces et des Risques (ASTRA) pour aider les évaluateurs à rédiger l'EMR. Ce logiciel effectue automatiquement un bon nombre des calculs décrits dans ce guide, ce qui réduit la nécessité pour les évaluateurs de faire des calculs compliqués. Ce guide est conçu pour permettre aux évaluateurs de développer une EMR sans avoir à utiliser un logiciel, bien que l'utilisation d'une telle technologie simplifie beaucoup le processus.

5.1. Préparation

La phase de préparation, expliquée plus en détail à la section 6, permettra d'établir la portée de l'évaluation et le niveau acceptable de risque résiduel. La portée de l'évaluation devrait être déterminée par une autorité de gestion des risques qui détermine quels actifs seront évalués dans l'EMR. L'autorité de gestion des risques devrait également confier l'évaluation à une équipe qualifiée de professionnels de la sécurité.

Au cours de cette phase, l'évaluateur ou l'équipe d'évaluateurs devrait recueillir suffisamment d'informations pour élaborer un plan de travail décrivant les principaux produits à chaque étape ainsi que les ressources nécessaires pour réaliser l'EMR. Une fois le plan de travail terminé, il devrait être examiné pour s'assurer qu'il respecte les délais requis, respecte les pouvoirs financiers appropriés et que les ressources sont disponibles pour le projet. Si le plan de travail de l'EMR est acceptable, la direction devrait documenter son approbation et demander à l'équipe de commencer l'évaluation.

5.2. Identification et Évaluation des Actifs

La phase d'identification et de valorisation des actifs, expliquée plus en détail à la section 7, permettra d'identifier tous les actifs visés par l'EMR. Il ne faut pas consacrer du temps et des

ressources à des actifs qui ne font pas partie de l'EMR, sauf s'il y a des interdépendances liées aux actifs pertinents. Tous les actifs qui se situent dans les paramètres désignés dans la phase de préparation doivent être clairement énumérés et une valeur doit leur être attribuée. Il existe plusieurs catégories pour chaque actif, allant de très bas à très haut. Pour les évaluations de la sécurité matérielle des biens au sein du GC, toutes les valeurs sont évaluées et attribuées en fonction des trois catégories de sécurité identifiées à l'annexe J du DGS: confidentialité, disponibilité et intégrité. Bien qu'ils ne soient pas explicitement mentionnés dans le DGS, les évaluateurs peuvent aussi tenir compte de la valeur associée aux actifs, soit la valeur monétaire spécifique du bien ou la valeur culturelle ou sociale associée à la compromission des biens.

La valeur des actifs est également attribuée en fonction d'une détermination du dommage, c'est-à-dire une représentation des dommages qui pourraient survenir si l'actif était compromis. Bien que les biens puissent recevoir plusieurs valeurs en fonction des niveaux de blessure perçus, la catégorie de blessures qui obtient le plus haut score devrait être prioritaire pour l'évaluation.

5.3. Évaluation de la Menace

La phase d'évaluation des menaces, expliquée plus en détail à la section 8, permettra d'identifier et d'énumérer toutes les menaces réelles et potentielles auxquelles les biens évalués pour l'EMR pourraient faire face. Les menaces peuvent être classées comme étant délibérées, accidentelles ou naturelles. Les menaces doivent être répertoriées et leur niveau de menace doit varier de très faible à très élevé. Cette valeur est déterminée en comparant la probabilité de l'occurrence d'une menace à la gravité de la menace ; autrement dit, on détermine ce qui pourrait se produire si la menace a un impact sur le bien.

5.4. Évaluation de la Vulnérabilité

Au cours de l'évaluation de la vulnérabilité, l'équipe EMR évaluera les biens en cours d'évaluation afin de déterminer quelles mesures de protection sont en place pour les protéger. Une fois identifiés, les évaluateurs déterminent de façon critique si ces mesures de protection sont efficaces en fonction d'une probabilité de compromis et de la gravité du résultat si les menaces identifiées compromettent les biens. Les vulnérabilités contribuent aux risques en augmentant la probabilité de menace, la probabilité de compromission et en permettant aux menaces de causer plus de dommages. Ce point est expliqué plus en détail à la section 9.

5.5. Calcul des Risques Résiduels

Le risque résiduel est le niveau de risque restant après que les actifs, les menaces, les mesures de protection et les vulnérabilités ont été comparés. Les évaluateurs peuvent déterminer le risque résiduel dans une EMR en comparant les valeurs totales des actifs, des menaces et des vulnérabilités relevant de la portée de l'EMR. Diverses méthodes d'EMR inciteront les évaluateurs à convertir chaque valeur de l'actif, des menaces et de la vulnérabilité en un nombre donné à l'aide de tableaux prédéfinis d'évaluation du risque. Ces

numéros assignés permettent aux évaluateurs de déterminer rapidement le risque résiduel pour chaque actif évalué en multipliant la valeur de l'actif par les valeurs des menaces pertinentes et de la vulnérabilité connexe. La valeur totale représente un score de risque résiduel pour l'actif.

Chaque risque résiduel peut alors être comparé au niveau de tolérance au risque déterminé au début de l'EMR. Les risques qui correspondent ou qui sont inférieurs au niveau de tolérance ne nécessitent pas d'atténuation des risques; outefois, les risques résiduels qui dépassent le niveau de tolérance exigeront des mesures d'atténuation supplémentaires pour ramener le risque résiduel à un niveau acceptable.

5.6. Recommandations

La phase de recommandation, expliquée plus en détail à la section 10, contient la comparaison des risques calculés par l'équipe EMR par rapport au niveau de risque acceptable, identifié dans la phase de préparation. Pour les risques résiduels qui sont à ou en dessou du niveau cible de tolérance au risque, l'équipe devrait recommander le maintien du statu quo ou la modération des mesures de sauvegarde afin d'économiser les ressources. Dans le cas où les mesures de protection sont réduites ou supprimées, un nouveau calcul du risque résiduel est nécessaire pour la gestion. Dans tous les cas où le risque résiduel dépasse le niveau acceptable, l'équipe de l'EMR doit proposer des mesures pour ramener le risque résiduel au niveau acceptable. Le responsable de l'acceptation des risques liés à l'EMR identifié au cours de la phase de préparation examinera ensuite toutes les mesures de protection proposées et déterminera quelles recommandations seront mises en œuvre pour réduire le risque résiduel. Il est très important de noter que la tolérance globale au risque des départements ne devrait pas être ajustée pour répondre à la cote de risque résiduel de l'EMR. Il faudrait plutôt recourir à des mesures de sauvegarde pour ajuster le risque résiduel à un niveau correspondant à la tolérance au risque des départements.

5.7. Le Rapport Final de l'EMR

Le rapport sur l'EMR, expliquée plus en détail à la section 11, constitue le principal produit livrable du processus d'EMR. Le rapport final doit être bien expliqué et contenir suffisamment d'information pour permettre à l'équipe responsable de mettre en œuvre les mesures de protection recommandées et approuvées. Un rapport final sur l'EMR contiendra un résumé de chaque phase de l'EMR :

- Plan de travail;
- Évaluation des actifs;
- Évaluation des menaces;
- Évaluation de la vulnérabilité;
- Liste des risques résiduels prioritaires;
- Recommandations.

La décision 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 et une signature

officielle confirmant ces décisions. On trouvera plus de renseignements sur le processus de gestion des risques dans le document GSMGC-018 Guide du processus de gestion des risques pour la sécurité matérielle. Ce n'est qu'après la signature du rapport d'EMR par l'DPS ou son délégué que le processus sera terminé.

6. Préparation

La phase de préparation d'une EMR établira les pouvoirs de signature, déterminera la portée de l'évaluation et le niveau acceptable de risque résiduel. Les actifs à évaluer doivent être identifiés, les échéances de l'évaluation doivent être déterminées et une équipe de projet doit être chargée de remplir l'EMR. Au cours de cette phase, l'équipe EMR devrait recueillir suffisamment d'information pour élaborer un plan de travail. Le plan de travail sur l'EMR devrait être un document concis et clairement écrit décrivant la portée prévue de l'évaluation, les tolérances de risque convenues et les pouvoirs d'approbation, la composition de l'équipe, les échéanciers prévus pour effectuer l'évaluation., et des ressources supplémentaires sont recherchées pour compléter l'EMR. Le plan de travail doit être soumis et approuvé avant toute évaluation du site, surtout si l'équipe de projet engage des consultants pour aider. Cela permettra de limiter les retards inutiles dans le projet d'EMR.

6.1. Établir les Autorités d'Approbation

Avant de lancer une EMR, il faut désigner une autorité d'évaluation des risques pour approuver l'affectation des ressources nécessaires au projet et déterminer avec qui elle doit prendre les décisions relatives à l'évaluation des risques. Si ces rôles sont occupés par des personnes différentes, toutes doivent être informées et approuver le début de l'EMR. Le pouvoir de prendre des décisions d'évaluation des risques appartient généralement au chef de la sécurité (DPS) d'une organisation, qui est autorisé par la Directive sur la gestion de la sécurité 4.1.2.2 (DGS) à déléguer ce pouvoir. S'il n'est pas clair à qui l'autorité de gestion des risques a été déléguée, les évaluateurs doivent confirmer auprès de leur bureau du DPS par l'intermédiaire de la chaîne de gestion appropriée. Il y aura des coûts associés à la réalisation d'une EMR; Les heures de travail du personnel seront nécessaires, ainsi que des dépenses monétaires supplémentaires peuvent être engagées. S'assurer que l'autorité financière s'engage à permettre que ces ressources soient affectées à la réalisation de l'EMR. L'autorité d'approbation peut également être désignée comme propriétaire du risque, car elle accepte tout risque découlant des constatations de l'EMR.

6.2. Mandat et Portée du Projet

Une fois ces pouvoirs définis, un mandat de projet doit être établi et approuvé par les autorités d'approbation. Le mandat devrait comprendre les éléments suivants de l'organisation du GC:

- Niveau de tolérance au risque;
- Ressources approuvées pour le projet EMR;
- Budget/délais pour les recommandations;
- Les paramètres qui limiteront la portée de l'EMR de quelque manière que ce soit.

Le mandat devrait également préciser qui doit signer le rapport complet et si le DPS a délégué à ces personnes le pouvoir d'accepter tout risque résiduel dépassant le niveau de risque acceptable pour l'organisation. Avant de commencer l'EMR, les responsables du projet et les membres de l'équipe devraient bien comprendre la portée et le mandat du projet. Cela peut inclure les actifs à évaluer et, en fonction du niveau actuel de criticité des actifs, l'ampleur de l'évaluation justifiée. La portée de l'EMR variera en fonction du temps nécessaire pour effectuer l'évaluation et du montant des ressources disponibles. La portée d'une EMR peut varier, allant d'une évaluation étroite, comme celle d'une pièce contenant des documents sensibles dans une installation du GC, à une évaluation générale qui pourrait englober tous les actifs d'un portfolio de plusieurs immeubles.

Lorsqu'ils examinent la portée d'une EMR, les évaluateurs devraient déterminer s'il s'agit d'une évaluation générale de niveau stratégique qui porte sur un domaine particulier ou d'une évaluation approfondie et détaillée qui explore divers scénarios avec seulement quelques variables relatives aux actifs, aux menaces ou à la vulnérabilité. Cela aidera à établir les critères de l'évaluation, ce qui doit être évalué et ce qui est dans le cadre ou au-delà de l'évaluation. Il est impératif que les responsables de projet et les membres de l'équipe EMR s'entendent sur des paramètres clairs et définis afin d'éviter que la portée ne dépasse ou ne respecte pas l'évaluation prévue des domaines requis.

6.3. Comprendre le Niveau de Tolérance au Risque de la Direction

Un administrateur général est chargé de déterminer le niveau de risque global qu'un département est prêt à accepter et le DPS se voit déléguer la tâche d'évaluer le montant du risque résiduel qu'il est prêt à accepter du point de vue de la sécurité. Chaque organisation devrait établir un niveau de tolérance au risque qui reflète la sensibilité du travail qu'elle effectue et les types d'actifs qu'elle utilise pour exécuter ses services clés. Le DPS peut déléguer des décisions de gestion du risque, ce qui peut entraîner que différentes unités aient des niveaux de tolérance au risque différents de ceux de la base de référence. Les évaluateurs doivent déterminer qui est responsable de la gestion du risque associé aux actifs évalués pour l'EMR. Cette personne sera désignée comme étant l'autorité compétente (AC). Les projets EMR de plus grande envergure peuvent avoir plusieurs AC responsables de différents actifs qui seront évalués, vous devez tous les engager dans des discussions sur la tolérance au risque. Il doit y avoir un consensus entre tous les AC et l'équipe de l'EMR au sujet des niveaux de tolérance au risque. Il est impératif que l'équipe de l'AC et celle de l'EMR s'entendent sur le niveau cible, ainsi que sur ce à quoi ressemblera ce niveau une fois mis en œuvre. S'assurer que l'AC comprend les mesures utilisées pour mesurer le risque résiduel et confirmer que cela correspond à son niveau de tolérance au risque déclaré.

