BROCHURE D'INFORMATION SUR LA SÉCURITYÉ 5

Guide d'évaluation de la menace et des risques pour les technologies de l'information

november 1994

Le présent guide a été rédigé et publié par la Sous-direction de la sécurité des technologies de l'information de la GRC. Parmi les responsabilités que doit assumer la GRC, selon la Politique du Gouvernement du Canada sur la sécurité, il y a celles-ci: «élaborer, approuver et publier des documents techniques spéciaux relatifs à la sécurité des technologies de l'information (...) et prodiguer des conseils sur leur application» et «prodiguer, sur demande, des conseils sur l'évaluation de la menace et des risques». C'est avec l'intention de bien remplir son rôle d'organisme conseil que la GRC a entrepris la préparation de ce guide.

Table des matières

Table des matières

Guide d'évaluation de la menace et des risques pour les technologies de l'information

1. Introduction

Le présent guide a pour but d'aider les intéressés à évaluer les menaces et les risques auxquels sont exposés les biens liés aux technologies de l'information (TI) au sein de leur organisation, et à faire des recommandations concernant la sécurité de la TI. L'évaluation de la menace et des risques (ÉMR) vise à engager la participation de divers intervenants et à obtenir leur soutien, afin de permettre à la direction de prendre des décisions éclairées au sujet de la sécurité et de recommander des mesures de protection adéquates et économiques. L'ÉMR sert aussi à déterminer la pertinence des mesures de protection existantes et, s'il s'avère que celles-ci ne parviennent pas tout à fait à corriger les faiblesses relevées ou ne sont plus nécessaires, on peut alors recommander l'adoption de nouvelles mesures ou l'élimination des mesures devenues inutiles. L'ÉMR ne précise pas les mécanismes de prévention, de détection et d'intervention qu'il faut mettre en place pour réduire les risques; elle ne fait qu'indiquer les endroits où ces mécanismes doivent être appliqués et la priorité qu'il faut accorder à l'élaboration de tels mécanismes. Sous le rapport de la gestion des risques, l'ÉMR recommande des moyens de minimiser, d'éliminer et d'accepter les risques.

La planification de l'ÉMR comprend la délimitation du projet, le choix des méthodes appropriées, l'établissement du calendrier d'exécution, l'identification des intervenants clés et l'affectation de ressources au travail d'évaluation. Les personnes participant à l'ÉMR doivent être prévenues de la nécessité de préserver la nature délicate des documents de travail produits en cours de route. Ces documents renferment souvent des renseignements concernant la vulnérabilité des systèmes et des milieux d'exploitation, et on devrait leur fournir une protection équivalente à celle qui est accordée aux renseignements les plus confidentiels que l'on trouve dans ces systèmes.

Il faut prendre en considération certaines particularités de l'organisation qui pourraient commander des mesures de sécurité plus strictes, par exemple le mandat de l'organisation, son emplacement (c.-à-d. son éloignement), le milieu où elle se trouve («hostile», ouvert au public) et sa composition, c'est-à-dire ses ressources.

2. Marche à suivre

L'évaluation de la menace et des risques comporte habituellement les quatre étapes suivantes:

Préparation:	Determiner ce qu'il faut protéger;
Évaluation de la menace:	Determiner contre quoi il faut se protéger et les consequences d'une menace;
Évaluation des risques:	Determiner si les mesures de protection actuelles ou proposes sont satisfaisantes; et
Recommand-ations:	Determiner ce qu'il faudrait faire pour réduire les risques à un niveau acceptable pour la haute direction.

Chacune des ces étapes est décrite en détail dans les pages qui suivent.

2.1. Préparation

2.1.1. Définition du milieu

a) Déterminer l'évaluation de la menace et des risques

Avant de procéder à l'ÉMR comme telle, il est nécessaire d'en déterminer l'étendue, par exemple les systèmes à l'étude, l'interconnexion avec les autres systèmes et le profil des utilisateurs. L'ÉMR porte souvent sur plusieurs systèmes et milieux d'exploitation, de là la nécessité d'établir un ordre de priorité au moment de fixer l'étendue du projet, de telle sorte que les principaux sujets de préoccupation ou points sensibles soient évalués en premier.

b) Identifier les participants

Une fois qu'il a déterminé l'étendue de l'ÉMR, le praticien peut former une équipe

représentative d'utilisateurs du système à l'étude. Supposons, par exemple, que le système renferme plusieurs applications utilisées par divers groupes à l'intérieur de l'organisation. Afin de pouvoir disposer de tous les renseignements requis pour l'ÉMR, il faut constituer une équipe composée d'utilisateurs, de concepteurs, de préposés aux télécommunications et de personnel opérationnel. Une telle équipe fournira plus tard au praticien les renseignements dont il a besoin pour dresser la liste des menaces connues et mesurer leur incidence possible.

c) Déterminer les préoccupations intrinsèques

Toutes les organisations ont certaines préoccupations en matière de sécurité qui sont liées directement à la nature de leurs affaires. Le praticien doit prendre note de ces préoccupations car elles serviront à déterminer l'opportunité des mesures de sécurité existantes et à recommander des améliorations à ce chapitre.

d) Définir les conditions de base

Une fois terminé le travail préliminaire, le praticien peut établir le profil actuel de l'organisation en matière de sécurité. Ces paramètres représentent ce qu'on appelle les conditions de base sur le plan de la sécurité, à partir desquelles il est possible d'évaluer les risques et d'actualiser l'ÉMR. Par exemple, lorsqu'une mesure de protection quelconque est recommandée, cette mesure ainsi que la recommandation sont comparées aux conditions de base. Celles-ci sont nécessaires pour deux raisons:

1) elles fournissent un point de départ pour mesurer les progrès réalisés;

2) le milieu est sujet à des changements continus.

Dans le premier cas, les conditions de base permettent au praticien de constater les changements qui ont été apportés au milieu, et l'incidence de ces changements sur la sécurité. Dans le second cas, elles lui permettent de voir la différence entre le profil de sécurité actuel et les exigences futures en matière de sécurité, compte tenu des modifications apportées au milieu depuis que les conditions de base ont été établies.

