Guide sur la gestion des risques pour les secteurs des infrastructures essentielles

Sécurité publique Canada
Public Safety Canada

Avant-propos

La gestion du risque est une responsabilité partagée qui incombe à tous les intervenants des infrastructures essentielles, y compris les gouvernements, les partenaires du secteur privé, les premiers intervenants et les organisations non gouvernementales. L'établissement de partenariats et l'échange de renseignements constituent les composantes de base de la démarche canadienne visant à renforcer la résilience des infrastructures essentielles, mais il est impossible d'appliquer ces mesures sans tenir compte de la gestion des risques et de l'élaboration de plans et d'exercices visant à aborder ces risques.

Puisque les perturbations peuvent avoir des répercussions en cascade sur les secteurs et les administrations, le présent document vise à offrir des directives pratiques afin de mettre en œuvre une approche coordonnée et tous risques en matière de gestion des risques liés aux infrastructures essentielles. Cependant, pour aller de l'avant avec ce processus exhaustif ayant trait à la gestion du risque, les ministères et organismes fédéraux doivent collaborer avec leurs partenaires des infrastructures essentielles, y compris les intervenants du secteur privé et d'autres ordres de gouvernement. Bien que le présent document favorise l'adoption d'une approche commune pour gérer les risques liés aux infrastructures essentielles, il incombe en dernier ressort aux propriétaires, aux exploitants et à chaque administration de mettre en place une approche de gestion des risques qui correspond à leur contexte.

Le présent guide est une adaptation de la norme internationale ISO 31000, « Management du risque – Principes et lignes directrices », et comporte les sections suivantes :

1. Aperçu, principes et processus;
2. Réseaux sectoriels : communication et consultation;
3. Aperçus des secteurs : partie 1 – Opérations sectorielles;
4. Aperçus des secteurs : partie 2 – Profil des risques sectoriels;
5. Aperçus des secteurs : partie 3 – Plan de travail sectoriel;
6. Amélioration constante et rétroaction.

Les sections 2 à 6 se concentrent sur la mise en œuvre et contiennent les sous-sections suivantes :

Éléments clés : les intrants et les réalisations attendues;
Mise en œuvre : les méthodes de mise en œuvre recommandées;
Considérations : les questions, enjeux et défis dont il faut tenir compte.

L'amélioration continue constitue un des principes sous-jacents d'une gestion des risques judicieuse. Le présent guide sera donc mis à jour régulièrement en fonction des leçons tirées dans le cadre de l'application du processus. Le guide

le plus récent, les outils et les autres renseignements visant à appuyer l'approche tous risques en matière de gestion des risques liées aux infrastructures essentielles sont mis à jour régulièrement et affichés sur le site Web de Sécurité publique Canada à l'adresse suivante : http://www.securitepublique.gc.ca/prg/em/ci/index-fra.aspx.

Liste des modifications

Voici la liste des modifications apportées au présent Guide :

N°	Date	Modifié par	Commentaires
1.0	2010 07 01	Politique en matière d'infrastructures essentielles, Sécurité publique Canada	Version initiale

1. Aperçu, principes et processus

> *La gestion des risques est une pratique solidement établie au sein des secteurs de l'assurance, du génie, des finances et du risque politique. Il est clair cependant que la gestion des risques manque relativement de maturité dans la façon dont elle est appliquée au domaine de la sécurité intérieure. Certains pourraient faire valoir que la mise en œuvre de l'évaluation et de la gestion des risques dans les domaines de la sécurité intérieure et du contre-terrorisme est sans doute plus complexe que dans ses applications industrielles dont l'objectif primordial est de protéger les gens contre les pertes financières.* [Traduction]
>
> – « The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress », Congressional Research Service, février 2007

1.1 L'importance de gérer les risques collectivement

Les organisations prennent à un certain nombre de mesures en vue d'atténuer les risques à l'égard de leurs activités en combinant :

- la planification stratégique pour fixer des objectifs, déterminer les mesures à prendre, affecter les ressources et évaluer les progrès;
- des évaluations des risques pour cerner et évaluer les risques pour l'organisation;
- la planification de la gestion des urgences afin d'intégrer et de coordonner une méthode permettant de cerner et de minimiser l'incidence des risques qui se rapportent à toutes les opérations d'une institution;
- des méthodes de continuité des opérations pour faire face aux perturbations et assurer la poursuite des services essentiels;
- des mesures de sécurité pour s'attaquer aux menaces;
- une planification d'urgence pour veiller à ce que des mesures d'intervention adéquates soient en place en cas d'urgence.

Malgré ces mesures, d'importantes lacunes persistent. Il se peut que certains risques soient mal gérés du fait que l'on comprenne mal leurs causes ou leurs effets, qu'ils soient nouveaux ou que l'on manque de données sur la façon d'y aborder. D'autres peuvent déborder la sphère d'influence de l'organisation, notamment les vulnérabilités attribuables aux dépendances, les vulnérabilités de la chaîne d'approvisionnement ou des cyberréseaux. Il se peut aussi que les responsabilités pour aborder les risques soient mal comprises, peu claires ou partagées, ce qui conduit à l'inaction. Enfin, il se peut que certains risques soient trop rares pour justifier l'affectation de ressources ou que les conséquences soient trop lourdes pour qu'une organisation s'y attaque seule.

Les réseaux sectoriels, le Forum national intersectoriel, le Groupe de travail fédéral, provincial, territorial sur les infrastructures essentielles et d'autres

mécanismes créés par la Stratégie ont pour but de compléter les activités liées à la gestion des risques à l'échelle organisationnelle et régionale ainsi que d'aborder ces lacunes.

Par leur participation aux réseaux sectoriels, les partenaires des secteurs public et privé peuvent mieux intervenir en cas d'urgence, mieux cerner les vulnérabilités attribuables aux interdépendances, affecter collectivement leurs ressources aux secteurs prioritaires et concevoir des mesures mieux adaptées pour atténuer les risques, ce qui démontre une compréhension plus approfondie des opérations et des besoins pansectoriels.

Les gouvernements et les partenaires des secteurs public et privé travaillent en collaboration pour éclaircir et définir les rôles et les responsabilités, le cas échéant, et pour établir des partenariats de confiance dans un secteur et entre plusieurs secteurs. Les activités collectives de gestion des risques permettront au gouvernement :

- de cerner et aborder les lacunes législatives et stratégiques et d'y remédier;
- de fournir aux propriétaires et aux exploitants des analyses et des renseignements plus exacts, utiles et à jour sur les menaces et les risques;
- de collaborer avec les propriétaires et les exploitants pour faire valoir les avantages d'investir dans des mesures de sécurité et d'accroître la résilience;
- de fournir des outils, des pratiques exemplaires et d'autres conseils pour appuyer les activités liées à la gestion des risques au sein des secteurs des infrastructures essentielles;
- de renforcer l'échange de renseignements à durée de vie critique dans les situations de gestion des menaces et des incidents émergents.

Les activités collectives de gestion des risques présentent des avantages pour tous les intervenants des infrastructures essentielles, notamment :

- cerner les risques stratégiques, systémiques ou nationaux et les aborder;
- en cernant les risques attribuables aux dépendances et les aborder;
- intervenir plus rapidement et efficacement pendant les attaques et les perturbations;
- rétablir rapidement les actifs cruciaux et les services essentiels après une perturbation;
- en faisant appel au savoir-faire et aux ressources des secteurs public et privé pour faire face aux menaces existantes et naissantes;
- renforcer la résilience des infrastructures essentielles du Canada, pour faire du Canada un pays plus sûr.

1.2 Principes

Compte tenu des leçons retenues et des pratiques exemplaires de nos alliés internationaux, des provinces, des territoires et du gouvernement fédéral, les principes suivants s'appliquent au processus de gestion des risques décrits dans les présentes :

Niveau stratégique : ce processus se déroule au niveau sectoriel – c'est-à-dire les risques systémiques, stratégiques ou nationaux. Son but est de compléter les activités de gestion des risques à l'échelle organisationnelle et régionale. En particulier :

- les risques qui ont été cernés comme priorités stratégiques par le réseau sectoriel ou par les gouvernements;
- les risques susceptibles d'avoir des conséquences systémiques, pansectorielles ou multisectorielles, ce qui englobe les risques communs à de nombreux intervenants, les risques qui sont occasionnels mais qui ont des conséquences graves sur le secteur;
- les risques pour l'intérêt national.