Il est crucial que la direction et l'équipe d'évaluation aient une compréhension commune de la tolérance au risque, de l'approbation du projet et des hypothèses ou déterminations préalables. En cas de confusion ou de désaccord, le projet peut être retardé ou des

recommandations inadéquates ou inappropriées qui ne correspondent pas aux attentes de la direction.

6.4. Sélection de l'Équipe

La composition de l'équipe améliore grandement l'efficacité du processus d'EMR et contribue à la meilleure analyse et aux meilleures recommandations possibles. Bien que de nombreux EMR seront probablement effectués par une ou deux personnes, la taille et la composition de l'équipe seront dictées par les considérations suivantes:

- La portée de l'évaluation;
- Complexité des actifs;
- Urgence de la situation;
- Répartition des actifs;
- Disponibilité de personnel qualifié.

Une équipe devrait avoir au moins un (1) membre avec un ou plusieurs des éléments suivants :

- Une bonne compréhension du processus d'EMR;
- Une compréhension détaillée des besoins opérationnels du département ou de l'unité;
- Une compréhension approfondie des normes de sécurité et autres mesures de protection;
- Les niveaux d'autorisation et de contrôle de sécurité pour accéder à une installation ou un emplacement où se trouvent les biens faisant l'objet de l'évaluation.

Sans personnel qualifié, représentant à la fois les intérêts opérationnels et les considérations de sécurité, l'EMR qui en résulte ne pourrait pas contenir suffisamment d'information pour répondre aux préoccupations qui ont provoqué le lancement de l'évaluation.

Selon la portée du projet, l'équipe d'EMR peut également être composée de personnes qui peuvent fournir des détails sur les actifs, les menaces ou les vulnérabilités que le reste de l'équipe peut utiliser pour effectuer efficacement l'évaluation. Ces ressources pourraient comprendre:

- Personnel de sécurité des installations — superviseur local, gestionnaire de la sécurité du site ou membre(s) de l'équipe de sécurité;
- Gestion des installations — membres de l'équipe immobilière, architectes ou ingénieurs pour conseiller sur les considérations liées à la conception; et/ou
- Experts en la matière — spécialistes responsables de systèmes spécifiques s'ils relèvent du champ d'application de l'EMR effectuée (technologues de l'information, gardiens des documents classifiés).

Selon la taille et la complexité de l'EMR, ou le nombre et le niveau d'expérience des membres de l'équipe d'évaluation, on peut obtenir de l'expertise auprès d'autres départements pour fournir un soutien spécialisé et des conseils sur divers sujets. Ces

départements sont énumérés dans la Politique sur la sécurité du gouvernement (PSG) à l'article 5, « Rôles des autres organismes gouvernementaux ».

7. Identification et Évaluation des Actifs

Après la fin de la phase de préparation, l'étape suivante de l'EMR consiste à déterminer tous les biens à évaluer et à les analyser pour déterminer le niveau de blessure (estimation de ce qui pourrait se produire si ces biens sont compromis ou ne peuvent pas remplir leur fonction prescrite). Dans le contexte d'une évaluation des risques pour la sécurité matérielle au sein du GC, les catégories de blessures peuvent être évaluées selon l'une des quatre catégories suivantes : confidentialité, disponibilité, intégrité et/ou valeur. Les évaluateurs devraient analyser soigneusement tous les biens en fonction de ces catégories de blessures et déterminer quelle catégorie de blessures décrit le mieux la façon dont le bien pourrait être compromis.

Les évaluateurs devraient également déterminer le niveau de blessure associé à chaque catégorie de blessures. Cela peut aller de faible à très élevé, avec des niveaux plus élevés représentant un niveau global de dommage plus élevé si l'actif est sujet à compromis. La gravité de la compromission potentielle de chaque actif peut alors être organisée en une liste de priorités; Classant tous les actifs du niveau le plus élevé au niveau le plus bas. Une liste hiérarchisée des actifs les plus à risque de blessures permettra d'effectuer une analyse ciblée des menaces et vulnérabilités potentielles au cours des étapes ultérieures du processus d'EMR.

7.1. Identification des Actifs

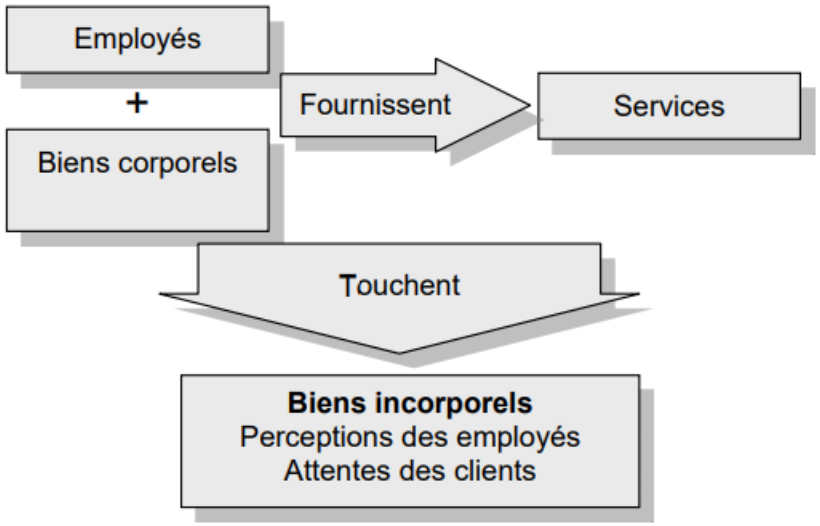
Il y a deux types d'actifs à considérer lors de la réalisation d'une EMR, les actifs corporels et incorporels.

- Les biens corporels sont plus faciles à identifier et à évaluer puisqu'ils englobent des objets pouvant être touchés physiquement et qu'il est plus facile de mesurer les dommages qui y sont causés. Les serveurs informatiques et l'équipement, les documents et les véhicules sont tous des exemples d'actifs corporels ;
- Actifs incorporels, qui peuvent être plus difficiles à identifier. Les niveaux de dommage pour les actifs incorporels sont souvent subjectifs et ouverts à l'interprétation des évaluateurs et des parties prenantes. Ces actifs comprennent des concepts tels que la confiance du public envers une organisation, sa réputation et la confiance dans la capacité d'un ministère ou d'un organisme à fournir des services essentiels.

Le personnel est également un bien pour l'organisation, car il interagit avec les biens matériels pour fournir des services. La prestation de services peut avoir un effet sur les actifs incorporels, comme les perceptions des employés et les attentes des clients. La capacité des employés de fournir des services en utilisant des actifs corporels a un effet direct sur ces actifs incorporels. La valeur du personnel peut être mesurée en utilisant leur valeur intrinsèque ou leur valeur opérationnelle, selon le plus élevé des deux. Le personnel qui peut prévenir des décès à grande échelle en remplissant ses fonctions opérationnelles aurait une valeur opérationnelle plus élevée que la mesure de la valeur intrinsèque de sa vie seule. Lors

de l'évaluation des actifs, il faut examiner attentivement les services que ces actifs doivent fournir, car cela peut aider à orienter l'analyse des actifs et des niveaux potentiels de dommage en fonction de la criticité du service fourni. Plus l'impact sur les actifs est grand, plus la prestation des services est perturbée, ce qui affecte à son tour les actifs incorporels comme les perceptions des employés ou les attentes des clients. La relation entre les actifs, le personnel et la prestation de services est mise en évidence dans le graphique ci-dessous.

Tableau 1 : Graphique des relations entre les employés, les actifs et les services



Alt Text: Le graphique ci-dessus illustre les aspects qui peuvent constituer un actif incorporel

Il est essentiel que toutes les catégories d'actifs soient prises en compte pour déterminer quels sont les actifs qui entrent dans le champ d'application de l'EMR et pour déterminer les interdépendances. Lors de la réalisation d'une EMR, il est fort probable que des actifs supplémentaires seront trouvés qui ne sont pas dans le champ défini de l'EMR. Les ressources ne doivent pas être dépensées inutilement pour des actifs qui ne sont pas dans le champ d'application de l'évaluation ou qui n'ont pas d'interdépendances valides, à moins que celles-ci aient été établies par le processus d'évaluation.

7.1.1. Relations Interdépendantes

Lors de l'analyse des actifs, il faut déterminer les relations interdépendantes avec d'autres actifs dans le champ d'application de l'EMR. Selon le moment et les ressources disponibles, il faut également tenir compte des interdépendances en fonction du niveau de dommage si les biens sont compromis et du niveau d'interruption de service qui pourrait en résulter.

Exemple : Un EMR est effectué sur une installation qui abrite des lingots d'or, un actif ayant une valeur monétaire. L'installation dispose également d'imprimantes spécialisées qui peuvent produire des certificats d'authenticité traçables avec des marques antifraude et un numéro de série. Dans ce cas, l'imprimeur spécialisé n'a pas de valeur monétaire

significative et, par conséquent, s'il est analysé indépendamment, il ne peut être considéré comme faisant partie du champ d'application de l'EMR. Cependant, le principal actif (l'or) dépend de l'imprimeur pour créer des certificats d'authenticité afin de faciliter les échanges commerciaux, ce qui rend les deux actifs interdépendants. Cela signifie que l'imprimeur devrait être inscrit et analysé comme un actif dans l'EMR, car une menace pourrait diminuer la confiance du public envers les lingots d'or négociés. Si l'imprimante était compromise, cela pourrait permettre de délivrer des certificats d'authenticité frauduleux. L'imprimeur permet de négocier les lingots en toute confiance, sans compromis, et doit donc être évalué à côté des lingots.

7.1.2. Criticité de l'Actif

Lors de l'évaluation d'un actif, il est important de tenir compte de son lien avec les objectifs opérationnels de l'organisation et les services qu'elle fournit. La criticité des actifs indique l'importance d'un actif pour la prestation de services essentiels, avec une note plus élevée, ce qui signifie qu'un compromis sur le bien aura un impact plus grave sur les fonctions opérationnelles. Déterminer la criticité d'un actif est essentiel, car certains actifs peuvent recevoir des notes faibles dans d'autres mesures telles que la sensibilité ou la valeur, mais cela pourrait être essentiel pour le département de poursuivre ses activités.

Exemple : Un département de service de licences en serveurs informatiques qui traite les demandes d'inscription. Cette instalation de serveurs commerciaux (COTS) peut avoir une faible valeur monétaire et ne stocke ni ne traite d'informations sensibles. Ces facteurs placeraient cet actif relativement bas sur de nombreux indicateurs, mais un compromis peut interrompre la prestation de services et exiger une note ou une valeur plus élevée sur le critère de criticité.

7.2. Évaluation des Dommages aux Biens

Après avoir identifié tous les actifs visés par l'EMR, les évaluateurs doivent déterminer le niveau de dommage pour chaque actif. Les blessures à un bien représente une détermination de ce qui pourrait se produire si le bien est sujet à compromis et ne peut pas contribuer à la prestation des services essentiels de l'organisation. Les blessures peuvent être évaluées selon plusieurs catégories: Préjudice physique, préjudice psychologique, dommages à l'environnement, réputation diminuée et perte de confiance dans l'institution.

La plupart des méthodes d'EMR ont un système pour attribuer des notes de blessures en fonction du préjudice potentiel causé par un compromis. Bien que les formules de calcul spécifiques varient selon la méthode d'EMR, les principes sous-jacents demeurent les mêmes — plus le niveau de compromis pour l'actif est élevé, plus le risque de préjudice potentiel sera évalué.

Le DGS fournit des critères spécifiques pour déterminer la lésion. Comme il est indiqué à l'annexe J du DGS, un dommage résulte de la perte d'un actif d'un ou de plusieurs des

critères suivants:

7.2.1. Confidentialité

La confidentialité est le degré de sensibilité des renseignements en ce qui concerne l'actif et le degré de blessure que l'on pourrait raisonnablement s'attendre à voir dans le cas d'une divulgation non autorisée. Le GC utilise un système de classification de la sensibilité des actifs qui est indépendant de toute méthode d'EMR utilisée. Les méthodes d'EMR peuvent convertir le niveau de sensibilité du GC en une valeur numérique à utiliser dans les calculs, ou attribuer un score générique tel que très faible à très élevé. Vous trouverez plus d'information sur le système de classification du GC ici: Niveaux de sécurité.

7.2.2. Disponibilité

La disponibilité évalue le degré de dommage possible découlant de la destruction non autorisée, de l'interruption ou du refus d'utiliser un bien. Les cotes de disponibilité peuvent s'appliquer aux actifs corporels ou incorporels, au personnel et aux services et représentent l'impact sur la capacité du bien à fournir des services. Plus l'impact d'une indisponibilité est élevé, plus le score de disponibilité sera élevé.