2.1.2. Inventaire et évaluation des biens

L'inventaire des biens de TI selon leurs regroupements physiques ou logiques peut s'avérer difficile, tout dépendant de la taille de l'organisation et de la qualité des activités auxiliaires, telles que la gestion du matériel et la production d'inventaires complets. Le praticien doit faire la liste des biens associés à la TI et leur attribuer une valeur. Les participants désignés à l'étape préliminaire l'aideront dans cette tâche. Les «propriétaires des renseignements traités à l'aide des applications de TI ont la responsabilité de préparer les énoncés de la nature délicate[1], où sont précisées les exigences particulières de chaque application en matière de confidentialité, d'intégrité et de disponibilité.

Le praticien doit tenir compte de plusieurs aspects contribuant à la valeur d'un bien, dont le prix coûtant de ce bien. Un bien peut avoir une valeur **acquise** qui dépasse de beaucoup son coût original. Prenons par exemple les données recueillies par des géologues en faisant l'inspection d'une région nordique éloignée pendant l'été. Les géologues avaient peut-être l'intention de les glaner pendant que l'endroit était accessible, pour les interpréter et les analyser plus tard durant les mois d'hiver. La valeur des données pouvait alors correspondre aux coûts de déplacement, de soutien et d'occupation des scientifiques pour toute la durée de l'inspection. Or, supposons un instant que les données aient été perdues en septembre. Comme la région n'aurait pas été accessible avant le printemps suivant, les géologues auraient perdu une année entière de travail, en plus du coût de l'inspection initiale, puisqu'il aurait fallu tout recommencer l'été suivant. À la valeur originale des biens on devait donc ajouter dans ce cas-là les coûts liés au soutien, au temps de travail et aux déplacements pour une année supplémentaire, ainsi

[1] Le paragraphe 2.1.4 porte sur l'énoncé de la nature délicate

qu'une valeur dénotant la spécificité sous le rapport du temps, des conditions et de l'opportunité.

Il faut aussi examiner la question de l'utilisation de méthodes qualitatives ou quantitatives afin de déterminer la valeur des biens. Quand on veut connaître la valeur acquise de certains biens, au lieu d'attribuer à ceux-ci une valeur monétaire, il est peut-être plus juste d'établir leur valeur relative, compte tenu des objectifs et du mandat de l'organisation, valeur dont témoignent les exigences en matière de confidentialité, d'intégrité et de disponibilité fixées pour ces biens.

2.1.3. Exigences en matière de confidentialité, d'intégrité et de disponibilité (CID)

Les exigences en matière de CID sont indiquées dans les énoncés de la nature délicate, dont il est question au paragraphe 2.1.4.

Confidentialité
La confidentialité a trait aux possibilités de divulgation. Dans certains cas, le degré de confidentialité peut varier en fonction du temps. Ainsi, certaines recherches peuvent devoir demeurer secrètes pendant que l'on recueille et que l'on traite les données, mais à partir du moment où celles-ci sont publiées et deviennent un document public, elles n'exigent plus le même degré de confidentialité. D'autres données, cependant, peuvent devenir plus confidentielles une fois regroupées, par exemple des renseignements sur l'approvisionnement d'unités individuelles qui, lorsque réunis, aident à concevoir la logistique appliquée aux déplacements de l'armée.

Afin d'évaluer les effets d'une perte de confidentialité, le praticien doit mettre en rapport le degré de sensibilité des données et les conséquences d'une divulgation inopportune. Les données doivent être classées ou désignées correctement à l'un des niveaux suivants :

NON CLASSIFIÉ OU NON DÉSIGNÉ	renseignements de base
DÉSIGNÉ	divers niveaux, renseignements personnels, renseignements délicats sur l'entreprise
CONFIDENTIEL	une atteinte à l'intégrité pourrait porter préjudice à l'intérêt national
SECRET	une atteinte à l'intégrité pourrait porter un grave préjudice à l'intérêt national
TRÈS SECRET	une atteinte à l'intégrité pourrait porter un préjudice exceptionnellement grave à l'intérêt national

L'aide-mémoire pour l'évaluation de la confidentialité (Tableau 1) énonce quelques-unes des questions auxquelles il faut répondre au moment de l'évaluation des exigences en matière de confidentialité du système ou des renseignements qu'il contient.

AIDE-MÉMOIRE POUR L'ÉVALUATION DE LA CONFIDENTIALITÉ	
	Les renseignements sont-ils délicats, eu égard à l'intérêt national, c.-à-d. classifiés?
	S'agit-il de renseignements personnels?
	Quelles seraient les consequences d'une perte de confidentialité de ces renseignements?

TABLEAU 1 – Confidentialité

Intégrité
L'intégrité se rapporte à l'exactitude et à l'intégralité des renseignements contenus dans le système et du système lui-même. Lorsque les exigences en matière d'intégrité sont élevées, comme c'est le

cas pour les transactions financières dans les systèmes bancaires, les pertes financières possibles fournissent une indication des sommes et des efforts qui doivent être investis dans les mesures de protection.

L'aide-mémoire pour l'évaluation de l'intégrité (Tableau 2) indique quelques aspects à envisager au moment de l'évaluation des exigences en matière d'intégrité du système ou des renseignements qu'il contient.

AIDE-MÉMOIRE POUR L'ÉVALUATION DE L'INTÉGRITÉ	
	Les effets de données inexactes
	Les effets de données incomplètes

TABLEAU 2 – Intégrité

Disponibilité

Le système, pour être considéré disponible, doit être en place et utilisable aux fins voulues. La possibilité d'une perte complète de la fonction de traitement des données est bien mince, mais elle existe néanmoins. Chose certaine, les utilisateurs doivent parfois composer avec des périodes d'indisponibilité plus ou moins longues. Le praticien doit aider les utilisateurs à déterminer à quel point ils comptent sur la disponibilité du système pour offrir le service attendu. Ceux-ci doivent définir clairement, pour les préposés au système, la durée maximale acceptable d'indisponibilité. Sous ce rapport, le terme «disponibilité» a trait à la continuité du service.

Pour établir l'ordre de priorité du traitement d'après les exigences en matière de disponibilité, le praticien se voit souvent obligé de se poser en arbitre entre les différents groupes d'utilisateurs et de les amener à s'entendre sur l'importance relative des applications pour chaque groupe. Le praticien doit aussi reconnaître que ces exigences changent souvent pendant la durée de vie des applications. Les utilisateurs doivent noter, pour les préposés au système, les effets d'une perte de disponibilité du système de TI, du personnel de soutien et des données.