Processus organisationnels complémentaires : dans la mesure du possible, le processus et l'approche doivent s'inspirer des mécanismes existants, de même que des menaces, des vulnérabilités et des évaluations des risques menées à l'échelle organisationnelle et sectorielle et les compléter. De même, la planification stratégique, la planification de la continuité des opérations, la planification de la gestion des urgences, la planification des interventions d'urgence et d'autres activités utiles doivent être envisagées et entreprises lorsqu'on se livre à des activités sur les infrastructures essentielles au niveau de l'industrie et du secteur.

Cadre commun : les infrastructures essentielles regroupent de nombreuses disciplines, industries et organisations différentes, qui peuvent toutes avoir des approches et des interprétations différentes des risques et de la gestion des risques, ainsi que des besoins différents. Pour rapprocher ces écarts, on a conçu un cadre commun qui permet la contribution flexible des différentes organisations d'un secteur que l'on peut combiner de manière à cerner, à évaluer et à comparer les risques entre les secteurs, de façon à les regrouper dans un profil national intersectoriel.

Processus itératif et graduel : la façon de décrire les opérations des secteurs ainsi que les interdépendances dans les secteurs et entre ceux-ci, d'évaluer et de mesurer les risques et de prendre des mesures pour les atténuer évoluera avec le temps à mesure que les leçons retenues sont assimilées, que l'environnement des risques évolue et que les secteurs innovent et changent. Ce processus est fondé sur des réalisations et des

objectifs discrets et faisables et il intègre la rétroaction et l'amélioration du processus proprement dit à chaque étape.

Les versions et les produits futurs se concentreront peut-être sur des menaces, des incidences et des vulnérabilités particulières hautement prioritaires; il faut donc examiner de près les opérations des secteurs comme les exigences opérationnelles techniques, les types d'actifs particuliers, les milieux d'exploitation régionaux et d'autres précisions, le cas échéant.

1.3 Processus

Le processus de gestion des risques présenté dans la norme ISO 31000 de l'Organisation internationale de normalisation propose une approche souple et générale de gestion des risques qui peut être adaptée aux besoins des secteurs et des sous-secteurs. Lorsqu'il est mis en œuvre, il permet :

- de gérer les risques de façon proactive plutôt que réactive;
- d'améliorer la détermination des menaces;
- de déterminer les vulnérabilités attribuables aux interdépendances;
- de respecter les normes internationales;
- d'accroître la confiance des intervenants;
- d'établir une base fiable en matière de prise de décisions et de planification;
- d'affecter efficacement les ressources pour s'attaquer aux risques;
- d'améliorer la gestion et la prévention des incidents tout en minimisant les pertes;
- d'améliorer l'apprentissage organisationnel et sectoriel;
- d'accroître la résilience.

Le processus de gestion des risques permettra aux réseaux sectoriels d'amorcer et d'entretenir un dialogue sur les problèmes relatifs aux infrastructures essentielles entre les milieux de la sécurité et du renseignement, les experts dans le domaine des risques, les ministères responsables, les gouvernements, les associations d'infrastructures essentielles et les propriétaires ainsi que les exploitants d'infrastructures essentielles.

Outre le fait de bâtir des relations de confiance, grâce au dialogue et à l'échange de renseignements, le processus devrait avoir comme résultat trois documents distincts mais qui se recoupent :

- Opérations sectorielles : le secteur et ses opérations;
- Profil des risques sectoriels : les risques pour le secteur;
- Plan de travail sectoriel : les activités futures du secteur et son plan pour aborder les risques prioritaires.

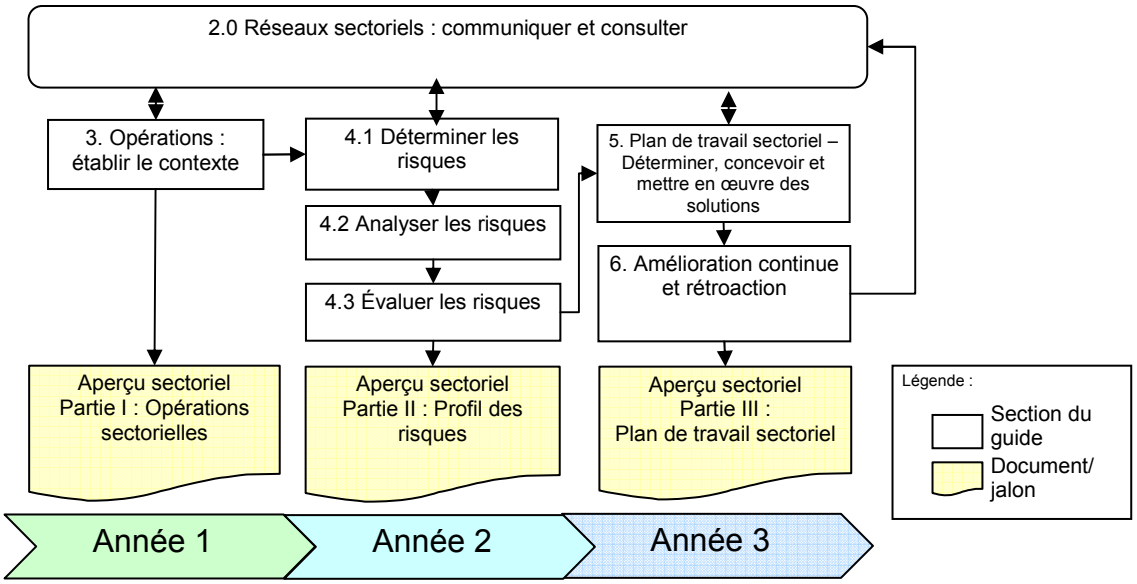
Ces documents peuvent être regroupés dans un aperçu sectoriel. Les renseignements que contiennent ces aperçus sectoriels seront regroupés dans un profil intersectoriel national qui précise les principaux risques encourus par les

infrastructures essentielles du Canada, énonce les interdépendances clés dans les secteurs et entre ceux-ci et fournit une feuille de route pour renforcer la résilience à l'échelle nationale.

La norme ISO liée à la gestion des risques a été adaptée pour *la Stratégie nationale et le Plan d'action* et pour le contexte des réseaux sectoriels. Elle englobe les éléments suivants :

- la communication et des consultations tout au long du processus;
- l'établissement du contexte;
- la détermination, l'analyse et l'évaluation des risques;
- la détermination, l'élaboration et la mise en place de mesures d'atténuation des risques;
- la surveillance, l'examen et l'amélioration constante des mesures d'atténuation des risques, de même que des processus et des pratiques en matière de gestion des risques.

Le schéma ci-après illustre le processus de gestion des risques, les liens entre les principales réalisations attendues (les parties I, II et III des aperçus sectoriels) et les sections de ce document d'orientation.



2. Réseaux sectoriels : communiquer et consulter

> *« L'analyse des risques pour la sécurité intérieure est un problème particulièrement complexe. Ce genre de problème ne se prête guère à des solutions simples, mais exige plutôt des techniques de résolution des conflits multipartites et axées sur la discussion. »* [Traduction]
>
> – Strategic Risk Management in Government : A Look at Homeland Security, Schanzer, Eyerman, de Rugy

La communication et les consultations permettent de nouer des relations de confiance – ce qui est particulièrement important pour gérer les risques auxquels sont exposés les infrastructures essentielles. Il s'agit d'un échange itératif de renseignements et d'opinions dont les objectifs sont :

- de bâtir des relations de confiance;
- de faire prendre conscience commune des risques et du processus de gestion des risques;
- de faire prendre conscience commune des rôles, des responsabilités et des capacités des différents intervenants;
- de veiller à ce que l'on tienne compte des nombreux points de vue;
- d'apprendre les uns des autres.

2.1 Élément clé

L'élément clé de cette mesure est d'établir une équipe de consultation pour communiquer avec les intervenants internes et externes et les consulter ainsi que de veiller à ce que l'on tienne compte de perceptions élargies et diversifiées. Les réseaux sectoriels et leurs membres s'acquittent de ce rôle.

2.2 Mise en œuvre

Les réseaux sectoriels fournissent des tribunes permanentes de discussion et d'échange de renseignements entre les intervenants d'un secteur en particulier et les gouvernements. Ces tribunes reflètent un modèle de partenariat qui permet aux gouvernements et aux secteurs des infrastructures essentielles de se livrer à tout un éventail d'activités (p. ex. évaluations des risques, plans visant à y remédier, exercices) propres à chaque secteur. Ces réseaux sectoriels favorisent également une collaboration plus étroite entre les partenaires des infrastructures essentielles et des activités d'échange de renseignements à la fois dans les réseaux sectoriels interdépendants et entre ceux-ci.