Exemple : Un travailleur essentiel qui ne peut pas travailler à distance pourrait avoir une cote de disponibilité élevée. Si une manifestation refuse à l'employé l'accès à l'installation, elle pourrait mettre fin complètement aux opérations jusqu'à ce que la disponibilité de la main-d'œuvre soit rétablie.

7.2.3. Intégrité

Un score d'intégrité mesure le degré de blessure possible si l'information est modifiée sans autorisation. Les exemples pourraient être, des renseignements financiers, des données sur le traitement médical et les résultats de sondages. Plus l'impact de la modification non autorisée est important, plus le score d'intégrité de l'actif sera élevé.

Exemple : Les données financières liées aux projets d'infrastructure internationaux auraient un score d'intégrité très élevé, car la modification non autorisée des données pourrait faciliter une fraude massive, dissimuler le détournement, et nuisent grandement à la confiance des partenaires internationaux dans la capacité du Canada de mener des projets internationaux.

7.2.4. Valeur

La valeur est la valeur monétaire de l'actif ou le revenu que l'actif peut générer. Cela peut être enregistré en valeur monétaire ou convertie en une cote telle que très faible à très élevée. Bien que la valeur monétaire ne soit pas mentionnée expressément à l'annexe J du DGS, une évaluation de la confidentialité, de la disponibilité ou de l'intégrité considère indirectement la valeur monétaire comme un critère.

Il est important de tenir compte des éléments suivants pour évaluer la valeur monétaire associée à la compromission d'un actif. La valeur est calculée en déterminant le coût de remplacement de l'actif lui-même, ainsi que tout revenu perdu du fait qu'il a été refusé pendant une période donnée. Plus le coût de remplacement ou la perte de revenu résultant d'un compromis est élevé, plus la valeur de l'actif est élevée.

7.2.5. Attribution des Niveaux de Blessures

Tous les actifs visés par l'EMR doivent être évalués afin de déterminer leur niveau de dommage. Il est possible que les actifs aient plus d'un niveau de dommage et chaque actif devrait avoir une brève description décrivant le raisonnement pour sa valeur attribuée. Au minimum, le récit doit refléter la valeur la plus élevée attribuée, mais des valeurs supplémentaires peuvent être présentées si l'équipe de l'EMR juge que les renseignements sont pertinents pour l'évaluation.

L'équipe de l'EMR devrait se concentrer sur la catégorie qui a le plus grand impact global sur l'actif et établir un ordre de priorité à cet égard. Bien que les méthodes d'EMR aient des échelles différentes pour évaluer la compromission des actifs, l'EMR définit le degré des blessures aux actifs en fonction de la confidentialité, de l'intégrité, de la disponibilité et de la valeur (CIDV), ce qui rend le processus plus conforme au DGS par rapport à d'autres méthodes.

Les tableaux d'EMR sont présentés et expliqués dans les tableaux 2 et 3:

Tableau 2 : Évaluation des blessures EMR: Confidentialité, Disponibilité, Intégrité et Valeur

Niveaux de préjudice comparatifs	Type de compromission				
	Divulgation		Destruction Interruption Suppression	Modification	Destruction Suppression
	Confidentialité		Disponibilité	Intégrité	Valeur
	Classifié	Protégé			
Très élevé	Très secret		Très élevé	Très élevé	Très élevé
Élevé	Secret	Protégé C	Élevé	Élevé	Élevé
Moyen	Confidentiel	Protégé B	Moyen	Moyen	Moyen
Faible	(Diffusion restreinte)	Protégé A	Faible	Faible	Faible
Très faible	Non classifié		Négligeable ou très faible		

Alt Text: Le tableau ci-dessus indique un niveau de blessure pour chaque catégorie de CIDV.

La détermination de l'évaluation de la confidentialité des biens du GC est directement liée à leur niveau de sensibilité. Pour obtenir des renseignements sur la détermination du niveau de sensibilité d'un actif, consultez les lignes directrices du SCT. Le tableau 2 ci-

dessus présente des mesures générales pour évaluer les dommages causés aux bien-fondés sur l'information par l'intermédiaire du CIDV

Les évaluateurs doivent déterminer la plus grave atteinte à l'intégrité des biens de la CIDV. Chaque catégorie de blessures CIDV est analysée et un niveau lui est attribué. Les évaluateurs qui souhaitent comprendre et quantifier les blessures subies par des personnes ou la valeur monétaire doivent se reporter au tableau 3.

Tableau 3 : Évaluation des Blessures par EMR: Répercussions Humaines et Financières

Niveau de préjudice	Répercussions humaines		Répercussions financières
	Physiques	Psychologiques	
Très élevé	Pertes de vie massives	Traumatisme généralisé	> 1 G$
Élevé	Pertes de vie possibles	Stress/traumatisme grave	> 10 M$
Moyen	Blessures/maladies mineures	Méfiance/doutes du public	> 100 K$
Faible	Inconfort	Léger embarras	> 1 K$
Très faible	Négligeables	Négligeables	< 1 K$

Alt Text: Le tableau ci-dessus sert à déterminer le niveau de dommage en fonction des répercussions d'un compromis.

Exemple 1: Une cuve de purification d'eau dans une usine de traitement. Une manipulation non autorisée de l'équipement, qu'elle soit malveillante ou incompétente, pourrait nuire gravement à la santé des résidents qui se trouvent dans la zone de service public. En conséquence, le risque de blessure si l'actif est compromis est très élevé.

Exemple 2: Une liste de patients dans un centre de réadaptation pour alcooliques recevrait une note moyenne, car un compromis pourrait sérieusement embarrasser les patients et nuire à la confiance du public envers l'organisation pour protéger les renseignements sensibles.

7.3. Liste des Actifs Prioritaires

Une fois que tous les biens ont été évalués et qu'ils ont des valeurs, on peut les compiler dans une liste de biens prioritaires en commençant par les biens ayant la valeur la plus élevée (priorité la plus élevée) et en les classant par ordre décroissant jusqu'à la valeur la plus faible (priorité la plus basse).

Dans les cas où plusieurs actifs ont des notes numériques identiques, l'équipe EMR devra réévaluer et sélectionner l'ordre dans lequel ils seront répertoriés. Cela peut être fait en comparant les valeurs les plus élevées au deuxième rang, le cas échéant. Si les actifs ont des scores égaux dans les valeurs subséquentes, l'équipe peut faire un appel subjectif sur l'ordre de priorisation des actifs et inclure une explication de la décision. Lorsqu'il fait un appel

subjectif pour classer ces actifs, l'équipe de l'EMR devrait les aligner sur les objectifs généraux de l'EMR, le mandat de l'organisation et tout produit livrable de service qui pourrait être touché. On peut aussi déterminer quel actif est le plus susceptible d'être visé ou touché par un compromis. Le bien qui est le plus susceptible d'être ciblé ou touché devrait être placé à un niveau de priorité supérieur.

8. Évaluation de la Menace

La phase d'évaluation des menaces vise à déterminer les menaces potentielles auxquelles un actif est exposé et à les classer en fonction de la probabilité qu'elles se produisent et de la gravité du résultat causé par la menace. Les évaluateurs de l'EMR devraient analyser la façon dont une menace affectera les biens dans le cadre de l'évaluation. Cela se fait par la création de scénarios de menace, des descriptions chronologiques spécifiques de la façon dont une menace pourrait affecter un actif en fonction des données disponibles sur les menaces. Il est possible qu'une menace affecte plusieurs actifs, dans ce cas un scénario de menace sera généré pour chaque actif sujet à la menace. Inversement, les actifs peuvent être affectés par des menaces multiples et seront donc inclus dans des scénarios de menace multiple.

Pour effectuer une évaluation de la menace, quelle que soit la méthodologie utilisée, les évaluateurs des EMR doivent déterminer la probabilité qu'une menace se produise et l'impact de celle-ci si elle se manifeste. Le Royaume-Uni (UK) utilise un système similaire à la méthodologie EMR pour évaluer les menaces. The National Risk Register (NRR) est la version externe de l'évaluation des risques pour la sécurité nationale (NSRA), que le gouvernement britannique utilise pour évaluer les risques les plus graves auxquels son pays fait face. Le NRR contient une liste où de nombreuses menaces courantes sont analysées et mises à jour annuellement. Cette méthode détermine la vraisemblance en utilisant une matrice qui attribuera un niveau numérique d'un (1) à cinq (5). La probabilité dans la méthode NRR est séparée entre les menaces délibérées et accidentelles, et n'utilisera qu'une des deux. La gravité/impact est déterminée sur une échelle, à laquelle on attribue une valeur numérique allant d'un (1) à cinq (5) en fonction de l'une des trois (3) mesures: Décès, pertes et/ou coût financier. Ces deux valeurs numériques sont ensuite visualisées sur un graphique qui contient toutes les menaces analysées et permet aux évaluateurs de déterminer rapidement les menaces les plus graves qui nécessitent une attention.

8.1. Catégories de Menaces

Les menaces peuvent provenir de diverses sources. Diverses méthodes d'EMR classent les menaces en trois catégories communes: Les risques délibérés, accidentels et naturels. Chaque catégorie devrait être évaluée, sauf si elle est exclue du champ d'application de l'EMR. Il est conseillé de travailler individuellement sur chaque catégorie, car il peut être facile d'ignorer les menaces naturelles et accidentelles, en prêtant la plus grande attention aux menaces délibérées.

8.1.1. Délibéré

Les menaces délibérées sont des tentatives de nuire à un bien, telles que le vol, la modification non autorisée, l'exploitation d'informations ou toute autre activité malveillante. Les menaces délibérées peuvent être entreprises par un large éventail d'acteurs, tels que des acteurs étatiques, le crime organisé, des crimes de chance, des menaces internes ou des acteurs motivés par l'idéologie. Les données de la police locale peuvent donner une idée des éléments criminels potentiels qui pourraient constituer une menace dans la région; Ces renseignements devraient être recueillis et analysés. La vérification des ressources locales, régionales ou nationales en matière de nouvelles peut aider à identifier les groupes qui pourraient être motivés par une idéologie pour perturber un actif qui peut faire l'objet d'un recoupement avec des partenaires des services de police afin de déterminer leur importance dans la région.

Les menaces posées par les acteurs étatiques peuvent être plus difficiles à déterminer, car il y aura peu de données disponibles directement liées à leurs motivations ou capacités. Lors de l'évaluation des menaces pesant sur les acteurs étatiques, il peut être avantageux de référé au menace fondé sur conception (MFC), liste des données disponibles, les lacunes étant comblées par des prédictions de motivations et de capacités. Le MFC est un profil du type, de la composition, de la capacité, de la méthode, des dommages projetés ou de l'intensité d'une menace délibérée, accidentelle ou naturelle à la sécurité et aux opérations d'une installation. Les MFC peuvent être utilisées conjointement avec une EMR pour déterminer les caractéristiques spécifiques des menaces qui nécessitent une atténuation. Si l'évaluation porte sur des biens qui ont de la valeur et peuvent être ciblés par des États hostiles, il est recommandé de consulter les renseignements et les contacts figurant sur Sécurité publique Canada.

Le risque d'initié est particulièrement dangereux, car l'acteur de la menace aura une connaissance intime de l'organisation et pourra tirer parti de la confiance des collègues pour contourner les mesures de protection. Les risques d'initiés montrent souvent des signes avant-coureurs, comme le fait que le personnel entre dans des installations en dehors des heures de travail, tente d'accéder à des renseignements sur des biens qui ne font pas partie de ses tâches quotidiennes et se comporte avec mécontentement envers ses supérieurs ou le gouvernement. Le risque interne peut également être associé à des employés loyaux qui sont soumis à un chantage, à une manipulation ou à une coercition de la part d'un acteur menaçant pour forcer l'employé à compromettre ses actifs. Sécurité publique Canada à plusieurs ressources en ligne sur le risque d'initiés disponible ici.

8.1.2. Naturel

Les menaces naturelles peuvent être plus facilement identifiées grâce à une mine de données météorologiques qui sont ouvertement accessibles au public. Sécurité publique Canada a des ressources disponibles à utiliser, mais les effets des menaces naturelles sont notoirement difficiles à déterminer avec précision. Lorsque vous évaluez les menaces naturelles, utilisez des données historiques locales pour déterminer la gravité

de base du moment où ces événements se produisent et utilisez cette information dans vos calculs d'EMR. Compte tenu des dommages potentiels aux biens ou de l'interruption des services, et de l'imprévisibilité associée aux risques naturels, les évaluateurs devraient examiner attentivement les menaces naturelles dans leurs critères d'évaluation, si possible en fonction de la portée de l'évaluation.

8.1.3. Accidentel

Les menaces accidentelles sont des compromis causés par une erreur humaine, comme des dommages physiques, mécaniques ou électriques, accidentels et des dysfonctionnements logiciels. La menace d'accidents est la plus courante dans les opérations quotidiennes et l'impact peut être multiplié par un manque de formation ou une mauvaise culture de sécurité. Un élément clé pour les menaces accidentelles est l'absence de toute intention malveillante, mais l'impact potentiel sur les actifs pourrait être aussi grave que dans n'importe quelle autre catégorie. Les acteurs de menaces délibérées peuvent exploiter des menaces accidentelles pour masquer des actions malveillantes. Les menaces accidentelles sont identifiées en examinant les données sur les incidents, en interviewant les chefs d'équipe et le personnel, et en évaluant les mesures de protection pour déterminer leur efficacité.