Les services jugés ***essentiels ou d'une importance capitale pour l'organisation*** doivent être connus. Comme ces services ont un grand besoin de disponibilité, il faut porter une attention spéciale aux ressources de soutien ainsi qu'aux aspects environnementaux qui touchent la prestation de services.

Le praticien doit reconnaître tous les éléments critiques contribuant à la prestation des services essentiels qui pourraient être vulnérables aux menaces. De tels éléments sont aussi considérés comme des «biens» aux fins de l'ÉMR.

L'aide-mémoire pour l'évaluation de la disponibilité (Tableau 3) énumère certains aspects à considérer au moment de l'évaluation des exigences en matière de disponibilité.

AIDE-MÉMOIRE POUR L'ÉVALUATION DE LA DISPONIBILITÉ	
	Les modifications aux exigences de disponibilité pendant le cycle de vie du système
	Les effets notés d'une perte de disponibilité
	Les périodes maximales acceptables d'indisponibilité

TABLEAU 3 – Disponibilité

2.1.4. Énoncés de la nature délicate

Les exigences en matière de CID sont indiquées dans les énoncés de la nature délicate (ÉND). La préparation d'un énoncé de la nature délicate[2] doit tre une condition préalable la mise en place

[2] L'Annexe B fournit un exemple d'énoncé de la nature delicate.

d'une nouvelle application ou à l'apport de modifications aux applications existantes. Les applications conçues et mises en place sans énoncés de la nature délicate souvent ne présentent pas les exigences en matière de sécurité nécessaires pour protéger adéquatement les renseignements présents dans le système. Il appartient au centre de décision qui utilise l'application, en est le propriétaire ou y verse des données, de préparer l'énoncé de la nature délicate. L'analyse menant à la rédaction de ce document est parfois exécutée par différentes personnes qui chacune ont un intérêt particulier dans le système ou les données à l'étude.

Le groupe représentant les utilisateurs qui participe à la rédaction de l'énoncé de la nature délicate peut se composer d'une ou de plusieurs personnes, selon la taille et la complexité de l'application en question.

Un énoncé séparé est requis pour chaque application importante tournant déjà sur un système informatique ou qu'on prévoit installer. Par exemple, l'application de la paye et celle des inventaires nécessiteraient chacune un énoncé distinct, même si elles devaient être exécutées sur le même système. L'évaluation de la nature délicate n'est pas nécessairement liée aux coûts d'acquisition ou de remplacement, mais plutôt à une valeur relative attribuée aux exigences de l'application en matière de confidentialité, d'intégrité et de disponibilité.

2.2. Évaluation de la menace

La seconde étape de l'ÉMR est l'***évaluation de la menace***. Soulignons ici les concepts de catégories, de probabilité, de conséquences, d'incidence et de vulnérabilité. Des menaces telles que des tremblements de terre, des tentatives de piratage informatique, des attaques de virus, etc., sont classées par catégories, selon la nature de l'atteinte à l'intégrité des biens. La Figure 1 renferme des exemples de menaces dans chaque catégorie.

CATÉGORIE DE MENACES	EXEMPLES DE MENACES
DIVULGATION	Signaux compromettants Interception Procédures d'entretien inadéquates Piratage informatique
INTERRUPTION	Tremblement de terre Incendie Inondation Code pernicieux Panne de courant
MODIFICATION	Erreur d'entrée de données Piratage informatique Code pernicieux
DESTRUCTION	Tremblement de terre Incendie Inondation Pointes de courant
ENLÈVEMENT	Vol de données Vol de systèmes

FIGURE 1 – Exemples de menaces

2.2.1. Description de la menace

Les menaces pouvant guetter les biens à l'étude doivent être décrites par le praticien. Elles peuvent être de nature accidentelle ou intentionnelle.

2.2.2. Catégories de menaces

Il existe cinq grandes ***catégories*** de menaces: divulgation, interruption, modification, destruction et enlèvement ou perte.

Divulgation
Les biens exigeant une grande **confidentialité** sont vulnérables à la **divulgation**. Cette catégorie de menaces met les biens sensibles en danger par la

divulgation non autorisée de renseignements de nature délicate.

Interruption
L'interruption touche principalement les services en s'attaquant à leur **disponibilité**. Une panne de courant est un exemple parfait de menace entrant dans cette catégorie.

Modification
Ce genre de menace compromet essentiellement l'**intégrité** des biens, laquelle, selon la PGS, englobe l'exactitude et l'intégralité des renseignements. Une tentative de piratage informatique ferait partie de cette catégorie s'il y avait des changements d'apportés.

Destruction
Tout ce qui détruit ou contribue à détruire les biens entre dans cette catégorie. Les biens qui nécessitent une grande **disponibilité** sont particulièrement vulnérables à la **destruction**. Les tremblements de terre, les inondations, les incendies et le vandalisme sont tous des éléments destructeurs.

Enlèvement ou perte
Lorsqu'un bien a été volé, perdu ou égaré, ce sont surtout les facteurs **confidentialité** et **disponibilité** qui sont en cause. Les ordinateurs portatifs ou portables sont particulièrement vulnérables à un enlèvement ou une perte.

2.2.3. Probabilité de realization de la menace

Le praticien doit déterminer le genre de menace qui guette chaque bien et, d'après l'expérience acquise et les renseignements fournis par les organismes responsables et d'autres sources, la probabilité que cette menace se concrétise.

Les niveaux de probabilité «faible», «moyenne» et «élevée» sont définis comme suit dans la Politique du gouvernement du Canada sur la sécurité:

On peut employer la mention **sans objet** pour indiquer que la menace n'est pas pertinente dans une situation donnée.

Faible signifie qu'il n'y a aucun précédent et qu'il est peu probable que la menace se concrétise.

Moyenne signifie qu'il y a des précédents et que la menace est vraisemblable.

Élevée signifie qu'il y a d'importants précédents et que la menace est fort probable.

2.2.4. Conséquences, incidence et exposition

Une fois qu'il a dressé la liste des biens et déterminé les genres de menaces auxquelles ils sont exposés, le praticien doit évaluer l'incidence d'une menace qui pourrait se concrétiser en l'absence de mesures de protection. Pour ce faire, le praticien doit comprendre et être en mesure de décrire les affaires de l'organisation. Il lui faut envisager les effets possibles sur le travail accompli, sur l'organisation elle-même et sur chacun de ses éléments qui comptent sur les renseignements ou les services offerts par les biens menacés.