Dans la mesure du possible, les réseaux sectoriels reposent sur des mécanismes existants. C'est pour cette raison que bon nombre des intervenants

ont déjà été identifiés : ce sont les membres du réseau sectoriel et/ou des organisations représentées par les membres du réseau sectoriel.

Un mandat ou toute autre forme d'entente mutuelle concernant les opérations des réseaux sectoriels constitue un point de départ qui permettrait de définir les rouages du réseau, ses objectifs et les ressources dont ils pourraient avoir besoin. Le mandat ou l'entente aiderait également à définir la façon dont le réseau sectoriel communiquera avec le milieu élargi des intervenants des infrastructures essentielles et le consultera.

Les discussions liées aux menaces, aux vulnérabilités, aux opérations, aux capacités et à d'autres renseignements connexes pourraient être sensibles. C'est pourquoi l'une des premières réalisations concrètes du *Plan d'action*, après la création du réseau sectoriel, consiste à élaborer, à adopter et à mettre en œuvre un protocole d'échange et de protection des renseignements qui permettra de discuter ouvertement des risques, des vulnérabilités et d'autres enjeux.

2.3 Considérations

Échange de renseignements
Les intervenants touchés par un risque encouru par un secteur ne sont pas tous forcément membres du réseau sectoriel. Il faut donc tenir compte de la façon de fournir des renseignements utiles à tous les intervenants touchés et des circuits à utiliser pour ce faire. Cela englobe les intervenants et les organisations interdépendants.

De même, il faut tenir compte de la meilleure façon d'échanger des renseignements sur les risques et les enjeux intersectoriels qui ont été cernés et abordés lors du Forum national intersectoriel, de même qu'au sein du Groupe de travail fédéral, provincial, territorial sur les infrastructures essentielles.

Protection des renseignements
La protection des renseignements est une préoccupation majeure du gouvernement et des organisations du secteur privé, qu'il faut savoir concilier avec l'échange des renseignements. D'ailleurs, cet équilibre est nécessaire pour faire progresser la résilience générale des infrastructures essentielles.

Plusieurs enjeux doivent entrer en ligne de compte au moment d'échanger et de protéger des renseignements :

> **Protection des renseignements en vertu de la *Loi sur l'accès à l'information* :** le cadre juridique de la *Loi sur la gestion des urgences* reconnaît qu'il est essentiel de pouvoir échanger des renseignements précis et fiables en temps opportun avec le secteur privé pour permettre au gouvernement de jouer le rôle de chef de file des infrastructures

essentielles à l'échelle nationale. La *Loi sur la gestion des urgences* comporte une modification accessoire à la *Loi sur l'accès à l'information* qui autorise le gouvernement du Canada à protéger les renseignements concernant les infrastructures essentielles qui sont fournis à titre confidentiel au gouvernement par des tierces parties, sous réserve des critères énoncés dans la *Loi*.

Classification des documents : renseignements non classifiés ou de source ouverte permettent la plus libre circulation de l'information. Les renseignements classifiés ou d'autres renseignements sensibles (p. ex. les secrets commerciaux, les renseignements opérationnels, la propriété intellectuelle) sont assujettis à une protection juridique, physique et procédurale. Dans la mesure du possible, les parties doivent envisager de préparer une version non classifiée ou de haut niveau des renseignements sensibles ou classifiés de manière à pouvoir les échanger (sous réserve des protocoles d'échange et de protection des renseignements des réseaux sectoriels).

Contraintes sur les mesures et l'échange de renseignements : les ministères et organismes fédéraux, provinciaux et territoriaux sont assujettis à des lois, des règlements et des procédures auxquels ils doivent se plier, ainsi que leurs représentants. Le secteur privé peut lui aussi être assujetti à des contraintes et à des limites régissant la façon dont il peut fonctionner au sein d'un réseau sectoriel, à cause de questions comme la composition du conseil d'administration, les politiques de l'entreprise, les restrictions imposées aux subventions et les règlements d'ordre juridique. Il se peut que les petites entreprises soient limitées quant à la quantité de ressources qu'elles peuvent contribuer et au temps qu'elles peuvent consacrer au partenariat. Le fait de reconnaître et de comprendre les contraintes et les limites de toutes les parties d'élaborer des stratégies pour régler ces questions permettant au réseau de fonctionner de manière plus efficace.

Recours à des experts en dehors des réseaux sectoriels

Selon la nature des communications, d'autres entités peuvent être invitées à traiter de certains points précis inscrits à l'ordre du jour, notamment :

- des ministères et organismes investis de mandats connexes ou qui se recoupent;
- des spécialistes et des experts;
- des intervenants d'autres secteurs (y compris de secteurs interdépendants);
- des clients;
- des organismes et des ministères de réglementation;
- des organisations et des entités qui peuvent être touchées par les activités et les opérations du secteur;
- des groupes d'intérêts spéciaux;
- des entrepreneurs, des fournisseurs et d'autres intervenants de la chaîne d'approvisionnement du secteur;

- des organismes de services d’urgence;
- des organisations à but non lucratif;
- des organismes et des ministères chargés de la sécurité et du renseignement.

3. Partie I – Opérations sectorielles

« Le risque vient de ne pas connaître ce que vous faites. » [traduction]
– Warren Buffet

Par risque, on désigne l'incertitude qui entoure les incidents futurs et leurs résultats. Il s'agit de la chance qu'un événement survienne et qu'il ait des répercussions sur les objectifs.

Les conséquences potentielles de la perturbation d'un service ou d'un produit critique ne peuvent être évaluées et résolues que si le service ou le produit est connu. Les menaces et les dangers ne peuvent être déterminés qu'en fonction des systèmes et des actifs qu'ils ciblent; et les effets en cascade attribuables aux dépendances ne peuvent être résolus que dans la mesure où ils sont connus. Ainsi, pour évaluer les risques significatifs encourus par un secteur, il est nécessaire de connaître ses objectifs et ses fonctions, de même que ses services et produits, et de comprendre sa chaîne d'approvisionnement et ses opérations.

3.1 Élément clé

La principale réalisation concrète de cette étape du processus de gestion des risques est « l'Aperçu sectoriel, partie I – Opérations sectorielles ». Il s'agit d'un document qui décrit le contexte du secteur, ses services et ses produits critiques ainsi que ses dépendances.

3.2 Mise en œuvre

L'élément le plus important de cette étape consiste à comprendre pourquoi le secteur est essentiel. Les secteurs fonctionnent dans différents contextes, ont des attentes et des exigences différentes ainsi que des cultures différentes. Il n'existe pas d'approche unique qui permette de déterminer ce qu'il y a d'essentiel à propos d'un secteur. Les secteurs peuvent utiliser un certain nombre de méthodes et d'approches[*] pour déterminer ce qui est essentiel. À tout le moins, le document des opérations sectorielles doit comporter :

✓	Une description **des services et des produits critiques** – les extrants des infrastructures essentielles – c'est-à-dire les services et les produits dont la compromission sur le plan de la	*Nota : Les résultats des analyses des répercussions sur les opérations organisationnelles et des évaluations du caractère essentiel permettent de mieux comprendre ce qui est essentiel au*

[*] Voir Outils et renseignements.

	disponibilité ou de l'intégrité se soldera par de graves préjudices à la santé, la sécurité ou le bien-être économique des Canadiens, et au bon fonctionnement du gouvernement.	*niveau d'un secteur.*
✓	Une description des **dépendances** du secteur – les services et les produits du secteur et d'autres secteurs qui sont indispensables pour produire ou fournir les services et les produits critiques du secteur.	*Nota : Une **dépendance** est un service ou un produit nécessaire pour fournir « un service ou un produit critique ».*
✓	Un aperçu de **la chaîne d'approvisionnement du secteur et des opérations de soutien** – soulignant la façon dont les services et les produits critiques sont créés, produits, transmis et distribués. Cela englobe les produits et les services fournis par les partenaires du secteur privé de même que par le secteur public.	*Nota : Le niveau de précision approprié doit être déterminé par le réseau sectoriel ou le ministère responsable.* *Il se peut que certains réseaux sectoriels ne souhaitent décrire que les principaux systèmes et caractéristiques de la chaîne d'approvisionnement, tandis que d'autres pourraient décrire la chaîne d'approvisionnement plus en détail – en mentionnant les sous-systèmes, les réseaux et les types d'actifs nécessaires pour produire et fournir les services et les produits critiques.* *Ces descriptions ne doivent pas contenir de renseignements sur les vulnérabilités particulières, l'emplacement et les caractéristiques d'actifs particuliers ou d'autres renseignements sensibles.*

Ce document peut également :

- souligner la raison pour laquelle le secteur est important pour le Canada et les Canadiens, et pour l'Amérique du Nord – ce qui peut englober sa contribution au PIB, le nombre de personnes employées, la valeur des importations et des exportations et d'autres statistiques importantes;
- fournir un aperçu des principales tendances qui touchent le secteur – comme les tendances d'ordre technologique, social, économique, géographique, environnemental ou politique. On peut également faire état des moteurs opérationnels, des débouchés commerciaux et des risques opérationnels, le cas échéant;
- donner un aperçu des capacités du secteur en cas d'urgence;

- décrire l'organisation du secteur, notamment les rôles et responsabilités de divers ordres de gouvernement, les principaux protagonistes, la législation de contrôle, la réglementation et/ou les conventions internationales;
- souligner toutes les considérations internationales et régionales.