8.2. Évaluation de la Probabilité d'une Menace

La probabilité de menace est la probabilité qu'une menace compromette un actif et peut être difficile à déterminer avec précision compte tenu des incertitudes entourant des menaces particulières. Les méthodes d'EMR comprendront généralement des matrices pour aider à déterminer un score de vraisemblance à utiliser dans leurs calculs. Les données entrantes peuvent comprendre des données régionales, comme des incidents impliquant des installations ou des biens similaires, la fréquence d'événements criminels, des données météorologiques historiques et d'autres renseignements de ce genre.

Le tableau 4 est un outil d'évaluation de la vraisemblance utilisé dans la méthodologie EMR. L'évaluateur recueillera des données pour déterminer la fréquence d'une menace, le lieu où elle a eu lieu et comparera l'emplacement des biens, les autres biens au même endroit ou des biens similaires à d'autres endroits. Ces valeurs sont ensuite utilisées pour déterminer une valeur de vraisemblance globale pour la menace spécifique. Ce tableau devrait être utilisé pour réfléchir de façon critique aux scénarios de menace.

Tableau 4: Matrice de Probabilité des Menaces EMR

Fréquence passée	Même endroit, biens semblables	Endroit distant mais biens semblables ou Même endroit mais biens différents	Endroit distant, autres biens
Quotidienne	Élevée	Élevée	Élevée
1 à 10 jours	Élevée	Élevée	Moyenne
10 à 100 jours	Élevée	Moyenne	Faible
100 à 1 000 jours	Moyenne	Faible	Très faible
1 000 à 10 000 jours	Faible	Très faible	Très faible
Plus de 10 000 jours	Très faible	Très faible	Très faible

Alt Text: Il s'agit d'un graphique tiré de la méthodologie EMR pour déterminer la probabilité d'une menace.

Exemple : Un service fédéral de comptage des bulletins de vote. La portée est d'évaluer spécifiquement le risque lors du comptage. Une menace identifiée est celle des manifestants antigouvernementaux qui tentent de perturber le décompte des bulletins. Les données montrent qu'il s'agit d'un type d'incident qui se produit régulièrement et à chaque élection pour cet emplacement. Les élections ne se tiennent que tous les quatre ans, donc en utilisant le graphique, la fréquence passée serait de 1 000 à 10 000 jours. Avec cette entrée de données, la production de vraisemblance serait évaluée comme étant faible. Ce score ne reflète toutefois pas la probabilité réelle, car l'incident se produit à chaque fois que les bulletins de vote sont comptés. Compte tenu de la portée de l'évaluation, il est plus précis de déterminer la fréquence passée comme étant quotidienne, étant donné que des incidents similaires se sont produits à cet endroit chaque fois que les paramètres de l'évaluation sont présents. Le recalcul de la probabilité avec cette information plus précise donnerait une cote de probabilité plus révélatrice de Hautes. Ce raisonnement devrait être expliqué dans l'EMR pour démontrer comment le score de vraisemblance a été déterminé.

8.3. Évaluation de la Gravité des Menaces

La gravité d'une menace reflète les conséquences de la menace qui affecte le bien évalué et l'ampleur des dommages qui peuvent survenir. Pour évaluer la gravité de la menace, comparez-la aux catégories de blessures les plus importantes de chaque actif identifié à la section 7: Identification et évaluation des actifs. Ensuite, analyser le montant des dommages qu'une menace pourrait causer si elle compromet l'actif. Plus une menace peut causer des dommages, plus la gravité des menaces est élevée. Tenir compte de l'effet de la menace sur la criticité, la confidentialité, la disponibilité, l'intégrité, la valeur monétaire et les pertes potentielles d'un actif en cas d'incident. Chaque méthodologie détermine la gravité d'une menace, généralement dans une matrice comme celle utilisée par l'EMR. L'exemple de la section 8.2 Évaluation de la probabilité d'une menace est développé ci-dessous à l'aide de ce tableau pour démontrer l'application pratique de l'évaluation de la gravité.

Tableau 5 : Matrice de Gravité des Menaces EMR

Capacités de l'agent de menace délibérée	Magnitude des accidents ou des risques naturels	Incidence ou gravité de la menace
Connaissances/compétences étendues et ressources considérables	Hautement destructifs Erreur extrêmement grave Utilisation abusive généralisée	Élevée
Connaissances/compétences limitées et ressources considérables **ou** Connaissances/compétences étendues et ressources limitées **ou** Connaissances/compétences modérées et ressources moyennes	Modérément destructifs Erreur grave Utilisation abusive importante	Moyenne
Connaissances/compétences limitées et ressources limitées	Peu destructifs Erreur mineure Utilisation abusive limitée	Faible

Alt Text: les graphiques ci-dessus représentent un graphique de la méthodologie EMR pour déterminer une gravité des menaces

Exemple : Les intervenent d'urgences locales ont partagé des données provenant de rencontres antérieures avec ce groupe antigouvernemental. Les données suggèrent qu'ils sont associés idéologiquement à un mouvement de protestation international. Le groupe opère exclusivement dans des cellules locales, sans aucune collaboration directe avec les groupes similaires. La communication entre les groupes se limite aux pages des médias sociaux publics qui sont facilement surveillées. Un examen des rapports d'incident à cet endroit faisant intervenir le groupe suggère qu'il est prêt à causer des dommages mineurs aux biens (graffitis) et qu'il mènera des tactiques de déni de service peu qualifiées (collage de verrous, obstruction des routes, blocage de l'accès du personnel, etc.). Un examen des données montre que le groupe n'a aucune intention violente, mais résistera passivement à l'arrestation si la police est impliquée. La police locale et les services de sécurité privés ont réussi à contenir et contrôler le groupe dans un délai de trois heures pour tous les incidents enregistrés à cet endroit. Lorsqu'on utilise ces renseignements pour déterminer les capacités du groupe, on y voit des ressources et des compétences limitées. Pour déterminer l'incidence des incidents causés par le groupe, les données indiquent que le groupe est modérément destructeur et cause une interruption du service, qui ne dure généralement pas plus de trois heures. Ces données correspondent à un niveau de gravité de Faible dans la matrice EMR.

8.4. Calcul des Niveaux de Menace

On peut déterminer les niveaux globaux de menace en comparant les niveaux de menace associés à la probabilité qu'une menace se produise et aux répercussions de ce qui se

produit si la menace se produit, ainsi que la gravité de la menace. Plus le score est élevé, plus la menace est grave. Ces cotes utiliseront généralement les pertes potentielles, la perte de valeur financière, le dommage à la réputation ou la gravité du refus de service pour attribuer une cote de menace. La méthode d'EMR choisie comportera généralement un calcul ou une matrice qui comparera les cotes/niveaux de probabilité et de gravité pour produire un niveau global de menace. Voici un exemple tiré de la méthodologie EMR en utilisant les données recueillies dans le cas d'exemple 8.2 Évaluation de la probabilité de menace et 8,3 Évaluation de la gravité de la menace. Un niveau de menace sera généré à l'aide de la matrice.

Tableau 6: Matrice des niveaux de menace EMR

Incidence de la menace	Probabilité de la menace			
	Très faible	Faible	Moyenne	Élevée
Élevée	Faible	Moyenne	Élevée	Très élevée
Moyenne	Très faible	Faible	Moyenne	Élevée
Faible	Très faible	Très faible	Faible	Moyenne

Alt Text: Le graphique ci-dessus représente une matrice de la méthodologie EMR pour déterminer les niveaux de menace

Exemple : Le groupe antigouvernemental a reçu un score de vraisemblance élevé et un score de gravité faible. Lorsque ces données sont entrées dans la matrice EMR, elles génèrent un score de menace final de moyen. Selon les renseignements analysés, ce résultat reflète la situation et sera consigné avec toutes les données à l'appui dans le rapport final de l'EMR. Une fois que toutes les menaces ont été traitées, la dernière étape de cette phase consiste à créer une liste des menaces prioritaires en commençant par le niveau de menace le plus élevé jusqu'au niveau le plus faible. Les décideurs ont ainsi un aperçu de toutes les menaces identifiées, y compris des notes sur chacune d'elles et le calcul qu'ils ont reçu.

9. Phase d'Évaluation des Risques

Après avoir déterminé les actifs et les menaces qui pourraient avoir une incidence négative sur ces actifs, les évaluateurs doivent maintenant analyser de façon critique si les mécanismes en place pour protéger leurs actifs contre les menaces identifiées sont suffisants. On appelle cela une évaluation des risques. Certaines méthodes d'EMR considèrent la détermination des vulnérabilités comme un processus analytique distinct, tandis que d'autres tiennent compte des vulnérabilités et du rendement de sauvegarde dans le cadre de l'étape d'évaluation des risques. Peu importe l'ordre, les évaluateurs qui effectuent des EMR devraient toujours considérer où les actifs à évaluer sont les plus vulnérables aux menaces identifiées. Une fois les vulnérabilités identifiées aux côtés des actifs et des menaces, leurs valeurs sont ensuite multipliées pour atteindre un niveau de risque ou un score.

Au cours de l'évaluation de la vulnérabilité, l'équipe EMR évaluera les actifs qui ont été identifiés afin de déterminer quelles mesures de protection sont en place pour les protéger. Les mesures de sauvegarde sont des mesures ou contrôles de sécurité qui remplissent une ou plusieurs fonctions visant à atténuer le risque global en réduisant la valeur des actifs, les menaces ou les vulnérabilités dans le cadre d'un projet d'EMR. Une fois identifiés, les évaluateurs déterminent de façon critique si ces mesures de protection sont efficaces en fonction du fait que les menaces identifiées compromettent les biens (probabilité de compromission) et de la gravité (gravité du résultat), ce qui entraîne une vulnérabilité. Les évaluateurs peuvent ensuite utiliser des critères d'évaluation de la protection pour comparer toutes les informations connues sur le rendement de la protection et toute vulnérabilité associée, afin de produire une liste hiérarchisée des vulnérabilités. Une fois ces valeurs identifiées, elles sont ensuite comparées aux données sur les actifs et les menaces pour obtenir un calcul du risque résiduel.

Il existe d'autres façons de calculer les risques en utilisant différentes méthodes d'EMR. La méthodologie de gestion des risques de sécurité protectrice (NPSA, Royaume-Uni) et la série de gestion des risques 430 de la FEMA (FEMA, États-Unis) en sont quelques exemples. Selon la méthodologie du NPSA (Protective Security Risk Management PSRM | NPSA), les menaces et les vulnérabilités doivent être identifiées, en les alignant sur les actifs. Tous ont été évalués quant à leur probabilité (de l'événement de menace) et leurs répercussions (sur l'organisation ou les tiers) si la menace se produit. Les risques sont ensuite évalués, calculés et compilés pour constituer un registre des risques. Le registre des risques devrait contenir suffisamment de renseignements détaillés pour que les décideurs supérieurs puissent prendre des décisions majeures et porter un jugement sur l'appétit pour le risque, l'allocation des ressources et, pour les spécialistes de la sécurité, élaborer et mettre en œuvre toutes les mesures d'atténuation des risques qui pourraient être nécessaires.

Dans le cadre de la série 430 de la FEMA sur la gestion des risques (FEMA 430 : Site and Urban Design for Security), tâches de l'évaluation des vulnérabilités comprennent la collecte d'information sur le site et l'intégration dans un portfolio de vulnérabilité qui comprend des cartes SIG et d'autres renseignements pertinents, l'identification des couches de défense (mesures de protection), l'évaluation du site et du bâtiment, et détermination de la cote de vulnérabilité. FEMA 452 a également une liste de contrôle d'évaluation des vulnérabilités qui peut être un outil utile pour les évaluateurs de déterminer les vulnérabilités: Un bref aperçu est contenu dans le document FEMA 430 — Section 2.2.4. Il contient une liste de questions pour déterminer les vulnérabilités des actifs et guider la préparation de l'évaluation globale du risque. Le processus d'évaluation des risques de la FEMA analysera la menace (probabilité d'occurrence), la valeur des actifs et les vulnérabilités (conséquences de l'occurrence) pour déterminer le niveau de risque. Le processus consiste à préparer des matrices d'évaluation du risque, à déterminer les cotes de risque (menace x valeurs des actifs x vulnérabilités) et à hiérarchiser les cotes de risque plus élevées en fonction des vulnérabilités observées pour cibler les mesures d'atténuation potentielles.