Tout au cours de ce processus, le praticien cherche à répondre à la question suivante: «Quelle est la conséquence de chaque menace?» En d'autres termes, quels seraient les pertes ou autres effets, réels ou anticipés, que pourrait entraîner la réalisation de cette menace?

La Politique du gouvernement du Canada sur la sécurité propose un mécanisme de compte rendu des conséquences fondé sur l'évaluation du **préjudice**. Dans le cas des biens ou des renseignements classifiés ou désignés, on parlera de préjudices **moins graves**, **graves** ou **exceptionnellement graves**, et les conséquences pourraient être classées comme suit : «**perte de confiance**», «**atteinte au caractère confidentiel**», «**perte de bien**», «**perte de service**» ou

toute autre catégorie ainsi définie par le praticien.

La gravité des conséquences (exceptionnellement grave, grave, moins grave) peut varier selon les priorités de l'organisation ou du service. Par exemple, **une perte de confiance** peut constituer un **grave préjudice** dans un service et un **préjudice exceptionnellement grave** dans un autre service. L'**évaluation des conséquences** permet au praticien de déterminer l'incidence d'une menace pour l'organisation, eu égard aux coûts réels et perçus liés à une perte de confidentialité, d'intégrité ou de disponibilité.

En déterminant l'**exposition**, l'organisation peut classer les scénarios des risques selon la probabilité et les conséquences et ainsi accorder des priorités.

La cote de mesure de l'exposition pour les biens et les données est indiquée au Tableau 4, où l'incidence a préséance sur la probabilité. Ce tableau permet d'établir l'ordre de priorité des conséquences en prenant en considération la probabilité qu'une menace se concrétise et l'incidence qu'aurait cette menace sur l'organisation si elle devait se concrétiser. Le Tableau 4 fait abstraction des moyens de protection mis en oeuvre pour contrer chaque menace.

2.2.5. Résumé de l'évaluation de la menace

L'évaluation de la menace, telle que définie dans cette partie, comporte les étapes suivantes:

a) Décrire la **menace**, en précisant la nature, la forme et le moment où elle peut se concrétiser.

b) Classer la menace dans la **catégorie** pertinente.

c) Déterminer la **probabilité qu'elle se realise**.

d) Déterminer ses **consequences** sur les operations si elle devait se concrétiser.

		INCIDENCE (PRÉJUDICE)		
		Exception-nellement grave	Grave	Moins grave
PROBABILITÉ	ÉLEVÉE	9	8	5
	MOYENNE	7	6	3
	FAIBLE	4	2	1

TABLEAU 4
Degrés d'exposition des biens et des données[3]

e) Juger de la gravité de son **incidence** : moins grave, grave, exceptionnellement grave.

f) Attribuer une **cote de mesure de l'exposition** à chaque menace, selon sa gravité relative pour l'organisation.

g) **Déterminer l'ordre de priorité** des menaces, d'après les cotes de mesure mentionnées en f.

Le Tableau 5 est un exemple de feuille de récapitulation sur laquelle on peut inscrire des renseignements sur les menaces qui guettent chaque bien.

[3] À noter que, dans ce tableau, l'incidence a préséance sur la probabilité.

BIEN	ÉVALUATION DE LA MENACE					
	AGENT/ ÉVÉNEMENT	CATÉGORIE DE MENACES	PROBABILITÉ DE RÉALISATION	CONSÉQUENCES DE LA MENACE SI ELLE SE CONCRÉTISE	INCIDENCE (PRÉJUDICE)	COTE DE MESURE DE L'EXPOSITION
Décrire le bien.	Décrire l'événement ou l'agent menaçant.	Divulgation Interruption Modification Destruction Enlèvement	Faire Moyenne Élevée	Énumérer les consequences pour l'organisation de la menace, si elle devait se concrétiser.	Exceptionnel-lement grave, grave, moins grave.	Chiffre de 1 à 9.

TABLEAU 5 – Évaluation générale de la menace

2.3. Évaluation des risques

L'évaluation des risques est nécessaire afin de déterminer les risques courus par l'organisation lorsque les mesures de protection[4] existantes ou proposées sont jugées insuffisantes pour protéger le bien contre une menace donnée. Si les mesures en place ne sont pas adéquates, il faut noter et analyser les points faibles.

L'évaluation des risques est **«une évaluation des probabilités qu'on profite des points faibles, d'après l'efficacité des mesures de sécurité existantes ou proposées.»**

Cette définition fait de l'évaluation des risques une évaluation des points faibles et de la probabilité que l'un de ces points faibles soit exploité, malgré les mesures de sécurité existantes ou proposées.

2.3.1. Évaluation des mesures de protection existantes

La prochaine étape logique du processus d'ÉMR consiste à déterminer quelles mesures déjà en place peuvent contrer chacune des menaces constatées. Cela étant fait, le praticien peut évaluer la protection dont dispose l'organisation ou l'installation contre chaque menace et déterminer s'il subsiste des points faibles.

2.3.2. Points faibles

On devrait porter attention aux moments où le bien est le plus vulnérable, par exemple pendant les heures d'accès au public ou d'accès libre, ou pendant le transport. Il arrive que le niveau de confidentialité d'un bien soit lié au temps. Ainsi, des renseignements jugés confidentiels pendant qu'ils sont à l'étude ou en voie de compilation (p. ex. les données sur le budget) peuvent perdre leur caractère délicat dès qu'ils sont communiqués au public.

[4] L'évaluation des risques se fait de deux façons: d'abord à la lumière des mesures de protection en place, plus en tenant compte des mesures de protection proposées.

Il y a trois scénarios possibles dans le domaine de la sécurité. Le premier, illustré à la Figure 2, est la situation d'**équilibre**. C'est la situation idéale, où les menaces sont connues et les mesures de protection appropriées sont en place pour réduire les risques à un niveau acceptable pour la haute direction de l'organisation.