Les ministères responsables pourront également vouloir organiser des ateliers, mener des sondages ou se servir d'autres méthodes de consultation pour déterminer les services, les produits, les systèmes critiques et les dépendances.

3.3 Considérations

La plupart des méthodes de planification de la continuité des opérations tiennent compte des services et des produits critiques ainsi que des interdépendances d'une organisation. Ces renseignements, lorsqu'ils sont regroupés au niveau sectoriel, permettent de mieux comprendre ce qui peut être jugé essentiel au niveau du secteur.

À mesure que le processus de gestion des risques avance, l'opinion de ce qui est essentiel, des dépendances et de la façon dont la chaîne d'approvisionnement fonctionne évoluera. La première version établira un point de référence, par rapport auquel on pourra mesurer les progrès dans le temps.

Pour décider du niveau de précision approprié, il faut comprendre ce qui revêt de l'importance pour le secteur et ce qui lui permettra de mieux de cerner les risques et les mesures d'atténuation. Il se peut que certains secteurs souhaitent avoir une description très détaillée du secteur, d'autres une description simplifiée, ou les deux.

La description des produits et des services critiques, de la chaîne d'approvisionnement et des dépendances d'un secteur fournit un point de référence commun pour analyser les risques. L'objectif **n'est pas** de déterminer la valeur relative d'un actif, d'un système, d'un service ou d'un produit quelconque. Il se peut qu'un système ait une valeur de remplacement élevée, mais qu'il ne soit pas essentiel pour fournir un service ou un produit critique.

La détermination de ce qui est essentiel dépend d'un certain nombre de facteurs, notamment :

- **Tolérance à l'égard du risque :** le caractère essentiel d'un service ou d'un produit peut dépendre de la volonté à accepter que ce service ou produit coure un risque. Cette tolérance à l'égard du risque peut dépendre sur le contexte du service ou du produit en question, de la façon dont le service ou produit peut être perturbé et des attentes de la population et des intervenants. Par exemple, la tolérance à l'égard du risque des perturbations de courte durée dans les télécommunications terrestres lors

d'une tempête peut être différente de la tolérance à l'égard des défaillances de la salubrité des aliments pour bébés.

- **Portée et concentration :** certains systèmes et actifs peuvent être plus essentiels s'ils représentent un pourcentage élevé du service ou du produit critique, une part significative de l'économie d'une région ou s'ils sont seulement situés dans une certaine région.
- **Substituabilité :** il se peut que certains systèmes, actifs, services et produits soient plus essentiels s'il est difficile de les remplacer.
- **Perspective :** le caractère essentiel peut dépendre de l'endroit où vous vous trouvez – ce qu'une organisation produit ou fournit est essentiel pour cette organisation, et peut l'être pour le secteur ou la région où l'organisation mène ses activités, mais moins essentiel au niveau systémique, stratégique et national. Les réseaux sectoriels ne doivent pas oublier que l'objet et la portée se situent au niveau stratégique et non pas au niveau organisationnel ou régional**.**

4. Partie II – Profils des risques sectoriels

Le deuxième module de l'Aperçu sectoriel concerne les risques. Le processus consiste à déterminer les dangers et les menaces – naturels ou anthropiques qui sont les plus susceptibles de toucher le secteur, afin de mesurer leur probabilité relative et leurs conséquences ainsi que de les évaluer. Le module vise à créer un profil des risques sectoriels – une description des risques encourus par le secteur, ainsi que de leur priorité relative.

Une approche tous risques à l'égard de la gestion des risques ne signifie pas que tous les dangers seront évalués et abordés, mais plutôt qu'ils seront pris en compte. Les menaces et les dangers, comme les catastrophes naturelles, les menaces et les accidents qui sont susceptibles de perturber des secteurs au niveau stratégique, systémique ou national doivent être évalués en profondeur. L'annexe B fournit une liste des menaces et des dangers dont il faut tenir compte, même si le secteur peut avoir son mot à dire.

Parmi les éléments suivants qui vont au-delà de la portée actuelle de ce processus de gestion des risques, mentionnons :

- les grands dossiers mondiaux à long terme ou plus vastes comme les changements climatiques ou la concurrence à l'égard de l'énergie;
- les événements quotidiens – comme la criminalité dans la rue – qui peuvent entraîner des épreuves et des dommages sur une longue période, mais qui ne nécessitent pas de mesures d'urgences du gouvernement fédéral ou d'une province, ou qui n'ont pas le potentiel de perturber des services ou des produits critiques;
- les « risques positifs » (comme les perspectives commerciales) ou les risques que présente le fait de ne pas saisir une telle occasion.

Signalons que les risques attribuables à des facteurs extérieurs, comme les perturbations de produits et de services interdépendants, et que les actes délibérés sans intention de nuire comme la fermeture d'une frontière, **font partie** de la portée de ce processus.

Nota : Une méthode d'évaluation des risques a été conçue par Recherche et développement pour la défense Canada à l'intention des réseaux sectoriels. Les ministères responsables peuvent obtenir une copie de cette méthode auprès de la Division des politiques en matière d'infrastructures essentielles, Sécurité publique Canada.

4.1 Détermination des risques

4.1.1 Éléments clés

Cette étape du processus d'évaluation des risques a pour but de cerner les menaces et les dangers susceptibles de perturber les services et les produits critiques cernés par les réseaux sectoriels. Elle fait appel au savoir collectif que le secteur possède de ses risques – d'après le document des opérations sectorielles, les menaces organisationnelles, les vulnérabilités et les évaluations des risques; de toutes les évaluations des menaces et des risques au niveau du secteur; et d'autres renseignements utiles (comme les documents stratégiques, les évaluations de la gravité de la situation). Cette étape vise à :

- dresser une liste (ou un « registre ») des risques qui sont susceptibles de perturber le secteur; et, basé sur cette liste
- de cerner les risques prioritaires qui doivent faire l'objet d'une évaluation plus approfondie.

4.1.2 Mise en œuvre

Le but de cette étape est d'établir une liste claire, concise et exhaustive des risques potentiels (que l'on appelle également parfois un « registre des risques ») fondée sur les événements susceptibles d'empêcher, de détériorer ou de retarder la prestation de biens et de services critiques.

Le registre des risques est généralement sous la forme d'un tableau, d'un tableur ou d'une base de données et peut contenir les renseignements suivants :

- **énoncé ou description du risque :** phrase décrivant le risque;
- **origine du risque :** la menace ou le danger qui est à l'origine du risque;
- **zones touchées :** l'élément du secteur touché;
- **cause du risque :** pourquoi la menace ou le danger constitue un risque pour le secteur;
- **état/intervention du réseau sectoriel :** la priorité relative du risque et les mesures prises par le réseau sectoriel (le cas échéant);
- **contrôles existants :** ce qui est actuellement en place, ou les mesures connues de maîtrise du risque;
- **sources d'information :** d'autres références;
- **renseignements sur l'évaluation du risque :** comme la probabilité et les conséquences établies dans les évaluations des risques réalisées au niveau sectoriel, au niveau organisationnel ou tout autre renseignement sur le risque;
- d'autres renseignements, comme les menaces connexes, la gravité ou les évaluations de la vulnérabilité, le degré d'incertitude des renseignements sur le risque, les régions susceptibles d'être touchées et les tendances –

par exemple si le risque augmente ou diminue – peuvent également être consignés.