Ces méthodologies adoptent chacune des approches différentes pour effectuer une EMR, mais les normes de base sont similaires. L'objectif de l'EMR, de la FEMA et de la PSRM est d'identifier

les risques en observant les menaces qui pourraient affecter les biens et de déterminer quels seraient la probabilité et l'impact sur ces biens. Chacune de ces méthodes d'EMR peut être utilisée indépendamment pour effectuer votre analyse, mais l'objectif est de comprendre comment calculer le risque. Les étapes de cette phase seront axées sur la méthodologie EMR.

9.1. Évaluation de la Vulnérabilité

Une évaluation de la vulnérabilité évalue la sensibilité potentielle du bien à la compromission par rapport aux menaces identifiées et fournit une base pour déterminer les mesures d'atténuation visant à protéger ces biens. L'objectif est d'analyser l'efficacité des mesures de protection, plutôt que la menace pour laquelle elles sont censées protéger. C'est la différence entre faire une évaluation de vulnérabilité et examiner les vulnérabilités pour une évaluation des risques plus vaste.

Contrairement à la menace ou à l'actif, les professionnels de la sécurité peuvent avoir une plus grande influence sur la vulnérabilité dans le processus d'EMR. Il est toujours possible de modifier ou de corriger la vulnérabilité en tant qu'approche préventive d'une menace. La phase d'évaluation de la vulnérabilité comprend cinq étapes séquentielles:

9.1.1. Identification/Inscription des Mesures de Sauvegarde

La première étape cruciale de l'évaluation de la vulnérabilité consiste à déterminer les mesures de protection qui sont présentes pendant l'évaluation. L'objectif est de dresser la liste, avec un niveau de détail approprié, de toutes les mesures de protection existantes qui entrent dans le champ d'application de l'évaluation. Il peut s'agir de mesures de protection qui sont actuellement en vigueur ou qui sont envisagées ou proposées pour une mise en œuvre immédiate (par exemple, celles qui font partie d'un processus de réaménagement des bâtiments ou de conception de la sécurité). Afin d'évaluer les vulnérabilités qui exposent les actifs dans le cadre d'un projet d'EMR à des risques plus élevés, il faut d'abord déterminer les mesures de protection existantes et proposées, puis les analyser pour déterminer leur efficacité relative.

Les sauvegardes peuvent également être considérées comme des « couches défensives » pour la protection de tout actif essentiel. La plupart des équipements de sécurité sont mieux évalués comme des mesures de sauvegarde plutôt que comme des actifs. Savoir identifier les mesures de protection peut être simplifié si elles sont réparties par couches. Une approche en couches, comme la sélection de zones par exemple, peut être utilisée pour déterminer les mesures de protection qui sont les plus appropriées dans chaque zone d'une installation du GC. Pour mieux comprendre ce processus, reportez-vous à GSMGC-015 (2023) Guide pour l'établissement des zones de sécurité Matérielle. Cela peut aider à diviser certaines zones en groupes, plutôt qu'à évaluer une installation dans son ensemble. Il peut permettre une collecte de données plus ciblée lors de l'identification des garanties zone par zone.

9.1.2. Évaluer l'Efficacité des Mesures de Sauvegarde

Lors de l'évaluation des mesures de protection et de la détermination des vulnérabilités, il est important de se rappeler que les risques et les vulnérabilités causales sont inversement proportionnels à l'efficacité des mesures de protection. Autrement dit, plus la protection est efficace pour protéger l'actif, moins il y a de vulnérabilités. Les mesures de sécurité plus rigoureuses mises en œuvre pour protéger les actifs permettent de réduire les vulnérabilités et les risques connexes. Si ces types de mesures de protection remplissent leur fonction et assurent la protection des biens, des personnes et des renseignements, il pourrait en résulter moins de vulnérabilités. Si leur fonction est entravée ou exploitée, leur efficacité diminue et il pourrait en résulter davantage de vulnérabilités.

La plupart des mesures de protection remplissent une ou plusieurs fonctions de sécurité de base: protection, détection, intervention et récupération (« PDIR ») pour plus d'information, consulter GSMGC-019 (2023) u Guide de protection, de détection, de réponse et de recuperation. Les mesures de protection ont une incidence sur toutes les variables de risque (actifs, menaces et vulnérabilités), mais elles portent principalement sur les vulnérabilités. Il faudrait aussi envisager la prévention et la dissuasion, mais surtout s'occuper de l'atténuation des menaces potentielles et non pas directement des vulnérabilités. En fin de compte, les mesures de protection qui contribuent à réduire les variables de risque primaires peuvent être attribuées à une diminution de la probabilité qu'un événement menaçant se produise. Bien que nous ne puissions pas toujours contrôler la sensibilité de nos actifs, ou contrôler comment et pourquoi nos menaces se manifestent, les professionnels de la sécurité ont le plus grand contrôle sur la façon dont nous répondons à ces menaces. Le tableau de méthodologie EMR, D-1 illustre la façon dont les mesures de protection ont une incidence sur les variables de risque et sur les événements liés aux menaces.

Sur la base des concepts du PDIR, les fonctions de sécurité suivantes peuvent aider l'évaluateur à mesurer l'efficacité de la protection:

- **Évitement —** En utilisant l'évitement comme fonction de sécurité, l'impact principal serait de protéger la valeur des actifs et de réduire la probabilité qu'une menace se produise. Il réduirait ou éviterait le risque et pourrait potentiellement réduire la valeur de l'actif. Par exemple, de nombreux magasins de proximité limitent les liquidités disponibles à un petit montant après les heures normales de travail. Cela n'empêche pas quelqu'un de venir voler de l'argent, mais cela atténue la perte de grosses sommes d'argent;
- **Dissuasion —** En utilisant la dissuasion comme fonction de sécurité, l'impact principal serait de réduire la probabilité qu'une menace se produise. L'objectif est de dissuader les agents de menace délibérés qui envisagent une attaque, diminuant ainsi les intentions et la probabilité d'occurrence des agents de menace. L'installation de panneaux d'avertissement (opérations de vidéosurveillance, alarmes ou chiens de garde) pourrait servir de dissuasion, mais ne pas remédier directement aux vulnérabilités;

- **Prévention —** lorsque l'on cible des types de menaces spécifiques pour réduire la probabilité d'occurrence, la plupart des mesures préventives tendent à remédier à des vulnérabilités spécifiques, ce qui diminue la probabilité de compromission si une menace se présente. Il peut s'agir de barrières physiques ou virtuelles (murs, portes, portails, serrures, mots de passe). Des mécanismes d'identification et d'authentification robustes réduisent la probabilité ou les tentatives d'accès non autorisé à un bâtiment, mais pour un acteur de menace dédié, ces seuls mécanismes ne peuvent pas dissuader leurs efforts;
- **Détection —** La détection d'événements menaçants peut corriger certaines vulnérabilités et permettre une intervention rapide pour contenir, limiter les dommages et limiter la gravité des résultats en cas d'événement. Par exemple, les patrouilles de gardes, la vidéosurveillance et les capteurs de mouvement;
- **Réponse —** lorsqu'elle est associée à la détection, la fonction de sécurité de la réponse atténue les vulnérabilités. S'il n'y a pas de mécanismes d'intervention appropriés en place, la prévention et la détection ne servent qu'à dissuader. Si la prévention et la détection sont associées à une réponse rapide, la combinaison de mesures de sauvegarde peut réduire considérablement les vulnérabilités potentielles et atténuer le risque en réduisant le montant des dommages découlant d'un compromis;
- **Rétablissement —** Les mécanismes de rétablissement peuvent compenser d'autres vulnérabilités et favoriser un retour plus rapide aux opérations normales. La récupération peut également atténuer la gravité du résultat. Cette fonction de sécurité pourrait comprendre les procédures de sauvegarde, le stockage hors site des données essentielles, etc.

Une fois les mesures de protection identifiées, il faut déterminer leur efficacité afin d'atténuer les risques potentiels. Le calcul de l'efficacité des mesures de sauvegarde comprend:

- Les fonctions de sécurité exécutées par toutes les mesures de protection qui indiquent comment elles interagissent avec les variables de risque principales, à savoir les valeurs des actifs, les menaces et les vulnérabilités;
- Indiquer l'impact des mesures de sauvegarde sur les événements menaçants.

Tableau 7: Incidence de la Protection sur les Variables de Risque et les Événements de Menace

Fonctions de sécurité	Incidence des mesures de protection…						
	…sur les variables de risque				…sur les incidents		
	B_{Val}	M		V	O_{Prob}	C_{Prob}	C_{Grav}
		V	G				
Évitement[4]	⇓	↓			↓		⇓
		⇓			⇓		
Dissuasion		⇓			⇓		
Prévention[5]			↓	⇓	↓	⇓	
Détection				⇓			⇓
Réaction				⇓			⇓
Reprise				⇓			⇓

Légende

B_{Val} – Valeurs du bien. **M** – Menace. **P** –Probabilité de la menace.
G – Gravité de la menace (capacités de l'agent de menace). **V** – Vulnérabilité.
O_{Prob} – Probabilité d'occurrence. C_{Prob} – Probabilité de compromission.
C_{Grav} – Gravité des conséquences.
Incidence primaire – ⇓ Incidence secondaire – ↓

Alt Text: le graphique ci-dessus représente un tableau de la méthodologie EMR comme exemple visuel de détermination des impacts de sauvegarde et de leur interaction avec les variables de risque, ainsi qu'avec les événements de menace.

Bien que l'efficacité des mesures de protection et des sauvegardes puisse être mesurée en fonction de la façon dont les mesures de protection influent sur les variables de risque, à savoir les vulnérabilités, l'efficacité des mesures de protection peut également être mesurée en fonction des variables associées à un événement de menace lui-même; ce qui pourrait se produire si une menace tente d'avoir un impact direct sur un actif. L'impact des menaces sur le rendement de la protection peut être mesuré selon trois critères: la probabilité d'occurrence (PO) qui est déjà calculée dans la phase précédente, la probabilité de compromission (PC) et la gravité du résultat.

Probabilité de Compromis (PC): est la possibilité d'un accès non autorisé, de la divulgation, de la destruction, du retrait, de la modification, de l'utilisation ou de l'interruption des biens ou des renseignements. Un compromis entraînerait des dommages importants à la santé, à la sécurité ou au bien-être économique des Canadiens ou au fonctionnement efficace du gouvernement. La PC peut être évaluée par l'intermédiaire de la fonction de sécurité de la prévention en tant que mesure préventive efficace pour réduire la probabilité qu'un événement menaçant compromette un bien.

Gravité du Résultat (GR): est le dommage qui pourrait en résulter si un événement de menace devait réussir à compromettre les mesures de protection en place en exposant des vulnérabilités. Le GR dépend de l'efficacité des mesures de protection en place et

peut être évalué par les fonctions de détection, d'intervention et de récupération. Lorsque les mesures de protection sont efficaces, elles peuvent réduire le montant des dommages découlant d'un événement compromettant.

Lors de l'évaluation des mesures de sauvegarde, la meilleure pratique consiste à examiner directement les mesures de sauvegarde existantes plutôt que de s'appuyer sur des rapports ou des photographes. Observez comment les mesures de protection fonctionnent et interagissent avec le personnel et d'autres biens donnent aux évaluateurs une perspective réaliste et indique s'il y a des vulnérabilités connexes qui pourraient découler du fonctionnement de ces mesures. Par exemple, une serrure à combinaison de haute qualité remplit-elle une fonction de prévention efficace en protégeant les renseignements si une combinaison incorrecte est saisie ou si le contenant est laissé déverrouillé ? Est-ce un système de contrôle d'accès qui permet une détection efficace puisqu'il mesure l'accès non autorisé à une installation ?

9.1.3. Identification des Vulnérabilités

Une fois que les mesures de protection ont été déterminées et évaluées pour en déterminer l'efficacité, les évaluateurs devraient déterminer les vulnérabilités qui sont présentes. Les vulnérabilités peuvent être attribuables à des lacunes dans le rendement de la protection ou à des vulnérabilités connexes. Tout comme l'évaluation du rendement des mesures de sauvegarde, les équipes d'EMR devraient examiner attentivement tous les actifs visés et utiliser les renseignements recueillis dans le cadre de leurs conclusions sur les scénarios de menace pour déterminer de façon critique si les mesures de protection en place peuvent protéger les actifs.

Une méthode pour aider à cette analyse peut consister à diviser les vulnérabilités en classes de vulnérabilité, qui sont des regroupements génériques basés sur les exigences générales de la politique de sécurité définie dans le PSG et les procédures obligatoires pour le contrôle de la sécurité matérielle (annexe C) de la Directive sur la gestion de la sécurité. Il faudrait en tenir compte lors de l'assemblage des données recueillies précédemment, afin d'avoir une portée plus ciblée pour les analyses ultérieures. La méthodologie EMR énumère 17 classes de vulnérabilités pour aider les évaluateurs à déterminer les vulnérabilités à prendre en considération; Cependant, toutes les classes ne seront pas nécessaires dans tous les environnements de sécurité. De plus, toutes les classes de vulnérabilité ne seraient pas particulièrement pertinentes pour les environnements de sécurité physique. Les ministères qui s'occupent principalement de la sécurité des technologies de l'information (TI) ou de la planification de la continuité des activités présentent des vulnérabilités potentiellement différentes de celles auxquelles sont confrontés les praticiens de la sécurité matérielle. Les types de mesures de protection déjà en place, la fonction principale du département et l'information traitée seraient de bons indicateurs des classes de vulnérabilité auxquelles un département pourrait être plus sensible.