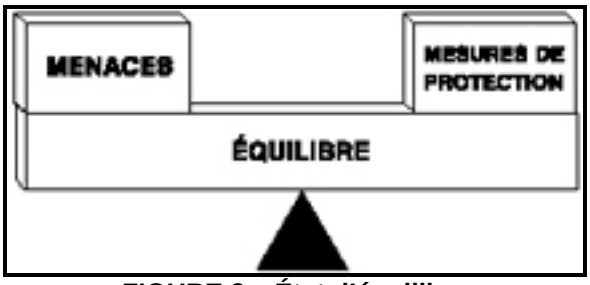

FIGURE 2 – État d'équilibre

Le second scénario que l'on peut trouver dans une organisation est ce que l'on appellerait l'état de **vulnérabilité** (Figure 3), où les menaces l'emportent sur les mesures de protection. L'insécurité ainsi produite peut entraîner diverses pertes de TI qui compromettent la confidentialité, l'intégrité et la disponibilité de l'information.

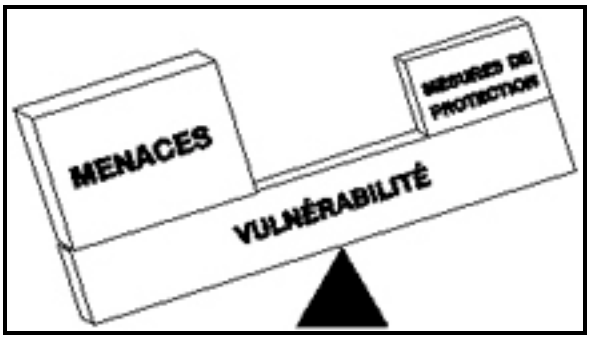

FIGURE 3 – Vulnerable State

Le troisième scénario est celui qu'on appelle l'état de sécurité **excessive** (Figure 4), où les mesures de protection employées sont excessives par rapport aux menaces. On se trouve à engager des dépenses superflues dans des mesures de sécurité qui n'ont aucune commune proportion avec la menace, et qui ne sont donc pas justifiables.

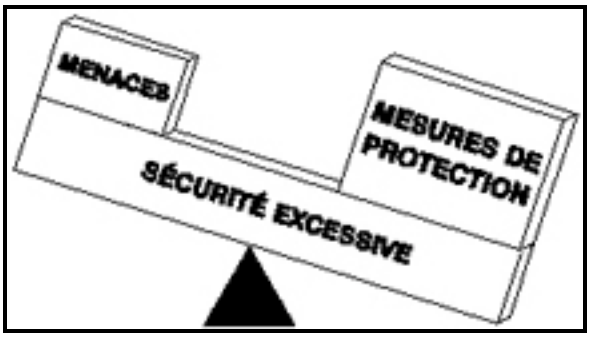

FIGURE 4 – Excessive State

Lorsqu'il est établi que la situation correspond à celle qui est exposée à la Figure 3 - État de vulnérabilité, le praticien doit envisager la possibilité qu'on exploite un ou plusieurs points faibles. Cela dépend d'un certain nombre de facteurs, dont quelques-uns ont été examinés dans l'évaluation de la menace:

- La probabilité qu'une menace se concrétise;
- Les motifs possibles pour exploiter les points faibles;
- La valeur du bien vulnerable pour l'organisation et pour l'agent menaçant; et
- L'effort requis pour exploiter les points faibles.

Par exemple, il peut y avoir des points faibles, mais en raison de l'absence de l'un ou de plusieurs des facteurs ci-dessus, ils ne seront peut-être jamais exploités.

2.3.3. Risques

Le risqué est défini comme « *la probabilité que des points faibles soient exploités* ».

Voici les trios niveaux de risque qui peuvent exister au sein de l'organisation:

élevé — Exige une attention immédiate et la mise en place de mesures de protection dans les plus brefs délais;

moyen — Exige de l'attention et la mise en place de mesures de protection dans un avenir rapproché; ou

faible — Exige une certaine attention et la mise en place éventuelle de mesures de protection en vue d'une sainte gestion des affaires.

Le praticien pourra décider de la priorité à accorder à chaque élément du programme de gestion des risques, en se fondant sur des facteurs tels que la nature des menaces observées et l'incidence de ces menaces sur l'organisation. Après examen des points faibles et des mesures de protection existantes, il déterminera l'opportunité de ces dernières et recommandera des changes. L'Annexe E fournit un exemple d'évaluation des risques en cas de menaces délibérées.

Le Tableau 6 est un exemple de feuille de récapitulation pour l'inscription de renseignements sur l'évaluation des risques pour chaque bien.

2.4. Recommandations

La dernière étape du processus d'ÉMR consiste à faire des recommandations. Les recommandations ont pour buts d'améliorer la situation de l'organisation au plan de la sécurité par la réduction des risques, de proposer des moyens de reprise des affaires advenant qu'une menace cause des dommages et de définir les limites de mise en oeuvre de ces moyens. Une fois que les mesures servant à renforcer celles qui sont déjà en place et à accroître l'ensemble de la sécurité ont été proposées, on peut réévaluer le niveau de risque (élevé, moyen, faible).

BIEN	**MENACE**	**Évaluation des risques**		
		MESURES DE PROTECTION EXISTANTES	**VULNÉRABILITÉS**	**RISQUE**
Décrire le bien	Décrire la menace particulière à laquelle il est exposé	Décrire les mesures de sécurité déjà en place pour protéger le bien contre la menace	Décrire tout point faible observé	Établir le niveau de risque

TABLEAU 6 – Évaluation générale des risques

2.3.4. Résumé de l'évaluation des risques

L'évaluation des risques décrite dans cette partie comporte les étapes suivantes:

a) examiner les measures de protection existantes;

b) relever les points faibles; et

c) determiner le niveau de risqué d'après un certain nombre de facteurs.

2.4.1. Mesures de protection proposées

À ce stade-ci, le praticien a déjà analysé la nature des menaces, leur incidence si jamais elles devaient se concrétiser et la vulnérabilité de l'organisation à ces menaces. Il a ensuite évalué le niveau de risque. Si le praticien pense qu'il y a possibilité de réduire les risques, il fait des recommandations en ce sens. Il peut recommander divers scénarios, qui ont chacun des conséquences et des coûts

particuliers, et parmi lesquels la haute direction fera un choix.

Lorsque l'évaluation des menaces et des risques donne lieu à des recommandations précises, le praticien doit aussi songer à la **faisabilité** de ces recommandations.