Seuls les menaces et les dangers susceptibles d'avoir une incidence sur le secteur doivent être pris en considération. Une liste des menaces et des dangers se trouve à l'**annexe B** du présent document. Cette liste constitue un point de départ – parmi les autres sources d'information permettant d'allonger la liste, mentionnons :

- les évaluations précédentes des risques, des menaces et des vulnérabilités;
- les registres historiques des catastrophes naturelles, des accidents et des attaques;
- les modèles et la théorie scientifiques;
- l'expérience locale ou étrangère;
- l'avis d'experts;
- les entrevues structurées;
- les groupes de discussion;
- les plans stratégiques et d'activités;
- les déclarations de sinistre;
- l'expérience de l'organisation et du secteur.

Il faut tenir compte de la fiabilité et de la disponibilité des renseignements au moment d'établir les scénarios et de déterminer leur importance relative. **S'il y a des lacunes au niveau des renseignements, cela doit être également consigné dans le registre des risques.**

On peut prévoir que le nombre de risques potentiels encourus par un secteur est considérable; il est donc impossible de tous les évaluer. Le réseau sectoriel devra donc déterminer quels risques doivent être évalués plus en profondeur.

Les facteurs déterminants doivent être consignés dans le registre des risques. Un certain nombre de critères doivent être pris en considération, notamment :

- risque élevé (d'après une évaluation préliminaire des probabilités et des conséquences);
- vulnérabilité élevée;
- hausses prévues des conséquences ou de la probabilité;
- éléments essentiels aux intérêts ou au mandat du secteur;
- risques attribuables à des interactions et des dépendances complexes dans les secteurs et entre ceux-ci;
- éléments communs à de nombreux propriétaires et exploitants où l'on estime qu'une compréhension plus approfondie du risque se soldera par de meilleures stratégies d'atténuation;
- menaces et dangers dont on comprend mal la probabilité ou les conséquences;
- stratégies d'atténuation des risques réalisables et rentables.

Signalons que les menaces et les dangers jugés prioritaires pour faire l'objet d'une évaluation plus approfondie dans ce processus ne sont pas forcément les mêmes priorités établies par d'autres évaluations des risques, même s'il s'agit d'évaluations tous risques.

4.1.3 Considérations

Il est important de dresser une liste aussi exhaustive que possible, puisque les menaces et les dangers qui ne sont pas cernées à cette étape ne figureront pas dans d'autres analyses.

Les menaces et les dangers cernés à cette étape peuvent dépasser la portée du processus décrit ici (c.-à-d. les changements climatiques). Ils doivent néanmoins être consignés dans le registre, car il se peut que les méthodes futures d'évaluation des risques tiennent compte de ces menaces, ou que le réseau sectoriel décide de prendre des mesures pour atténuer les risques connexes même s'ils n'ont pas été officiellement évalués.

Un registre des risques est un document évolutif qui assure la continuité de la détermination des menaces et de l'évaluation des risques entre les périodes d'évaluation. Il permet de classer les mesures par ordre de priorité et garantit que la totalité des menaces et des dangers connus sont pris en considération, même s'ils n'ont pas été officiellement évalués.

D'après le registre des risques et le processus d'évaluation, on établit un profil des risques sectoriels. La section 4.3 de ce document analyse en profondeur le profil des risques sectoriels.

4.2 Analyse des risques

L'analyse des risques désigne l'évaluation des conséquences et leur probabilité et d'autres attributs des risques.

L'analyse des risques permet :

- de mieux comprendre les vulnérabilités du secteur;
- de disposer de plus de données sur les conséquences ou la probabilité afin de prendre des décisions judicieuses;
- de mieux comprendre les risques pour orienter les plans d'atténuation;
- de mieux comprendre les lacunes de connaissances;
- de mieux comprendre les risques résiduels (c.-à-d. les risques qui persistent après les efforts d'atténuation);
- de mieux comprendre la tolérance à l'égard de ce risque.

4.2.1 Éléments clés

Les intrants sont les menaces et les dangers potentiels que l'on a jugés hautement prioritaires; les extrants sont une liste des risques classés par ordre de priorité en fonction de la probabilité et des conséquences de l'incident en question.

4.2.2 Mise en œuvre

À tout le moins, l'évaluation des risques doit :

1) évaluer la perturbation des services et des produits critiques fournis par le secteur;
2) évaluer le risque :
    a. déterminer la probabilité de la menace ou du danger;
    b. déterminer les conséquences de la menace ou du danger, en tenant compte de la perturbation des services et des produits critiques.

Il existe quantité de techniques pour réaliser une telle analyse :

- le recours à des groupes d'experts pluridisciplinaires;
- des entrevues structurées avec des experts dans le domaine d'intérêt;
- des questionnaires et des sondages.

Il faut consigner les hypothèses formulées dans l'analyse. Il faut également cerner et consigner les facteurs qui ont une incidence sur les conséquences et la probabilité.

4.2.3 Considérations

Il n'existe pas une seule façon d'évaluer les risques – la méthode et les pratiques exemplaires employées pour évaluer les risques évolueront. Peu importe la technique utilisée pour évaluer les risques, il faut consigner les leçons retenues et les recommandations d'amélioration.

Un événement peut avoir des conséquences multiples et des répercussions sur des objectifs multiples. Les méthodes existantes de maîtrise des risques et leur efficacité doivent entrer en ligne de compte.

Il faut tenir compte des conséquences d'un point de vue d'un système et d'un secteur, et non pas d'une organisation ou d'un actif précis, à moins que les conséquences sur une organisation ou un actif aient une importance nationale, systémique et sectorielle.

Le fait de reconnaître les intérêts variables des parties qui évaluent le risque au niveau sectoriel et d'en tenir compte fournit un terrain d'entente permet d'établir des partenariats de confiance. Il faut tenir compte des différents intérêts. Par exemple, les organismes du secteur privé se soucieront des coûts se rattachant aux risques comme un manque à gagner, l'atteinte à leur réputation et d'autres préoccupations, alors que les organismes du secteur public se concentreront plutôt sur les questions de sécurité publique.

Conseil : Les évaluations des risques sont plus uniformes entre les secteurs et on possède une meilleure compréhension intersectorielle si des collègues d'autres secteurs (en particulier des secteurs interdépendants) font partie du processus d'évaluation des risques.

4.3 Évaluation des risques

L'évaluation des risques doit donner lieu à des discussions sur :

- le niveau de tolérance ou d'acceptation des risques;
- les priorités en matière de prévention et d'atténuation des risques;
- les priorités liées à d'autres mesures.

4.3.1 Éléments clés

Les risques évalués constituent les intrants de cette étape sont; ces risques doivent être mesurés pour établir un profil des risques sectoriels comportant les éléments suivants :

- le classement des risques par ordre de priorité;
- les données manquantes;
- les leçons retenues.

La partie II de l'Aperçu sectoriel : Profil des risques sectoriels doit être une version non classifiée du profil des risques sectoriels, si le profil ou une partie de ce profil est classifié.

4.3.2 Mise en œuvre

Les risques peuvent être évalués en les divisant en trois catégories :

- les risques qui sont intolérables et pour lesquels des mesures de réduction, de prévention ou d'atténuation sont indispensables;
- les risques au sujet desquels les avantages et les coûts des activités de prévention et d'atténuation doivent être pris en compte par rapport aux conséquences néfastes;

- les risques sont négligeables – les conséquences sont très faibles, la probabilité est mince ou le risque est accepté ou toléré. Aucune mesure de réduction des risques n'est recommandée.

Les critères d'évaluation doivent reposer sur :
- les conséquences;
- les probabilités;
- la façon et la mesure dans laquelle les services et les produits critiques du secteur risquent d'être perturbés;
- l'incertitude liée aux conséquences ou aux probabilités d'incidents.

Le registre des risques doit être actualisé à mesure qu'ils sont évalués au moyen de certaines des données suivantes provenant de l'évaluation des risques, notamment :
- les connaissances sur la menace ou le danger et ses causes;
- une description du ou des scénarios utilisés lors de l'évaluation, notamment les hypothèses formulées;
- les résultats de l'évaluation;
- les recommandations sur la nécessité de revoir l'évaluation des risques.

4.3.3 Considérations

À mesure qu'évolue la compréhension des risques, il peut valoir la peine de revoir et d'actualiser le registre des risques.

Parmi les autres points à examiner dans l'évaluation des risques, mentionnons :
- l'origine de chaque menace ou danger;
- quand, où, comment et pourquoi la menace ou le danger pourrait se matérialiser;
- les rôles, les responsabilités et les mandats;
- les personnes touchées;
- les personnes susceptibles de participer aux mesures de réduction des risques;
- les mesures de contrôle qui existent actuellement pour faire face à ce risque;
- la possibilité que certaines mesures contribuent à atténuer des risques multiples;
- les effets cumulatifs d'événements multiples.