Exemple : Un lecteur de carte d'accès permet aux personnes autorisées d'accéder à certaines zones d'un bâtiment. Il est efficace en ce sens qu'il refuse l'entrée à ceux qui n'ont pas de laissez-passer et d'autorisation pour la zone. Les vulnérabilités peuvent inclure une autre personne qui suit la personne autorisée ou une personne autorisée tenant la porte pour quelqu'un qui n'a pas scanné sa carte, qu'elle ne sache pas si cette personne a accès à la zone ou non. Ces deux vulnérabilités peuvent compromettre et l'impact pourrait être grave.

9.1.4. Analyse des Répercussions de la Vulnérabilité

Après avoir identifié les vulnérabilités, leurs impacts doivent être évalués en fonction de la probabilité de compromission (PC) et/ou de la gravité du résultat (GR). EMR recommande d'utiliser la PC et la GR comme mesures pour analyser les impacts des vulnérabilités, car elles fournissent une base pour effectuer une analyse comparative de toutes les différentes vulnérabilités qui en résultent et pourraient exposer les actifs à un préjudice. Les évaluateurs doivent déterminer l'impact sur le PC en fonction de l'efficacité relative des mécanismes de prévention associés et l'impact sur la PO en fonction de l'efficacité relative des mécanismes de détection, d'intervention et de rétablissement associés. Ces impacts devraient être classés en calculs individuels pour le PC et le GR respectivement, qui vont tous deux de faible à élevé. Une fois que la PC et le GR ont été déterminés séparément, les évaluateurs peuvent ensuite comparer les deux valeurs à l'aide d'un tableau de comparaison dans l'EMR pour déterminer la cote de vulnérabilité globale.

Ils sont divisés en deux calculs distincts selon leurs fonctions de sécurité. Chaque fonction mène à un niveau différent en fonction de l'efficacité de la mesure de sauvegarde; Toutes les mesures de sauvegarde n'exercent pas la même fonction de sécurité et devraient donc être séparées pour indiquer cette fonction. Des mesures préventives efficaces réduisent la probabilité qu'un événement menaçant compromette un actif. Les mesures de prévention sont associées à la protection des témoins, ce qui pourrait inclure un verrouillage efficace d'une armoire sécurisée, car cela réduit la probabilité que quelqu'un accède avec succès aux renseignements contenus dans l'armoire verrouillée.

Des mesures efficaces de détection, d'intervention et de rétablissement, qui sont associées à un GR, réduisent le montant des dommages ou le niveau d'impact découlant d'un événement menaçant, compromettant. Par exemple, avoir un système d'alarme dans un espace de bureau qui est capable de détecter lorsqu'un code d'alarme a été saisi incorrectement ou si un accès non autorisé à l'espace est détecté. Cela créerait une alarme sonore et générerait une réponse, ce qui permettrait de déterminer si la porte a été fermée correctement ou non. Cela permet une récupération rapide et complète et un travail de reprise en peu de temps.

Tableau 8: Diagramme de Probabilité de Compromis EMR

Efficacité des mesures de protection	Vulnérabilités connexes	Probabilité de compromission
Aucune mesure de protection Mesure inefficace en grande partie Probabilité de compromission > 75 %	Facilement exploitables Besoin de peu de connaissances/ compétences/ressources Biens hautement accessibles Biens très complexes/fragiles/portables Employés mal informés/formés	Élevée
Mesure modérément efficace Probabilité de compromission 25-75 %	Pas facilement exploitables Besoin de certaines connaissances/ compétences/ressources Biens modérément accessibles Biens modérément complexes/fragiles/portables Employés modérément informés/formés	Moyenne
Mesure très efficace Probabilité de compromission < 25 % (mesure remplissant uniquement des fonctions de détection, de réaction ou de reprise)	Difficiles à exploiter Besoin de très bonnes connaissances/ compétences/ressources Accès aux biens rigoureusement contrôlé Biens très simples/robustes/statiques Employés bien informés/formés	Faible (sans objet)

Alt Text: Le graphique ci-dessus représente un tableau de la méthodologie EMR pour comprendre la probabilité de compromis en fonction de l'efficacité de la sauvegarde ou des vulnérabilités associées résultant d'une mauvaise mise en œuvre des sauvegardes.

L'efficacité des mesures de sauvegarde et les vulnérabilités connexes sont déterminées par la mauvaise mise en œuvre des mesures de sauvegarde. Si aucune mesure préventive n'était en place ou qu'elle était largement inefficace, le CP associé serait élevé. Les mécanismes qui empêchent certaines menaces de se produire, tout en permettant à d'autres de causer des dommages, ne sont que modérément efficaces. Les mesures de protection qui réduisent la probabilité que la plupart des menaces se produisent sont très efficaces. Plus la protection est efficace pour protéger un actif ou un groupe d'actifs, moins il y a de chances qu'il y ait un compromis complet. Plus une mesure de sauvegarde est inefficace pour atteindre l'objectif prescrit, et plus les vulnérabilités associées sont nombreuses, plus le CP est élevé. Pour chaque actif présentant une vulnérabilité identifiée, déterminer l'impact de la PC en fonction de l'efficacité relative des mécanismes de prévention associés, de la facilité d'exploitation et d'autres facteurs identifiés. Attribuer un niveau de faible, moyenne ou élevée du tableau 8 ci-dessus. Sélectionnez non applicable si la vulnérabilité concerne uniquement les mesures de détection, d'intervention et de rétablissement.

Exemple: Une serrure à combinaison de haute qualité remplit une fonction de prévention; Elle empêche un individu d'accéder aux renseignements ou de permettre l'entrée dans une armoire, une porte, une clôture, etc. Si la serrure est une protection très efficace avec une fonction de prévention, cela se traduirait par une PC de faible.

Tableau 9 : Graphique de la sévérité des résultats de l'EMR

Efficacité de la mesure de protection	Vulnérabilités connexes	Gravité des conséquences
Aucune mesure de protection Mesure en grande partie inefficace Biens exposés à des préjudices importants	Détection improbable des compromissions Dommages difficiles à contenir Délais de reprise prolongés/Niveaux de service faibles Biens très complexes/fragiles Employés mal informés/formés	Élevée
Mesure modérément efficace Biens exposés à des préjudices modérés	Compromissions probablement détectées au fil du temps Dommages partiellement contenus Délais de reprise/Niveaux de service modérés Biens relativement complexes/fragiles Employés modérément informés/formés	Moyenne
Mesure très efficace Biens exposés à des préjudices limités (Mesure remplissant uniquement une fonction de prévention)	Compromissions presque certainement détectées rapidement Dommages rigoureusement contenus Reprise rapide et complète Biens très simples/robustes Employés bien informés/formés	Faible (sans objet)

Alt Text: Le graphique ci-dessus représente un tableau de la méthodologie EMR pour comprendre la gravité du résultat en fonction de l'efficacité de la mesure de sauvegarde ou des vulnérabilités associées résultant d'une mauvaise mise en œuvre des mesures de sauvegarde.

L'efficacité des mesures de sauvegarde et les vulnérabilités connexes sont déterminées par la mauvaise mise en œuvre des mesures de sauvegarde. Les insuffisances ou les vulnérabilités pourraient accroître le GR en permettant à une menace de continuer à passer inaperçue et sans contrôle. Plus la mesure de sauvegarde est efficace pour détecter si un actif ou un groupe d'actifs pourrait être compromis, et plus les mesures de réponse et de récupération sont en place, moins il y a de risque qu'il y ait un impact grave. Plus une mesure de sauvegarde est inefficace et moins elle remplit son objectif prescrit, et plus les vulnérabilités associées sont nombreuses, plus la GR est élevée. Pour chaque vulnérabilité exposant des actifs dans le cadre de l'évaluation, les évaluateurs déterminent l'impact sur la GR en fonction de l'efficacité relative des mécanismes de détection, d'intervention et de rétablissement associés. Attribuer un niveau de faible, moyen ou élevé dans le tableau 9 ci-dessus. Sélectionnez non applicable si la vulnérabilité concerne uniquement les mesures de prévention.

Exemple: Un système d'alarme effectue une fonction de détection, de réponse et de récupération en créant une alarme pour avertir qu'une entrée non autorisée a eu lieu. Si le système d'alarme est une protection largement inefficace avec une fonction de détection, de réponse ou de récupération et qu'il n'a pas été en mesure de détecter une compromission potentielle si quelqu'un désactivait le clavier du code d'alarme, cela pourrait entraîner plus de dommages, ce qui entraînerait un GR de haute.

9.1.5. Attribution du Niveau de Vulnérabilité

Après avoir évalué la PC et le GR individuellement, les décideurs qui évaluent les vulnérabilités peuvent comparer ces valeurs ensemble pour générer un calcul global d'un niveau de vulnérabilité. Dans l'EMR, les cotes de vulnérabilité peuvent être classées de très faible à très élevé en utilisant le tableau de comparaison ci-dessous.

Exemple : Un verrou à combinaison pour un conteneur de sécurité remplit une fonction de prévention en réduisant la probabilité que le contenu, information secrète, soit volé ou compromis. Si le verrou est cassé et non efficace, cela générerait un niveau de vulnérabilité de Haut, mais comme le verrou à combinaison n'effectue pas de détection, de réponse ou de récupération, il serait évalué comme Bas ou N/A. Lors de la combinaison des deux scores: Haut x bas ou N/A, génère un niveau de Moyen. C'est le niveau de vulnérabilité globale le plus élevé qui peut être calculé en fonction du rendement d'une fonction de prévention uniquement lié à la protection.

Cet exemple démontre que les évaluations de la vulnérabilité des mesures de sauvegarde, si elles sont effectuées individuellement plutôt qu'en toute interdépendance, peuvent entraîner des problèmes potentiels. Lorsqu'il existe des faiblesses distinctes, mais interreliées liées aux fonctions de PDIR les calculs de l'évaluation de la vulnérabilité de base devraient être étendus pour examiner ces relations de coopération afin de déterminer, de manière plus globale, le niveau de vulnérabilité.

Tableau 10: Matrice des Niveaux de Vulnérabilité EMR

Incidence sur la gravité des conséquences (détection, réaction et reprise)	Incidence sur la probabilité de compromission		
	Faible (s.o.)	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très élevée
Moyenne	Faible	Moyenne	Élevée
Faible (s.o.)	Très faible	Faible	Moyenne

Alt Text: Le graphique ci-dessus illustre le processus de calcul des niveaux de vulnérabilité à partir de la méthodologie EMR en utilisant le tableau d'évaluation de la vulnérabilité de base

9.1.6. Évaluation Approfondie de la Vulnérabilité

Il existe malheureusement certaines limites à l'évaluation de la vulnérabilité de base. Une évaluation de base porte sur l'identification et l'évaluation des mesures de protection à partir d'une seule dimension, soit la probabilité de compromission (prévention) ou la gravité du résultat (détection, réponse, rétablissement). Toutes les mesures de protection n'ont pas un impact indépendant sur les deux. Lorsqu'une mesure de sauvegarde ne remplit qu'une seule des fonctions ci-dessus (PC ou GR), la fonction qu'elle n'exécute pas est toujours évaluée à un niveau (faible ou non applicable). Ainsi, selon le tableau 10 ci-

dessus, la vulnérabilité la plus élevée ne peut atteindre que Medium. Une évaluation approfondie de la vulnérabilité examine le tableau d'ensemble en réévaluant les mesures de protection ayant une seule fonction en examinant les mesures de protection ensemble et en étudiant comment les vulnérabilités en cascade peuvent avoir un impact sur la fonction de cette mesure. Cela permet de déterminer plus précisément le rendement de cette mesure de sauvegarde et le niveau de vulnérabilité correspondant.

Si une mesure de protection comme un portail verrouillé n'a qu'une fonction de sécurité pour limiter les individus dans une zone (prévention), elle est absente dans le cas de la détection, de l'intervention et du rétablissement, ce qui lui donne une cote basse ou N/A en utilisant une évaluation de vulnérabilité de base. En utilisant l'évaluation de la vulnérabilité étendue, le PC et le GR qui en résulteraient, selon la fonction de cette mesure de protection, considéreraient également les autres mesures, les étiquetant aussi haut, tout comme sous la fonction de prévention pour le PC.