2.4.2. Risques prévus

Dans certains cas, les mesures de protection proposées réduiront ou élimineront quelques risques, mais pas tous. Les autres risques devront alors être notés et reconnus par la haute direction. Supposons par exemple que l'évaluation originale des risques révèle un taux de risque élevé et que l'équipe d'ÉMR recommande plusieurs mesures de protection faisant passer ce taux à moyen-bas. Les risques sont réduits mais ils ne sont pas complètement disparus, et la haute direction doit prendre connaissance du niveau de risque prévu et l'accepter ou non. Si les dirigeants se disent insatisfaits du niveau de risque, cela signifie qu'il faudra trouver d'autres mesures de protection pour réduire encore plus ou éliminer les risques.

On peut classer les mesures de protection mises en oeuvre de plusieurs façons, par exemple:

– en se reportant à la colonne de l'évaluation de l'incidence dans l'aide-mémoire pour l'évaluation de la menace (voir le Tableau 5 et l'Annexe C);
– en comparant le niveau de risqué avant qu'une mesure de protection ne soit mise en oeuvre, dans la colonne Risques de l'Évaluation des risques (Tableau 6 et Annexe C), avec ce même niveau évalué plus tard, dans la colonne des Risques prévus à l'étape des Recommandations (Annexe C).

Les risques auxquels on a attribué une cote de 9 devraient être examinés en premier car il s'agit d'événements dont la probabilité est élevée et qui peuvent avoir de très graves conséquences. Dans certains cas, il est souhaitable de ramener le niveau de risque d'élevé à bas, surtout lorsque la cote de mesure de l'exposition est élevée.

2.4.3. Évaluation globale des mesures de protection

Les mesures de protection devraient être évaluées en function des trios catégories suivantes:

– entièrement satisfaisantes;
– satisfaisantes dans l'ensemble;
– ont besoin d'être améliorées.

Les risques de menaces délibérées à l'endroit de l'organisation ont été établis à l'aide de la Grille d'évaluation des risques décrite à l'Annexe E. Dans le cas des menaces **accidentelles**, les risques sont évalués en se fondant sur les précédents survenus dans l'organisation ou dans des institutions semblables et sur l'efficacité observée des mesures de protection mises en place pour contrer ce genre de menaces. La plus grande priorité doit être accordée aux menaces présentant un risque élevé pour l'organisation. Pour chacune de ces menaces, le praticien devra proposer des mesures destinées à éliminer les risques ou à les réduire à un niveau acceptable pour la haute direction. Il évaluera ensuite l'opportunité de ces mesures en jugeant si elles sont **entièrement satisfaisantes, satisfaisantes dans l'ensemble ou si elles ont besoin d'amélioration**.

Le praticien détermine la pertinence et l'interdépendance des mesures de protection et tâche de répondre aux questions suivantes : Les mesures sont-elles incompatibles? Une mesure en rend-elle une autre inutile? La mesure de protection adoptée est-elle disproportionnée par rapport à la menace? Quelles menaces ne sont pas entièrement contrées? Quel est le risque que soient exploitées des faiblesses qui n'ont pas été entièrement corrigées et par qui ces faiblesses pourraient-elles être exploitées?

3. Mises à jour

L'ÉMR est un document essentiel à la réalisation des objectifs de l'organisation en matière de sécurité. Il faut la mettre à jour au moins une fois l'an, et toutes les fois qu'un incident révèle une lacune dans l'évaluation existante. On doit aussi l'actualiser quand des changements sont prévus aux systèmes ou aux milieux d'exploitation de la TI, changements qui pourraient créer de nouveaux risques ou rendre certaines mesures de protection redondantes.

3.1. Révisions régulières

Des révisions régulières permettent au praticien de revoir l'ÉMR et de vérifier si les exigences en matière de sécurité de la TI au sein de l'organisation ont changé. De telles révisions sont nécessaires à la lumière des rapports changeants entre les techniques en place dans le domaine de la TI et les techniques dont disposent les agents menaçants pour s'attaquer aux systèmes de TI de l'organisation.

3.2. Modifications aux systèmes

Les modifications apportées aux systèmes peuvent transformer le profil de sécurité. Il faut donc évaluer au préalable toute modification. L'ÉMR fournit au praticien un point de départ à partir duquel il peut mesurer les effets des modifications. À titre d'exemples de modifications, notons l'abandon des ordinateurs autonomes au profit d'un réseau local, l'introduction de nouvelles applications dans les systèmes existants ou encore d'un réseau longue distance pour les milieux de TI existants, un changement dans les liens ou les protocoles de communication utilisés pour transmettre l'information d'un service à l'autre, ou un changement dans le niveau de sécurité des renseignements les plus délicats dans le système.

3.3. Modifications à la description de la menace

Les modifications à la description de la menace risquent aussi d'avoir une incidence sur l'ÉMR. Par exemple, lorsque la motivation d'un agent menaçant diminue ou que celui-ci doit dépenser plus d'efforts, la menace provenant de cette source peut s'en trouver réduite. Comme les modifications susmentionnées ne suivent pas toujours un cycle donné, le praticien doit se tenir au fait des niveaux de menace courants et mettre à jour l'ÉMR en conséquence.

4. Conseils et orientation

4.1. Menaces

Les sources de renseignements historiques sur les menaces varient, selon le genre de renseignements voulus. Dans le cas des renseignements sur les événements qui se sont déjà produits au sein de l'organisation, le praticien doit consulter l'agent ministériel de la sécurité. Pour ce qui a trait aux renseignements sur les enquêtes menées aux termes du Code criminel du Canada concernant des biens de TI, le praticien doit s'adresser à l'officier responsable de la Sous-direction de la sécurité des technologies de l'information de la GRC. S'il s'agit de renseignements relatifs à la sécurité des communications (COMSEC), il lui faut consulter le Centre de la sécurité des communications. Le Service canadien du renseignement de sécurité (SCRS) fournit au besoin des renseignements sur des menaces ainsi que des conseils relativement à l'évaluation de la menace.

4.2. L'ÉMR

On peut obtenir des avis et des conseils concernant le processus d'ÉMR décrit dans le présent document en s'adressant à l'officier responsible de la Sous-direction de la sécurité des technologies de l'information de la GRC.

GLOSSAIRE

Analyser : Étudier ou déterminer la nature des choses et leurs relations entre elles.