5. Partie III – Plan de travail sectoriel

> *« Le meilleur temps pour réparer sa toiture, c'est lorsque le soleil brille. »*
> [Traduction]
> – John F. Kennedy

À partir de la troisième année du plan d'action, les réseaux sectoriels doivent avoir établi des plans de travail propres au secteur afin de réduire les risques et d'entreprendre d'autres activités liées aux infrastructures essentielles. On prévoit que les plans de travail continueront d'évoluer parallèlement aux infrastructures essentielles, aux menaces qui planent contre elles et aux stratégies visant à les protéger contre ces menaces.

Les plans de travail doivent être :

- **détaillés :** ils doivent porter sur les éléments physiques, cybernétiques et humains des infrastructures essentielles. Les plans de travail doivent porter sur tous les risques ainsi que cerner et aborder les interdépendances au sein des secteurs et entre ceux-ci;
- **intégrés :** les plans de travail sectoriels doivent être complémentaires à l'échelle des gouvernements fédéral, provinciaux et territoriaux;
- **axés sur les risques :** les plans de travail doivent reposer sur une compréhension des risques et être conçus pour permettre de mesurer, d'évaluer et de rendre compte de l'efficacité des efforts d'atténuation. Les propriétaires, les exploitants et les gouvernements peuvent donc réévaluer les niveaux de risque une fois le plan mis en œuvre.

5.1 Éléments clés

Cette étape du processus consiste à trouver des options permettant s'attaquer aux risques, de les évaluer d'établir un plan pour la mise en œuvre et la surveillance des options retenues.

La principale réalisation concrète est un plan de travail sectoriel qui fait état des activités du réseau sectoriel en vue d'atténuer les risques et qui comporte :

1) des buts et objectifs;
2) des mesures d'atténuation – les mesures particulières qui permettront d'atteindre les buts et les objectifs et d'atténuer les risques qu'elles ciblent;
3) un plan de mise en œuvre qui comprend un plan de surveillance et de suivi des résultats;
4) un plan d'exercices pour mettre à l'essai et valider les mesures prises.

5.2 Mise en œuvre

Le processus qui sert à dresser un plan fructueux d'atténuation des risques est tout aussi important que le plan proprement dit. Les étapes ci-après constituent une démarche générique d'élaboration du plan d'atténuation des risques – il se peut qu'il faille modifier l'ordre des étapes ou des tâches afin de répondre aux besoins du secteur.

5.2.1 Établir des buts et des objectifs d'atténuation

L'établissement de buts et d'objectifs clairs contribue à clarifier les solutions aux problèmes et aux enjeux au fur et à mesure qu'ils surviennent. Des buts et des objectifs explicites offrent le cadre nécessaire sur lequel fonder les décisions relatives aux mesures d'atténuation.

Les buts sont des déclarations prospectives générales qui décrivent succinctement le but du processus d'atténuation des risques et ce que le réseau sectoriel cherche à obtenir. Ils ne doivent pas préciser des mesures d'atténuation précises (celles-ci seront conçues ultérieurement), mais plutôt mentionner les améliorations générales souhaitables.

Les objectifs définissent les stratégies ou les mesures de mise en œuvre permettant d'atteindre les buts cernés. Contrairement aux buts, les objectifs sont particuliers et mesurables. Ils développent les buts et fournissent d'autres précisions sur la façon de les atteindre. Il est important d'avoir des objectifs mesurables car ils constituent une feuille de route qui favorise la mise en œuvre fructueuse de la stratégie.

La formulation des buts et des objectifs d'atténuation des risques doit reposer sur l'examen et l'analyse de l'évaluation des risques.

5.2.2 Élaborer un plan de mise en œuvre

Une fois les buts et les objectifs cernés, il faut alors reconnaître, évaluer et classer par ordre de priorité les mesures permettant d'atteindre les objectifs.

5.2.2.1 Élaborer un plan de mise en œuvre : étape 1 – Déterminer les options

Le point de départ de la détermination des options réside souvent dans un examen des mesures, des pratiques exemplaires et des leçons retenues en vigueur à l'échelle nationale et internationale pour atténuer ce type de risque.

Les options d'atténuation des risques peuvent chercher :

- à éviter le risque en arrêtant les activités qui lui donnent naissance ou en ne les commençant pas;
- à réduire la probabilité de la menace ou du danger;
- à réduire les conséquences de la menace ou du danger;
- à modifier les conséquences de la menace ou du danger;
- à partager le risque (par une assurance, des coentreprises, des partenariats);
- à conserver le risque.

L'analyse des risques doit permettre de bien comprendre les causes sous-jacentes, les sources, la chaîne des événements qui donne lieu aux incidents, les conséquences et d'autres éléments, notamment :

- les facteurs de causalité qui peuvent aider à déterminer les types de mesures à prendre pour prévenir les préjudices futurs;
- les causes immédiates et tous les facteurs sous-jacents, la chaîne probable des événements donnant lieu à l'incident, les conséquences potentielles et les conséquences réelles probables;
- la gamme des conséquences potentielles et les conséquences les plus probables;
- la gamme des probabilités et le niveau de confiance dans ces estimations.

La planification de la continuité des opérations, la gestion des conséquences, la gestion des urgences, l'atténuation des catastrophes, l'évaluation des vulnérabilités, l'assurance et d'autres disciplines connexes procurent une foule de mesures possibles. Ces disciplines sont bien établies et ne seront donc pas traitées dans le présent document.

Les scientifiques et les spécialistes des risques (p. ex. géologues, sismologues, hydrologues, etc.), de même que les gestionnaires des plaines inondables, les gestionnaires des urgences, les chefs des services des incendies, les ingénieurs des travaux publics, les ingénieurs des transports et les ingénieurs civils qui sont spécialistes de l'application des principes d'atténuation et de gestion des urgences, possèdent tous une expérience précieuse de ce qu'il faut pour atténuer les risques.

Certaines mesures de rechange potentielles peuvent nécessiter une étude plus approfondie avant de trouver une solution ou une mesure d'atténuation de remplacement.

5.2.2.2 Élaborer un plan de mise en œuvre : étape 2 – Reconnaître et analyser les capacités d'atténuation à l'échelle fédérale, provinciale, territoriale et locale

Le fait de comprendre les capacités qui existent pour atténuer les risques contribuera à déterminer les mesures qui sont les plus susceptibles d'obtenir des résultats fructueux. Cette analyse peut énumérer les organismes des

administrations locales, les ministères et les bureaux responsables de la planification, du respect des codes du bâtiment, de la cartographie, des édifices et de la gestion des actifs matériels ainsi que des fonctions de gestion des urgences. Les organisations à but non lucratif (comme la Société canadienne de la Croix-Rouge) et à but lucratif (comme les entreprises privées de sécurité) peuvent également posséder un potentiel applicable, de même que d'autres ministères ou organismes qui ne semblent pas avoir un effet direct sur les mesures d'atténuation mais qui peuvent avoir un effet indirect sur le programme d'atténuation dans son ensemble.

5.2.2.3 Élaborer un plan de mise en œuvre : étape 3 – Évaluer les mesures d'atténuation et les classer par ordre de priorité

L'évaluation doit établir si la mesure donnera des résultats au sujet des buts et des objectifs d'atténuation particuliers fixés par le réseau sectoriel.

Une fois les options d'atténuation des risques conçues, il faut les évaluer et les classer par ordre de priorité. Voici quelques points possibles à examiner :

- la facilité de mise en œuvre et la rentabilité;
- la possibilité que la mesure entraîne de nouveaux risques ou des conséquences imprévues;
- les impacts sur l'environnement (positifs et négatifs);
- les mesures visant des objectifs multiples;
- les résultats à long terme ou à court terme;
- l'efficacité;
- les retombées directes et indirectes;
- les obligations juridiques, réglementaires, sociales et morales;
- l'efficience;
- l'équité et l'acceptabilité;
- la chronologie et la durée.

5.2.2.4 Élaborer un plan de mise en œuvre : étape 4 – Rédiger le plan

Une fois les mesures déterminées, il faut élaborer un plan de mise en œuvre et s'entendre à son sujet. Le plan doit faire état des dates cibles, des responsabilités et des principaux jalons.

Au nombre des éventuels partenaires de l'élaboration et de la mise en œuvre du plan de travail, il peut y avoir les autorités locales, provinciales, territoriales et fédérales, des organisations du secteur privé et des entreprises, des établissements universitaires, des secteurs interdépendants et des organisations en amont et en aval.