Scénario Simple

La première façon d'envisager l'application d'une évaluation de vulnérabilité étendue est d'élaborer un scénario simple. Dans un scénario simple, conserver la cote de vulnérabilité initiale pour la fonction principale que la mesure de sauvegarde effectue. Soit PC ou GR, et réévaluer la cote de vulnérabilité faible ou N/A en fonction des critères manquants ou déficients à l'aide des autres données sur la vulnérabilité des sauvegardes recueillies pour l'évaluation. Si une mesure de sauvegarde ne remplit qu'une fonction de prévention (PC), mais aucune fonction de détection, de réponse ou de rétablissement (GR), les autres mesures de protection en cours d'évaluation remplissent-elles la fonction de détection, de réponse ou de rétablissement manquant ? Il faut tenir compte de l'ensemble des données pour déterminer comment les mesures de protection fonctionnent et quelles autres lacunes ou vulnérabilités pourraient être exploitées par des menaces pour compromettre les actifs évalués. Les évaluateurs sont souvent en mesure de déterminer que les vulnérabilités connexes associées à la protection, n'exécutant pas une fonction spécifique, donneront une cote de vulnérabilité plus fiable pour cette fonction manquante. En combinant la vulnérabilité primaire précédente avec cette nouvelle notation (une nouvelle notation de PC ou GR) permet de déterminer la vulnérabilité réelle.

Tableau 11: Tableau de Vulnérabilité EMR — Scénario Simple

Incidence sur la gravité des conséquences (détection, réaction et reprise)	Incidence sur la probabilité de compromission		
	Faible (s.o.)	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très élevée
Moyenne	Faible	Moyenne	Élevée
Faible (s.o.)	Très faible	Faible	Moyenne

Alt Text: Le graphique ci-dessus illustre le processus de calcul des niveaux de vulnérabilité à partir de la méthodologie EMR en utilisant le tableau d'évaluation de la vulnérabilité de base

Exemple: La protection utilisée est un verrou inadéquat sur une porte pour empêcher l'accès à un entrepôt qui fait peu pour empêcher l'accès non autorisé et le vol. On peut déterminer que cette mesure de protection inefficace a une faible fonction de prévention, ce qui donne une valeur de PC élevée. Le verrou seul n'effectue pas de détection, de réponse ou de récupération. Cela signifie que, selon les critères d'une évaluation de la vulnérabilité de base, cette faiblesse justifierait un faible ou S/O pour GR. Cela signifie que la cote de vulnérabilité totale serait plafonnée à la moyenne. Ce n'est pas un calcul fiable pour la cote de vulnérabilité globale ou réelle de l'entrepôt, car on n'a pas tenu compte du tableau d'ensemble, comme toute autre mesure de protection (ou absence de mesure) pour obtenir correctement cette cote de vulnérabilité. Supposons que l'entrepôt ne dispose pas de gardes de sécurité ni d'alarmes anti-intrusion pour détecter les entrées non autorisées. Lorsque vous appliquez les critères d'évaluation de la vulnérabilité étendue, vous devez tenir compte de tout autre mécanisme qui pourrait remplir la valeur manquante de GR et puisqu'il n'y en a pas qui pourraient influencer le GR pour l'entrepôt, et compléter la capacité de sauvegarde de la serrure, cela donnerait une cote élevée pour GR. Lorsque l'on considère la valeur PC précédemment identifiée comme étant élevée (le verrou faible) avec la valeur de haute nouvellement calculée pour la GR (aucune autre mesure de protection en place), on obtient un calcul de cote de vulnérabilité élevée x élevées = très élevée dans l'ensemble, une conclusion beaucoup plus réaliste.

Scénario Composé

Contrairement au scénario simple qui ne considère qu'une seule valeur manquante pour les calculs de vulnérabilité (soit PC ou GR), il devient un peu compliqué lorsque des vulnérabilités peuvent affecter à la fois le PC et le GR. Lorsque c'est le cas, les évaluateurs devraient tenir compte des éléments suivants lorsqu'ils recalculent une valeur faible ou N/A pour une valeur manquante de PC ou de GR :

- Commencez par identifier la valeur Faible ou NA pour la vulnérabilité manquante ou la fonction de sauvegarde (PC ou GR). Cette valeur manquante représente la valeur que la mesure de protection n'effectue pas — la valeur que vous

déterminerez au moyen de l'évaluation approfondie de la vulnérabilité ;

- Après avoir identifié la valeur manquante pour le PC ou le GR, considérer la valeur primaire que la mesure de sauvegarde effectue (une fonction de prévention PC ou une fonction de détection, de réponse ou de récupération GR). Y a-t-il d'autres mesures de protection qui remplissent la même fonction ? Si oui, quelles sont ces valeurs ? (Faible, Moyen ou Élevé) ;
- Si les cotes de ces autres mesures de protection sont identiques à celles de la mesure de protection évaluée (mêmes niveaux pour la fonction principale des mesures de protection [PC ou GR]), analyser la valeur de vulnérabilité manquante (la faible ou la N/A PC ou GR) utiliser le même format du scénario simple — envisager d'autres mesures de protection qui n'exécutent que la valeur faible ou N/A et conserver la valeur de la mesure de protection primaire;
- Si les valeurs primaires des mesures de protection diffèrent (la mesure de protection analysée pour la vulnérabilité étendue est plus ou moins efficace dans sa fonction primaire par rapport aux autres mesures de protection qui remplissent des fonctions similaires), les évaluateurs devront hiérarchiser la valeur la plus élevée ou la plus faible (la protection la plus efficace ou la moins efficace — la vulnérabilité la plus basse ou la plus élevée) pour l'évaluation de la vulnérabilité étendue. Les critères suivants peuvent aider à déterminer quelles valeurs prioriser dans ces circonstances:
    - Si la vulnérabilité plus grave est compensée par une mesure de sauvegarde plus efficace avec une cote de vulnérabilité inférieure, utiliser la valeur inférieure pour le calcul de la valeur primaire dans l'évaluation de la vulnérabilité étendue ;
    - Si la vulnérabilité plus grave compromet l'efficacité de la sauvegarde moins vulnérable, utiliser la valeur supérieure pour le calcul de la valeur primaire dans l'évaluation de la vulnérabilité étendue.

Exemple: Reconsidérer l'entrepôt avec un verrou inefficace, il avait une vulnérabilité moyenne en utilisant l'évaluation de vulnérabilité de base, et maintenant ajouter un garde de sécurité bien formé. La nouvelle mesure de sauvegarde pourrait être évaluée individuellement comme étant faible pour l'évaluation de la vulnérabilité, car elle offre une capacité de détection et d'intervention très efficace. Si le garde a une capacité de prévention modérément efficace, moyenne, et une capacité de détection et d'intervention très efficace, faible, la cote de vulnérabilité globale pour la protection du garde serait basse (moyenne x faible = faible).

Alors que le garde exécute à la fois une fonction de prévention (PC) et une fonction de détection, de réponse et de récupération (GR), notre jeu de verrous n'effectue qu'une seule de ces fonctions (GR). Si le verrou était également modérément efficace pour empêcher l'accès non autorisé à l'entrepôt, une cote de moyen pour la protection des témoins, la même que celle du gardien, nous pourrions appliquer un scénario simple pour calculer la fonction de détection, de réponse ou de récupération manquante pour le verrou en utilisant la valeur du gardien. Dans ce cas, les évaluateurs ont deux valeurs

primaires différentes pour la PC (élevée pour le verrouillage et moyenne pour le garde), et une seule peut être sélectionnée pour l'évaluation de vulnérabilité étendue de l'impact GR de l'antivol. Si le verrouillage faible est peu susceptible d'affecter la capacité du gardien à effectuer une fonction de prévention modérément efficace, il faut utiliser la cote inférieure de Moyenne (la fonction de sécurité de prévention du gardien). Si l'on peut exploiter le verrou et que le gardien n'est pas en mesure d'intervenir, ce qui compromet l'efficacité du gardien, il faut utiliser la cote de sécurité élevé (fonction de prévention de la serrure).

Le calcul du niveau de vulnérabilité global fondé sur l'évaluation approfondie de la vulnérabilité serait soit faible, soit moyen pour les vulnérabilités connexes. Cela dépend de la façon dont les fonctions de prévention interagissent en fonction des deux mesures de protection. Il n'est pas toujours facile de déterminer ou de clarifier comment les vulnérabilités interagissent, et la plupart des mesures de protection devraient être évaluées en tandem parce qu'un bâtiment, une zone ou une région aura probablement plusieurs mesures de protection en place. Ce processus souligne l'importance de considérer les vulnérabilités et les mesures de protection dans leur ensemble, plutôt que de les examiner individuellement. La performance d'une mesure de sauvegarde pourrait être compromise par une mesure de sauvegarde moins efficace, ou une série de mesures de sauvegarde ensemble fournirait la meilleure protection globale pour les actifs contre les menaces.

Une fois que toutes les vulnérabilités ont reçu une note basée sur une comparaison entre le PC et le GR, tous les renseignements sont compilés pour produire une liste exhaustive des vulnérabilités qui peuvent être classées de la plus grave à la moins grave. En triant les niveaux de vulnérabilité de très élevé à très faible, vous pouvez rapidement hiérarchiser les vulnérabilités individuelles et identifier celles qui sont les plus importantes et qui doivent être traitées en premier,

Tableau 12: Tableau de Vulnérabilité EMR — Scénario Composé

Incidence sur la gravité des conséquences (détection, réaction et reprise)	Incidence sur la probabilité de compromission (prévention)		
	Faible (S.O.)	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très élevée
Moyenne	Faible	Moyenne	Élevée
Faible (s.o.)	Très faible	Faible	Moyenne

Alt Text: Le graphique ci-dessus illustre le processus de calcul des niveaux de vulnérabilité à partir de la méthodologie EMR en utilisant le tableau d'évaluation de la vulnérabilité de base

Tableau 13: Tableau de Calcul des Vulnérabilités Prolongées

Sauvegarde	Impact de la PC (prévention)		SoC Impact (détection, réponse, récupération)		Niveau de vulnérabilité
Serrure	Élevé	X	Faible (ou aucun)	=	Moyen
Garde	Moyen	X	Faible	=	Faible

Alt text: Le graphique ci-dessus illustre les mesures de protection choisies à prendre en compte dans le scénario composé afin d'effectuer une évaluation approfondie de la vulnérabilité lorsqu'elles ont une incidence sur la PC et la GR.

9.2. Calcul du Risque Résiduel

Le risque résiduel représente la quantité de risque restant, après détermination des valeurs pour les données sur les actifs, les menaces et la vulnérabilité. Un calcul du risque résiduel consiste à déterminer les niveaux de risque résiduels qui vont de très faible à très élevé en fonction de la valeur des actifs identifiés au cours de l'évaluation, des menaces susceptibles de compromettre ces actifs, employés et services et de toute vulnérabilité connexe. Diverses méthodes d'EMR inciteront les évaluateurs à utiliser un calcul mathématique de base pour convertir les niveaux de risque en valeurs numériques qui peuvent être comparées ensemble pour exprimer un niveau total de risque résiduel. Dans l'EMR, le risque est fonction des valeurs de l'actif, de la menace et de la vulnérabilité ou R = f (Aval, T, V). Chaque valeur est multipliée pour donner une note globale de risque. Cela permet d'être plus précis pour déterminer quel risque doit être traité en premier et comment chaque risque devrait être géré en conséquence, selon la liste des priorités.

Tableau 14: Valeurs Alpha des Risques Résiduels pour les Cotes de Risque Numériques

Valeurs des actifs, menaces et vulnérabilités	très faible	faible	moyennes	élevées	très élevées
Cotes pour le calcul du risque	1	2	3	4	5

Cote de risque de base	1-4	5-12	15-32	36-75	80-125
niveau de risque	très faible	faible	moyen	élevé	très élevé

Alt Text: Les graphiques ci-dessus représentent des graphiques de la méthodologie EMR pour calculer les cotes de risque et s'aligner sur les valeurs alpha.

Dans le cadre de l'analyse, on a attribué un niveau de très faible à très élevé à chacune des trois variables (actifs, menaces et vulnérabilités). Pour déterminer le risque résiduel, il faut attribuer à chacun des trois facteurs, soit les valeurs de l'actif, de la menace et de la vulnérabilité, une note numérique allant d'un à cinq, conformément à la première moitié du tableau 16 ci-dessus. Une fois que les niveaux de risque sont évalués numériquement, d'un à cinq pour chaque variable, les résultats finaux du risque résiduel peuvent varier de 1 à 125 (actif x menaces x vulnérabilités).

Par exemple, la valeur d'un actif est de (5) x la valeur de la menace (5) x la valeur de la vulnérabilité (5), ce qui donne une cote de risque globale de 125.

Lorsque l'on calcule le risque résiduel à l'aide de l'EMR, les évaluateurs doivent se rappeler de bien peu de choses lorsqu'ils choisissent les niveaux à utiliser dans la formule du risque résiduel de la TRRA.