Bien : Tout article ayant une certaine valeur.

Conditions de base en matière de sécurité : Le profil de sécurité établi ou les conditions de sécurité déterminées à un moment donné.

Confidentialité : La sensibilité de l'information ou des biens à une divulgation non autorisée, évaluée à l'aide d'une cote de classification ou d'une désignation correspondant au niveau de dommage produit advenant une divulgation non autorisée.

Conséquences : Répercussions, effets.

Critique : Crucial, déterminant.

Danger : Divulgation sans autorisation, destruction, enlèvement, modification ou interruption.

Disponibilité : L'accessibilité, sur demande, pour exécuter certaines fonctions.

Équilibre: Balance existant entre une ou plusieurs forces opposées.

Évaluation de la menace : Évaluation de la nature, de la probabilité et des conséquences d'actes ou d'événements susceptibles de mettre en péril des biens ou des renseignements de nature délicate.

Évaluation des risques : Évaluation de la probabilité que des points faibles soient exploités, compte tenu de l'efficacité des mesures de protection existantes ou proposées.

Évaluer : Déterminer dans quelle mesure certains facteurs (menaces, points faibles et risques) minent le milieu d'exploitation de la TI. Estimer ou calculer le montant ou la valeur de quelque chose.

Exposition : La vulnérabilité à la critique ou à une attaque.

Incidence : Les effets d'une chose sur une autre.

Intangible : Qui échappe au sens du toucher.

Intégrité : L'exactitude et l'intégralité des renseignements et des biens et l'authenticité des transactions.

Menace : Tout acte ou événement pouvant avoir l'une ou plusieurs des conséquences suivantes : divulgation non autorisée, destruction, enlèvement, modification ou interruption de renseignements, de biens ou de services de nature délicate, ou blessures corporelles. Peut être délibérée ou accidentelle.

Mesures de protection : Moyens pris pour contrer une menace ou solutionner un problème de sécurité particulier.

Praticien : Personne oeuvrant dans un domaine spécialisé.

Probabilité : Caractère de ce qui est probable.

Processus : Série d'actions consécutives visant à obtenir un résultat.

Qualitative: Qui a trait à la qualité, décrivable.

Quantitative: Qui a trait à la quantité, quantifiable.

Tangible : Perceptible au toucher.

Technologie de l'information : Désigne les disciplines scientifiques, technologiques et techniques, de même que les technologies de gestion, qui servent à la manipulation, à la communication et au traitement de l'information; les domaines de l'informatique, des télécommunications, des réseaux et de leur convergence dans les systèmes; les applications, le logiciel et le matériel connexe ainsi que leur interaction avec les personnes et les machines.

ÉNONCÉ DE LA NATURE DÉLICATE

RENSEIGNEMENTS GÉNÉRAUX

Service: _____ Division: _____
Personne ressource: _____ Téléhone: _____

MILIEU:
(Système)
Nom du système: _____
Application: _____
Autre: _____

(Matériel)
Ordinateur central/Mini-ord.: _____
Micro-ordinateur: _____
RL/RLD/RMD: _____
Téléphone protégé/Télécopieur: _____
Autre: _____

CONFIDENTIALITÉ

Les renseignements traités sont-ils considérés:

CLASSIFIÉS ( ) Non ( ) Oui Niveau (si Oui): _____
or
DÉSIGNÉS ( ) Non ( ) Oui Niveau (si Oui): _____
or
Divulgables aux termes de la Loi sur l'accès à l'information?
( ) Non ( ) Oui
Détails: _____

Quelles seraient les conséquences d'une divulgation à des personnes non autorisées?

	Non	Oui
Perte de service	( )	( )
Pertes financières	( )	( )
Perte d'emploi	( )	( )
Problèmes juridiques	( )	( )
Perte de confiance	( )	( )
	( )	( )

Autre: _____

DISPONIBILITÉ

Quel est le degré d'importance des données dans le système?

Public:	( ) Faible	( ) Moyen	( ) Élevé	( ) Très élevé
Ministère:	( ) Faible	( ) Moyen	( ) Élevé	( ) Très élevé
Service:	( ) Faible	( ) Moyen	( ) Élevé	( ) Très élevé

Quelle est la plus grande durée d'indisponibilité (en jours) possible des renseignements dans le système?

( ) 1 ou moins ( ) 1-2 ( ) 3-10 ( ) 11-30 ( ) 30+

Existe-t-il des mesures d'urgence de reprise du service?

Sauvegardes:	( ) Unknown	( ) No	( ) Yes
Conservation hors-siège:	( ) Unknown	( ) No	( ) Yes

Autre moyen de reprise: _____

Indiquer ce qu'il en coûterait approximativement chaque jour si on excédait la durée d'indisponibilité permise:

Coût ($): _____

La destruction du système pourrait-elle causer ce qui suit?

	Non	Oui
Perte de service	( )	( )
Pertes financières	( )	( )
Perte d'emploi	( )	( )
Problèmes juridiques	( )	( )
Perte de confiance	( )	( )

Autre: _____

INTÉGRITÉ

Quelle est l'importance de l'exactitude des renseignements?

( ) Assez importante ( ) Très importante

Y a-t-il des mesures en place pour vérifier l'exactitude des renseignements? ( ) Non ( ) Oui

La corruption des renseignements pourrait-elle causer ceci?:

	Non	Oui
Perte de service	( )	( )
Pertes financières	( )	( )
Perte d'emploi	( )	( )
Problèmes juridiques	( )	( )
Perte de confiance	( )	( )

Autre: _____

Utilise-t-on régulièrement des programmes anti-virus?