Les réseaux sectoriaux doivent incorporer les principes de la gestion axée sur les résultats dans le plan de mise en œuvre, ce qui peut englober un modèle logique, des indicateurs de rendement et les résultats escomptés.

Il faut également établir la façon dont on surveillera le plan de mise en œuvre. Parmi les principaux paramètres de la surveillance de la mise en œuvre, mentionnons :

- la confirmation et l'éclaircissement des rôles et des responsabilités;
- l'intégration des mesures d'atténuation dans les opérations;
- la détermination des mécanismes et de la fréquence de surveillance de la mise en œuvre et des progrès enregistrés;
- l'établissement d'indicateurs d'efficacité ou de réussite;
- la description et l'échange des réussites (et des échecs) et leçons retenues.

Le plan de travail sectoriel doit également tenir compte de l'évolution des risques, du milieu opérationnel du secteur et d'autres facteurs. Le plan de travail doit également faire le suivi :

- des risques élevés;
- de l'expérience d'autres pays, secteurs et organisations à l'égard des stratégies d'atténuation des risques, notamment de leurs échecs possibles et des progrès des stratégies les plus prometteuses;
- l'évolution de la tolérance à l'égard des risques;
- les progrès technologiques susceptibles de modifier le contexte.

Pour bénéficier d'un soutien tout au long du processus de mise en œuvre, les intervenants doivent être tenus au courant des progrès graduels et du succès du programme. Les constatations des rapports d'étape et les principales activités peuvent être diffusées ou affichées sur le Portail des infrastructures essentielles de securité publique afin de tenir les intervenants au courant des réalisations et des éventuels revers.

S'il y a lieu, il peut être utile d'intégrer la surveillance de la mise en œuvre dans les processus qui existent déjà, comme les cycles budgétaires et d'autres cycles d'établissement de rapports.

5.3 Élaborer un plan d'exercices

Les exercices sont l'un des principaux mécanismes qui permettent de valider et de mettre à l'essai les mesures, les plans et les systèmes d'atténuation des risques. Les exercices permettent :

- d'encourager l'établissement de rapports entre et à travers les industries et les disciplines;
- d'éclaircir les rôles et les responsabilités de même que les capacités;
- de cerner et aborder les dépendances et les interdépendances des infrastructures essentielles et d'en tenir compte;
- de sensibiliser les gens aux risques encourus par les infrastructures essentielles;

- de donner aux membres du personnel la chance d'exercer les rôles qui leur sont confiés;
- de déterminer l'état de préparation pour un incident particulier;
- de cerner les lacunes des protocoles de communication, des procédures d'exploitation et des procédures d'intervention d'urgence.

Les réseaux sectoriels doivent établir un plan et un échéancier pour d'entreprendre des exercices afin de mettre à l'essai et valider les mesures d'atténuation des risques prises.

Conseil : Le fait d'intégrer les secteurs interdépendants et les organisations, ainsi que les responsables des interventions et de la gestion des urgences comme partenaires de la conception des exercices et comme protagonistes de l'exercice accroît la résilience.

Les exercices peuvent varier de simples exercices sur table à des simulations entièrement opérationnelles.

Exercice sur table	Méthode de mise à l'essai de plans où les participants examinent et analysent les mesures qu'ils prendraient dans le cadre d'un scénario particulier, présenté par un animateur. Les mesures particulières ne sont pas exécutées.
Exercice fonctionnel	Méthode de mise à l'essai de plans où les participants accomplissent une partie ou la totalité des mesures qu'ils prendraient en cas d'activation du plan afin d'intervenir dans le cadre d'un scénario particulier.
Exercice entièrement opérationnel	Méthode de mise à l'essai de plans où les participants suspendent leurs opérations normales et activent le plan comme si l'événement était réel.

Les résultats d'un exercice doivent permettre de cerner les lacunes et les limites des mesures actuelles.

Les ministères et organismes chargés d'appuyer les réseaux sectoriels doivent, dans la mesure du possible, adapter les leçons retenues à l'intention générale de tout le secteur et distribuer les leçons génériques retenues à tous les intervenants du secteur.

Les exercices doivent être planifiés et se dérouler en tenant compte de ce qui suit :

- le scénario doit refléter la réalité dans la mesure du possible;
- le scénario doit reposer sur l'évaluation des risques;
- les principaux intervenants doivent y participer et les rôles et les responsabilités doivent être clairement établis;

- les ressources peuvent être déployées ou simulées;
- les centres d'opérations d'urgence peuvent être activés;
- les équipements et les procédures figurant dans le plan d'urgence peuvent être utilisés;
- on peut tenir compte des liens avec d'autres organisations;
- il faut prévoir des séances de compte rendu à la fin de l'exercice;
- les leçons retenues doivent être consignées.

5.4 Considérations

Les décisions relatives aux risques rares mais sérieux nécessitent un examen attentif étant donné que les responsabilités juridiques, morales et sociales peuvent primer sur les paramètres économiques. Les risques peu probables mais aux conséquences graves ont moins de chances d'être « détectées par le radar » que les risques très probables et aux conséquences peu graves. Il se peut fort bien que les risques peu probables mais aux conséquences graves soient plus importants car les secteurs ont moins de chances de résister à ces types d'incidents.

Les lacunes relatives à l'information, aux ressources ou aux capacités doivent être signalées et figurer dans le plan de travail sectoriel.

Les impératifs de calendrier, comme les conditions climatiques saisonnières, les cycles de financement, les plans de travail des organismes et les budgets, doivent entrer en ligne de compte dans la détermination des ressources nécessaires.

Le fait de ne pas intégrer comme il se doit les leçons retenues d'un exercice dans les opérations est malheureusement trop courant dans les activités de gestion des urgences et des infrastructures essentielles. Les leçons retenues doivent être consignées et utilisées afin d'améliorer et de réviser les opérations, les mesures d'atténuation des risques et d'autres plans, et la haute direction d'une organisation doit suivre cette mise en œuvre.

6. Amélioration continue et rétroaction

Les risques ne sont pas statiques – la mise en œuvre du plan d'atténuation des risques et l'expérience après avoir résolu des incidents permettent de réduire les risques. En revanche, de nouvelles menaces font leur apparition, de nouveaux produits et services et de nouveaux venus dans les secteurs modifient le contexte et les opérations, l'innovation favorise de nouvelles technologies – autant d'éléments qui introduisent de nouveaux risques et de nouvelles vulnérabilités. Les réseaux sectoriels sont une tribune durable où l'on peut surveiller ce contexte évolutif des risques et y réagir.

6.1 Éléments clés

L'amélioration continue et la rétroaction doivent être incorporées dans chaque élément du processus de gestion des risques.

Les réseaux sectoriels doivent constamment prendre en compte et échanger les leçons retenues et les pratiques exemplaires afin d'améliorer la résilience des secteurs, les opérations du réseau sectoriel, d'autres réseaux sectoriels, les mesures prises par les gouvernements à tous les échelons, les procédés, les méthodes et les outils utilisés pour gérer les risques durant les opérations normales et à l'issue d'un incident.

6.2 Mise en œuvre

Les leçons retenues doivent être prises en compte durant les opérations sectorielles, après un incident et durant et après un exercice.

L'analyse après l'incident en particulier permet de mieux comprendre la façon d'améliorer le processus de gestion des risques. Cette analyse peut comporter :

- une comparaison entre l'événement actuel et l'évaluation des risques : le processus de détermination des risques a-t-il permis de discerner les risques de l'incident? Le risque a-t-il été bien évalué? Y a-t-il des données complémentaires? Y a-t-il de nouvelles données sur les vulnérabilités, les causes profondes ou d'autres éléments de la menace ou du danger?
- une évaluation des mesures d'atténuation des risques qui ont été prises : quels résultats ont-elles donnés? Les plans d'urgence et les plans de continuité des opérations ont-ils été suffisants? Ont-ils été bien exécutés? Les mesures d'atténuation ont-elles eu des conséquences?
- une revue de la liste des mesures d'atténuation à la lumière de l'incident survenu récemment : si de nouvelles infrastructures doivent être construites – doivent-elles comporter des caractéristiques pour en renforcer la résilience? Doivent-elles être construites dans un nouvel

emplacement ou selon un plan différent? Faut-il modifier l'ordre de priorité des mesures d'atténuation?
- une évaluation des lacunes de l'intervention et la détermination des améliorations à apporter aux plans d'intervention d'urgence, aux plans de continuité des opérations, à la formation, etc.;
- une évaluation des nouveaux équipements nécessaires ou les modifications des installations.