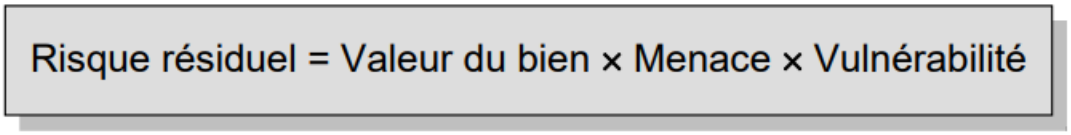
- **Menaces multiples affectant le même actif:** Étant donné que les biens peuvent être affectés par de multiples menaces (parfois avec des niveaux globaux de menace différents), les évaluateurs devraient créer des entrées distinctes pour les biens en fonction de la menace qui les affecte. Cela permettra d'utiliser un niveau global de biens et de menaces pour le calcul et les vulnérabilités sélectionnées spécifiquement pour le scénario de menace ;

- **Multiples vulnérabilités affectant le même actif :** Il arrive souvent qu'un actif puisse être exposé à des blessures en raison de multiples vulnérabilités, soit de mesures de protection déficientes, soit de vulnérabilités connexes. Lorsqu'ils choisissent parmi plusieurs vulnérabilités pour déterminer un niveau de vulnérabilité globale pour l'actif, les évaluateurs doivent hiérarchiser les vulnérabilités globales les plus élevées en fonction du scénario de menace à analyser. S'il y a plus d'une vulnérabilité avec le niveau le plus élevé pour le scénario, les évaluateurs peuvent utiliser ce niveau et expliquer dans leur justification que le niveau de vulnérabilité le plus élevé représente les diverses vulnérabilités élevées, puis fournir une description de ces vulnérabilités.

  Lorsqu'ils examinent les vulnérabilités qui représentent le plus haut niveau de vulnérabilité, les évaluateurs devraient veiller à bien examiner et protéger le rendement et l'évaluation approfondie de la vulnérabilité lors de la détermination et de la priorisation des vulnérabilités.

Il y a des cas où l'on utilise les niveaux précédents de très faible à très élevé, ce qui permettrait une hiérarchisation inappropriée des risques pour traiter d'abord. Par exemple, si vous avez deux risques qui sont de niveau élevé, il peut être difficile de déterminer quel risque doit être priorisé sur l'autre. Si un niveau de risque élevé se traduit par une cote de risque de 36 et que l'autre se traduit par une cote de risque de 45, la cote de risque de 45 (niveau de risque élevé) doit être prioritaire en premier dans la liste.

Tableau 15: Calcul du Risque Résiduel



Alt Text: Le graphique ci-dessus présente le calcul pour déterminer les niveaux de risque résiduel

9.2.1. Liste des Risques Résiduels par Ordre de Priorité

La dernière étape du calcul du risque résiduel consiste à compiler toutes les données dans une liste hiérarchisée. Cette liste de risques résiduels devrait être classée du plus grave au moins grave (très élevé à très faible). Comme nous l'avons déjà mentionné, l'attribution d'une valeur numérique permettra d'être plus précis, car les risques résiduels les plus élevés devront être traités en premier et seront mentionnés dans toute recommandation, à la prochaine étape de l'évaluation.

10. Recommandations

Les recommandations, lorsqu'elles sont approuvées et mises en œuvre, devraient réduire les niveaux inacceptables de risques résiduels à des niveaux acceptables. En concluant le processus d'EMR, les évaluateurs comparent leurs notes de risque résiduel avec le niveau de tolérance au risque établi pour l'évaluation. Si des risques se situent en dehors des seuils acceptables, les évaluateurs doivent effectuer une analyse supplémentaire pour modifier les mesures de protection existantes ou ajouter des mesures supplémentaires afin d'améliorer les vulnérabilités identifiées ou de réduire la gravité des menaces contre les actifs. Les évaluateurs devraient classer leurs recommandations en fonction de l'incidence qu'elles auront sur le risque résiduel.

Il est important de noter que l'autorité responsable des risques peut choisir de rejeter une recommandation visant à réduire le risque résiduel et d'accepter un niveau de risque résiduel plus élevé. Il convient de noter ces données à titre de référence. L'étape des recommandations d'un projet d'EMR comprend les éléments suivants:

- Identification des risques inacceptables;
- Sélection des mesures de sauvegarde potentielles;
- Évaluation des risques résiduels projetés.

10.1. Identification des Risques Inacceptables

Pour déterminer si un risque est inacceptable, la tolérance au risque définie dans la phase de préparation est comparée à celle de liste des risques résiduels par ordre de priorité. Tout risque résiduel qui dépasse le niveau de tolérance au risque défini est inacceptable et nécessite des recommandations d'atténuation pouvant réduire le niveau de risque au niveau de tolérance au risque approuvé.

10.2. Sélection des Mesures de Sauvegarde Potentielles

Chaque risque inacceptable identifié devrait recommander une ou plusieurs stratégies pour atténuer le risque. L'un des moyens les plus efficaces de réduire le risque résiduel consiste à ajouter ou à modifier les mesures de protection existantes pour tous les actifs évalués aux fins de l'évaluation. Efficace sauvegarde, il s'acquittera des fonctions de PDIR appropriées, réduira les vulnérabilités et les impacts des menaces et servira à atténuer plusieurs vulnérabilités en même temps. L'évaluateur doit s'assurer que les recommandations d'atténuation proposées sont raisonnables. Cette information est nécessaire pour que le signataire puisse prendre une décision compréhensive concernant la mise en œuvre. Ils évalueront la possibilité d'accepter un risque plus élevé, d'augmenter le budget ou de prolonger le calendrier du projet.

10.3. Évaluation du Risque Résiduel Projeté

Une fois que l'équipe EMR a déterminé et proposé des mesures de protection pour atténuer les risques qui dépassent les niveaux établis de tolérance au risque, ces recommandations sont évaluées afin de déterminer leur risque résiduel projeté une fois mis en œuvre. Pour le déterminer, retournez à Évaluation de la vulnérabilité et Calcul du risque résiduel et de compléter ces phases à nouveau en utilisant les données des mesures de sauvegarde proposées. Il est peu probable que les mesures de protection proposées contiennent des données historiques sur le site, et elles nécessiteront donc une collecte par d'autres moyens. Cela peut se faire par l'entremise de spécifications fournies par le fabricant, en examinant les offres de services des entreprises sous contrat ou en analysant les données d'installations similaires qui utilisent la mesure de sauvegarde dans leurs activités. Cela vous donnera une projection du risque résiduel dans le cas où les mesures de protection proposées seraient mises en œuvre.

Si les mesures de sauvegarde proposées ne font pas que le risque résiduel projeté est égal ou inférieur au niveau de tolérance au risque, répéter la section Sélection des mesures de sauvegarde potentielles, et Évaluation du risque résiduel projeté jusqu'à ce qu'une mesure de sauvegarde proposée ramène le risque résiduel dans des limites acceptables, ou jusqu'à ce que tous les efforts d'atténuation plausibles aient été étudiés. Le but de ce processus est de réduire le niveau de risque au plus bas niveau possible, idéalement à un niveau de tolérance au risque établi ou inférieur. Il peut y avoir des cas où la menace ou les vulnérabilités présentes peuvent rendre impossible d'atteindre le niveau de tolérance au risque souhaité; Dans ces cas, les commanditaires du projet doivent envisager officiellement d'accepter un niveau de risque plus élevé. Toutes les évaluations et recommandations, y compris celles qui n'atteignent pas la cote de risque résiduel souhaitée, devraient être incluses dans le rapport final. La possibilité de réduire le risque même si le niveau cible n'est pas atteint peut-être bénéfique pour une note globale des risques globaux.

11. Conclusion — Rapport final d'EMR

Ce document final est une compilation de toutes les informations recueillies jusqu'à présent, dans un seul document qui doit être présenté aux autorités responsables de l'acceptation des risques. Les renseignements présentés doivent être concis pour justifier la nécessité de toute recommandation. Chaque section devrait porter sur les questions les plus importantes à présenter à la direction pour examen, en laissant des renseignements plus détaillés dans les tableaux de synthèse et la documentation justificative.

Le plan du rapport final sur l'EMR devrait comprendre :

- **Résumé Exécutif —** Un résumé de toutes les phases de l'EMR et de leurs résultats. Un résumé devrait être aussi concis que possible tout en présentant le résultat de chaque phase pour fournir les informations pertinentes en un coup d'œil;
- **Contexte —** Fournir des renseignements sur l'organisation, son mandat et la prestation de services, les lieux évalués et tout autre renseignement qui pourrait fournir le contexte nécessaire;
- **Viser —** Une explication des raisons pour lesquelles l'EMR est lancée et de la façon dont le rapport final est utilisé;
- **Mandat —** Une compilation des informations recueillies dans Mandat et portée du projet;
- **Portée —** Une ventilation détaillée de la portée de l'évaluation, comme expliquée dans Mandat et portée du projet;
- **Identification et évaluation des Actifs —** Une description détaillée de tous les actifs visés par l'évaluation et de leur valeur, telle que décrite dans Identification et évaluation des actifs;
- **Évaluation des Menaces —** Une description détaillée de toutes les menaces identifiées et de leurs répercussions sur la prestation des services, comme décrite dans l'évaluation de la menace;
- **Évaluation de la Vulnérabilité —** Une description complète des vulnérabilités déterminées au cours de la phase d'évaluation de la vulnérabilité, comme décrit dans sous-phase de l'évaluation de la vulnérabilité;
- **Évaluation des Risques Résiduels —** Une ventilation détaillée de l'évaluation du risque résiduel, la façon dont elle a été déterminée et toute information à l'appui requise, comme décrit dans Calcul de la sous-phase du risque résiduel;
- **Recommandations —** Une description de toutes les recommandations, ce qu'elles sont, pour quoi elles ont été choisies et ce qu'elles visent à régler. Il suffit de dire ce qui doit être fait sans préciser comment, pourquoi et quels sont les résultats pour que vos recommandations soient acceptées et mises en œuvre. Ceci est décrit dans recommandations;
- **Toute pièce jointe, tout renvoi ou tout document justificatif —** Tous les renseignements et documents utilisés pour remplir l'EMR, y compris, sans s'y limiter, les procès-verbaux d'entrevue, les données du rapport de police, les documents de recherche et les renseignements sur le produit.

11.1. Rapport d'approbation — Rôle(s) des Autorités Responsables de l'Acceptation des Risques

Une fois que tous les renseignements ont été compilés dans un rapport final, l'autorité d'acceptation des risques, tels qu'elle est indiquée dans la phase de préparation signe pour terminer l'EMR. L'EMR n'est pas considérée comme définitive avant que cette étape ne soit terminée.

Lors de la signature du rapport final d'EMR, le signataire indique quelles recommandations seront formulées, le cas échéant. Si les recommandations retenues ne permettent pas d'atteindre le niveau de tolérance au risque, l'autorité signataire doit alors accepter le risque résiduel plus élevé et consigner ce fait pour référence future. Pour plus d'informations sur le processus d'acceptation des risques, consulter GSMGC-018 (2024) — Guide du processus de gestion des risques pour la sécurité matérielle.

Pour toutes les recommandations approuvées, des mesures devraient être mises en place pour s'assurer qu'elles sont exécutées dans les délais établis dans l'EMR. Un plan devrait également être élaboré pour examiner et évaluer les recommandations mises en œuvre après une période appropriée afin d'évaluer leur efficacité à réduire le risque résiduel au niveau acceptable. Des détails sur ce processus sont disponibles à l'adresse GSMGC-016 (2022) — u Guide du processus d'évaluation et d'autorisation de sécurité des installations.

12. Documents de référence et sources

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Niveaux de sécurité
- Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)
- Sécurité nationale
- International Atomic Energy Agency—Design Basis Threat (Lien anglais seulement)
- FEMA 430 Risk Management Series: Site And Urban Design For Security (Lien anglais seulement)
- FEMA 452 Risk Assessment: A How-To Guide To Mitigate Potential Terrorist Attacks Against Buildings (Lien anglais seulement)
- National Protective Security Authority (UK)—Protective Security Risk Management (Lien anglais seulement)
- The National Risk Register (NRR) — (UK) (Lien anglais seulement)
- GSMGC-015 (2023)— Guide pour l'établissement des zones de sécurité matérielle
- GSMGC-018 Guide du processus de gestion des risques pour la sécurité matérielle
- GSMGC-019 (2023) — Guide de protection, de détection, de réponse et de récupération
- GSMGC-016 Guide du processus d'évaluation et d'autorisation de sécurité des installations

13. Promulgation

Révisé et recommandé en vue de l'approbation.

J'ai examiné le document GSMGC-022 (2025) — Guide d'évaluation des menaces et des risques, et je recommande son approbation.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2025.01.17 08:24:38 -05'00'

Shawn Nattress,
Gestionnaire
Principal organisme responsable de la sécurité matérielle de la GRC

Date

Approuvé

J'approuve par la présente le document GSMGC-022 (2025) — Guide d'évaluation des menaces et des risques.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2025.01.31 13:54:57 -05'00'

André St-Pierre,
Directeur, Sécurité matérielle
Gendarmerie royale du Canada

Date