( ) Oui ( ) Non Fréquence: _____

Signature: _____ Date: _____

SOMMAIRE DE L'ÉVALUATION DE LA MENACE ET DES RISQUES

BIEN	ÉVALUATION DE LA MENACE						ÉVALUATION DES RISQUES			RECOMMANDATIONS		
	Agent/ Événement	Catégorie de menaces	Probabilité	Conséquence de la menace si elle se concrétise	Incidence	Cote de mesure de l'exposition	Mesures de protection existantes	Vulnéra-bilité	Risque	Mesures de protection proposées	Risque prévu	Évaluation des measures de protection
DÉCRI-RE le bien	DÉCRIRE l'événement ou l'agent menaçant	INDIQUER la catégorie de menaces: ✓ Divulgation ✓ Interruption ✓ Modification ✓ Destruction ✓ Enlèvement	ÉVALUER la probabi-lité de réali-sation: ✓ Faible ✓ Moyenne ✓ Élevé	DÉCRIRE les conséquences possibles, soit: ✓ Perte du caractère confidentiel ✓ Perte de confiance ✓ Perte du bien ✓ Perte de service ✓ etc.	ÉVALUER le préjudice: ✓ Excepti-onnellement grave ✓ Grave ✓ Moins grave	ATTRIBU-ER UNE COTE DE PRIORITÉ, de 1 à 9, à l'aide du tableau de mesure de l'exposition.	DÉCRIRE les mesures de sécurité en place pour contrer la menace.	DÉCRIRE les points faibles observés.	ÉTABLIR le niveau de risque: ✓ Faible ✓ Moyen ✓ Élevé	RECOM-MANDER la mise en place de nouvelles mesures de protection ou la suppression de mesures inutiles.	ÉVALUER le niveau de risqué prévu: ✓ Faible ✓ Moyen ✓ Élevé	ÉVALUER les mesures de protection: ✓ Entièrement satisfaisantes ✓ Satisfaisantes dans l'ensemble ✓ Ont besoin d'amélioration

Aide-mémoire pour l'exécution de l'ÉMR

La présente annexe renferme quatre aides-mémoire dont se sert le praticien pour bien planifier et suivre en suite chacune des étapes de l'ÉMR. Les quatre grandes étapes à planifier sont les suivantes : Préparation, Évaluation de la menace, Évaluation des risques, Recommandations.

1ère ÉTAPE – PRÉPARATION

ACTIVITÉ	DATE DU DÉBUT	DATE DE FIN	PARTICIPANTS R – responsable C – contributeurs		COMMENTAIRES
			R/C	Nombre de jours prévus	
2.1.1 Définir le milieu					
2.1.2 Prendre l'inventaire et évaluer les biens					
2.1.3 Exigences en matière de CID					
2.1.4 Énoncés de la nature délicate					
Étapes supplémentaires au besoin					

2e ÉTAPE – ÉVALUATION DE LA MENACE

ACTIVITÉ	DATE DU DÉBUT	DATE DE FIN	PARTICIPANTS R – responsable C – contributeurs		COMMENTAIRES
			R/C	Nombre de jours prévus	
2.2.1 Déterminer la catégorie de menaces					
2.2.2 Déterminer la probabilité de réalisation de la menace					
2.2.3 Préparer une évaluation de l'incidence					
2.2.4 Résumer l'évaluation de la menace					
Mesures supplémentaires au besoin					

3e ÉTAPE – ÉVALUATION DES RISQUES

ACTIVITÉ	DATE DU DÉBUT	DATE DE FIN	PARTICIPANTS R – responsable C – contributeurs		COMMENTAIRES
			R/C	Nombre de jours prévus	
2.3.1 Noter les mesures de protection existantes					
2.3.2 Reconnaître les points faibles					
2.3.3 Établir les niveaux de risque					
2.3.4 Évaluer l'opportunité des mesures de protection					
2.3.5 Résumer l'évaluation des risques					

4e ÉTAPE – RECOMMANDATIONS

ACTIVITÉ	DATE DU DÉBUT	DATE DE FIN	PARTICIPANTS R – responsable C – contributeurs		COMMENTAIRES
			R/C	Nombre de jours prévus	
2.4.1 Définir les recommandations visant à réduire les risques Établir une liste de priorité pour la mise en œuvre des mesures proposées					
2.4.2 Définir les recommandations pour assurer la poursuite des affaires					
2.4.3 Définir les recommandations pour l'application de la sécurité					
Préparer des documents servant à obtenir l'approbation écrite des gestionnaires supérieurs					
Mesures supplémentaires au besoin					

GRILLE D'ÉVALUATION DES RISQUES EN CAS DE MENACES DÉLIBÉRÉES

Afin de déterminer les niveaux de risque au sein d'une organisation, le praticien doit noter tous les facteurs qui contribuent à ce risque. Une des façons de procéder dans le cas de menaces **délibérées** est d'utiliser une grille d'évaluation des risques (Tableau E-1). La colonne AVANTAGE indique l'avantage que pourrait procurer à l'agent menaçant l'exploitation d'un point faible. La colonne de l'INCIDENCE indique les répercussions qui se feraient sentir dans l'organisation si la menace se concrétisait.

La colonne suivante, celle des EFFORTS DÉPLOYÉS indique les efforts qui sont faits par l'agent menaçant pour porter atteinte à la sécurité. Ces efforts sont évalués en tenant compte de l'efficacité des mesures de protection *existantes*.[5] La probabilité qu'une menace se concrétise diminue à mesure qu'augmentent les efforts que doit déployer l'agent menaçant.

Lorsqu'il est question de menaces **délibérées** à l'endroit des systèmes et des données, la grille d'évaluation des risques peut s'appliquer telle quelle. Cependant, on ne peut parler d'avantage ni d'efforts déployés par l'agent menaçant dans le cas des menaces **accidentelles.** Il faut alors trouver un autre moyen d'évaluer les risques présentés par ce genre de menaces. Comme les événements accidentels sont souvent imprévisibles, le praticien doit faire son évaluation des risques en fonction des tendances observées dans l'organisation et les autres institutions gouvernementales.

[5] Il faut se rappeler qu'au paragraphe 2.2.3 dans l'*Évaluation de l'incidence*, on a examiné le milieu en l'absence de mesures de protection. On examinera les risques compte tenu des mesures de protection **existantes**.

TABLEAU E–1 – GRILLE D'ÉVALUATION DES RISQUES

AVANTAGE (pour l'agent menaçant)	INCIDENCE (sur l'organisation)	EFFORTS DÉPLOYÉS (par l'agent menaçant)	RISQUES (pour l'organisation)
Élevé	Exceptionnellement grave	Faibles	Élevés
		Moyens	Moyens – Élevés
		Élevés	Faibles – Moyens
Moyen	Grave	Faibles	Moyens – Élevés
		Moyens	Moyens
		Élevés	Moyens – Faibles
Faible	Moins grave	Faibles	Faibles
		Moyens	Faibles
		Élevés	Faibles