6.3 Considérations

Les réseaux sectoriels doivent bien décrire les mesures ce qui ont donné des résultats concluants et insatisfaisants durant tout le processus de gestion des risques et communiquer ces données aux intervenants du secteur de même qu'aux les ministères responsables, d'autres réseaux sectoriels, le Forum national intersectoriel et Sécurité publique Canada, conformément au protocole d'échange et de protection des renseignements.

Annexe A : Termes et glossaire

Signalons que ces termes ne visent pas à définir la façon dont les divers éléments interagissent ou sont évalués, pas plus qu'ils ne représentent une norme du gouvernement du Canada. En revanche, ce sont des définitions courantes choisies en fonction de leur clarté afin d'employer un langage commun dans diverses disciplines.

Il faut admettre que ces termes peuvent être utilisés de différentes façons selon les secteurs et les disciplines. On prévoit que ce glossaire évoluera en fonction du milieu des intervenants des infrastructures essentielles.

Ce glossaire a été établi de concert avec Sécurité publique Canada, le Centre intégré d'évaluation des menaces, la Gendarmerie royale du Canada, le Service canadien du renseignement de sécurité et Recherche et développement pour la défense Canada.

Tous risques : la Stratégie établit une approche tous risques en matière de gestion des risques – en vertu de laquelle on tient compte de tout l'éventail des sources et des causes des incidents dangereux ou potentiellement dommageables. L'approche tous risques intègre les menaces naturelles et anthropiques, y compris les événements courants de gestion des urgences comme les inondations et les accidents industriels, ainsi que les événements liés à la sécurité nationale comme les actes de terrorisme et les cyberévénements. *(Source : Adapté du Plan fédéral d'intervention d'urgence (2009). Sécurité publique Canada.)*

Actif : personne, capacité personnelle, installation, matériel, information ou activité qui contribue à la réalisation d'un objectif.[Traduction} *(Source : Adapté du Lexique des risques du DHS.)*

Conséquences : résultats ou répercussions d'un incident. [Traduction] *(Source : Oxford English Dictionary.)*

> *Nota : Le type d'incident, son ampleur et les vulnérabilités, la valeur et les fonctions des actifs touchés déterminent les conséquences.*

Infrastructure essentielle : l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement. *(Source : Stratégie nationale et Plan d'action sur les infrastructures essentielles.)*

Services et produits critiques : extrants des infrastructures essentielles – services ou produits dont Service dont la compromission, du point de vue de la

disponibilité ou de l'intégrité, porterait un grave préjudice à la santé, à la sûreté, à la sécurité ou au bien-être économique des Canadiens, ou encore au fonctionnement efficace du gouvernement du Canada. *(Source : Politique sur la sécurité du gouvernement.)*

Dépendance : utilisation monodirectionnelle d'un actif, d'un système, d'un réseau ou d'un ensemble de ces éléments, dans plusieurs secteurs et entre ceux-ci, concernant l'intrant, l'interaction ou d'autres impératifs provenant d'autres sources pour bien fonctionner[1]. *(Source : nouvelle.)*

Incident : événement, causé par une action anthropique ou un phénomène naturel, qui peut causer un préjudice et nécessiter une intervention. [Traduction} *(Source : Lexique des risques du DHS.)*

Interdépendance : dépendances mutuelles, partagées ou réciproques. *(Source : nouvelle.)*

Probabilité : probabilité qu'un incident survienne. *(Source : nouvelle.)*

Risque : le risque se rapporte à l'incertitude qui entoure des événements et des résultats futurs. Il est l'expression de la probabilité et de l'incidence d'un événement susceptible d'influencer l'atteinte des objectifs de l'organisation. *(Source : Cadre de gestion intégrée des risques du SCT.)*

Gestion du risque : Une approche systématique servant à déterminer la meilleure voie à prendre en cas d'incertitude en identifiant, en évaluant, en comprenant, en communiquant les questions liées aux risques et en prenant des mesures à leur égard. *(Source : Cadre de gestion intégrée des risques du SCT.)*

Système : ensemble d'actifs, de ressources ou d'éléments qui fonctionnent ensemble comme un mécanisme ou un réseau d'interconnexion. [Traduction] *(Source : Adapté du dictionnaire Oxford.)*

Menace : situation dans laquelle il y a présence d'un danger et d'une exposition à celui-ci. Les menaces peuvent être d'origine naturelle ou anthropique, et être

[1] Les dépendances peuvent être :

- d'ordre physique : dépendance à l'égard des produits, services et ressources pour assurer un fonctionnement ininterrompu;
- informationnelles : dépendance à l'égard de l'information pour assurer un fonctionnement ininterrompu;
- d'ordre géographique : dépendance attribuable à la proximité géographique des infrastructures;
- d'ordre logique : dépendance attribuable à des facteurs économiques, politiques ou de gestion (c.-à-d. les effets des marchés et des prix des facteurs de production, le commandement et le contrôle des grandes organisations, les effets de la frontière sur le flux des marchandises et des personnes et d'autres).

accidentelles ou intentionnelles. *(Source : Plan fédéral d'intervention d'urgence (2009). Sécurité publique Canada.)*

> *Nota : La menace peut être évaluée pour déterminer la probabilité d'actes hostiles ou nuisibles. Pour ce faire, il peut falloir évaluer les intentions du protagoniste et sa capacité de prendre de telles mesures. L'évaluation peut également tenir compte de cibles particulières (comme des personnes ou des actifs particuliers), de cibles génériques (comme des secteurs, des catégories de cibles ou des régions), des modes d'attaque, des vulnérabilités, et contenir des recommandations sur la façon d'atténuer ou d'éliminer la menace.*

Vulnérabilité : caractéristique ou attribut d'un actif qui le rend vulnérable aux effets d'un incident. La vulnérabilité désigne à la fois la probabilité et les conséquences d'un incident. *(Source : Définition consensuelle du SARMA.)*

Annexe B : Liste des dangers et des menaces

Nota : Il n'existe pas de liste exhaustive des menaces et des dangers. On trouvera ci-après une liste des menaces et des dangers courants qui peuvent compromettre les infrastructures essentielles. On prévoit que cette liste évoluera.

Catastrophes naturelles	

Météorologiques :
- Tempête de vent, cyclone tropical, ouragan, tornade
- Orage
- Tempête de neige, de verglas, de grêle
- Inondation
- Onde de tempête
- Temps extrême
  - Vague de chaleur
  - Vague de froid
  - Sécheresse
  - Glacier, iceberg
	Géophysiques :
	- Séisme
	- Tsunami
	- Éruption volcanique
	- Glissement de terrain, coulée de boue, affaissement du sol
	- Tempête géomagnétique
	Incendie :
	- De forêt, de friche
	- Urbain
	- Incendie suivant un séisme
	Biologiques :
	- Maladies qui touchent l'être humain
	- Maladies qui touchent les animaux
	- Maladies qui touchent les végétaux
	- Infestation ou dégât causé par des animaux ou des insectes

Menaces intentionnelles/délibérées	

Attaques :
- Attaque chimique
- Attaque biologique
- Attaque radiologique
- Attaque nucléaire
- Attaque aux explosifs
- Cyberattaque
- Attaque aux armes conventionnelles
Attaque ennemie et guerre
Impulsion électromagnétique
	- Acte de sabotage
	- Espionnage (industriel et autre)
	- Crime (p. ex. vol, enlèvement, incendie criminel, extorsion)
	- Agitation sociale (émeute, manifestation licite/illicite, perturbation)
	- Grève ou conflit de travail
	- Autre :
	  ○ Fermeture d'une frontière
	  ○ Réforme de la réglementation

Risques accidentels/techniques	

Accident
- Accident des transports
- Déversement ou fuite de matières dangereuses (p. ex. d'explosifs, de liquide inflammable, de gaz inflammable, de matière solide inflammable, de comburant, de poison, biologique, radiologique et/ou corrosif)
- Incendie
  o Incendie urbain
  o Incendie industriel
  o Incendie chimique
- Explosion accidentelle
 	
Défaillance/technique
- Défaillance technique
- Défaillance mécanique
- Défaillance logicielle
- Erreur de l'exploitant
- Défaillance de processus/procédure
- Défaillance de structure (p. ex. effondrement d'un pont, effondrement d'une mine, effondrement/défaillance d'un barrage, défaillance d'une canalisation d'eau)
	- Perturbation/défaillance d'une IE dépendante (p. ex. perturbation de la prestation de services ou de produits critiques dans les secteurs de la technologie de l'information et des communications, des finances, de l'énergie, de l'alimentation, de la sécurité, du gouvernement, des soins de santé, de la fabrication, des transports ou de l'eau)