



Gouvernement
du Canada

Government
of Canada

LIGNE DIRECTRICE CANADIENNE SUR LA BIOSÉCURITÉ

EFFECTUER UNE ÉVALUATION DES RISQUES DE BIOSÛRETÉ



Risques

Canada

La *Ligne directrice canadienne sur la biosécurité – Effectuer une évaluation des risques de biosûreté* est disponible sur Internet à l'adresse suivante : <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/directrices.html>

Also available in English under the title:
Canadian Biosafety Guideline – Conducting a Biosecurity Risk Assessment

Pour obtenir des copies supplémentaires, veuillez communiquer avec :

Agence de la santé publique du Canada
100 chemin Colonnade
Ottawa (Ontario) K1A 0K9
Tél. : 613-957-1779
Télec. : 613-941-0596
Courriel d'ASPC : PHAC.pathogens-pathogenes.ASPC@canada.ca

On peut obtenir, sur demande, la présente publication en formats de substitution.

© Sa Majesté la Reine du chef du Canada, représentée par la ministre de la Santé, 2018

Date de publication : juin 2018

La présente publication peut être reproduite sans autorisation pour usage personnel ou interne seulement, dans la mesure où la source est indiquée en entier.

N° de catalogue : HP45-23/2018F-PDF
ISBN : 978-0-660-26276-5
N° de publication : 180020

TABLE DES MATIÈRES

PRÉFACE	vi
ABRÉVIATIONS ET SIGLES.....	x
CHAPITRE 1 - INTRODUCTION.....	1
1.1 Objectif et portée.....	1
1.2 Aperçu	2
1.3 Comment utiliser la Ligne directrice canadienne sur la biosécurité : <i>Effectuer une évaluation des risques de biosûreté</i>	5
CHAPITRE 2 - PRÉPARATION.....	9
2.1 Rassembler la documentation.....	9
2.2 Contexte de la menace.....	9
2.3 L'équipe d'évaluation.....	10
2.4 Calendrier	10
CHAPITRE 3 - INVENTAIRE DES RESSOURCES.....	13
3.1 Identification des ressources.....	13
3.2 Priorité des ressources	14
CHAPITRE 4 - PROBABILITÉ.....	17
4.1 Identification des événements de biosûreté.....	17
4.2 Adversaires	18
4.3 Ressources ciblées	20
4.4 Fréquence.....	20
4.5 Calcul de la probabilité.....	22
CHAPITRE 5 - CONSÉQUENCE.....	27
5.1 Effets sur la santé publique, la santé animale et l'organisation	27
5.2 Vulnérabilités et efficacité des mesures d'atténuation.....	31
5.3 Calcul de la conséquence.....	34
CHAPITRE 6 - DÉTERMINER LE NIVEAU DE RISQUE ET CRÉER LE REGISTRE DES RISQUES.....	37
6.1 Calcul du risque	37
6.2 Registre des risques.....	37

CHAPITRE 7 - TOLÉRANCE AU RISQUE	41
CHAPITRE 8 - ATTÉNUATION ET RÉVISION	45
8.1 Atténuation	45
8.2 Révision	45
CHAPITRE 9 - RAPPORT DES RÉSULTATS.....	49
9.1 Résumé du rapport	50
9.2 Objectif	50
9.3 Portée	50
9.4 Contexte	50
9.5 Contexte de la menace.....	51
9.6 Inventaire des ressources	51
9.7 Résultats de l'évaluation des risques.....	51
9.8 Tolérance au risque	51
9.9 Recommandations	51
9.10 Annexe	52
CHAPITRE 10 -GLOSSAIRE.....	55
CHAPITRE 11 -RÉFÉRENCES.....	59
ANNEXE A -RESSOURCES.....	63
ANNEXE B -RESSOURCE DE BIOSÛRETÉ	69
ANNEXE C -ÉVÉNEMENTS DE BIOSÛRETÉ.....	73
ANNEXE D -ADVERSAIRES.....	75
ANNEXE E -MESURES D'ATTÉNUATION DE BIOSÛRETÉ.....	79



PRÉFACE



PRÉFACE

Au Canada, les installations où sont manipulés et entreposés des agents pathogènes humains ou des toxines de groupe de risque 2, 3 et 4 sont réglementées par l'Agence de la santé publique du Canada (ASPC) en vertu de la *Loi sur les agents pathogènes humains et les toxines* (LAPHT) et du *Règlement sur les agents pathogènes humains et les toxines* (RAPHT). L'importation d'agents zoopathogènes, d'animaux infectés, de produits d'animaux, de sous-produits d'animaux (p. ex. des tissus ou du sérum), ou d'autres substances qui pourraient être porteurs d'un agent zoopathogène ou d'une partie de celui-ci (p. ex. une toxine) est réglementée par l'ASPC ou l'Agence canadienne d'inspection des aliments (ACIA) en vertu de la *Loi sur la santé des animaux* (LSA) et du *Règlement sur la santé des animaux* (RSA).

La figure suivante illustre la hiérarchie des documents qu'utilisent l'ASPC et l'ACIA pour surveiller les activités de biosécurité et de biosûreté. Chaque niveau de la pyramide correspond à un type de document. Les documents sont placés en ordre de priorité du haut de la pyramide vers le bas. La législation et les règlements se trouvent au sommet de la pyramide, car ce sont ces documents qui transmettent l'autorité légale à l'ASPC et l'ACIA. Le matériel d'orientation et les éléments techniques se trouvent au bas de la pyramide, car ils sont uniquement destinés à résumer les recommandations et les informations scientifiques.

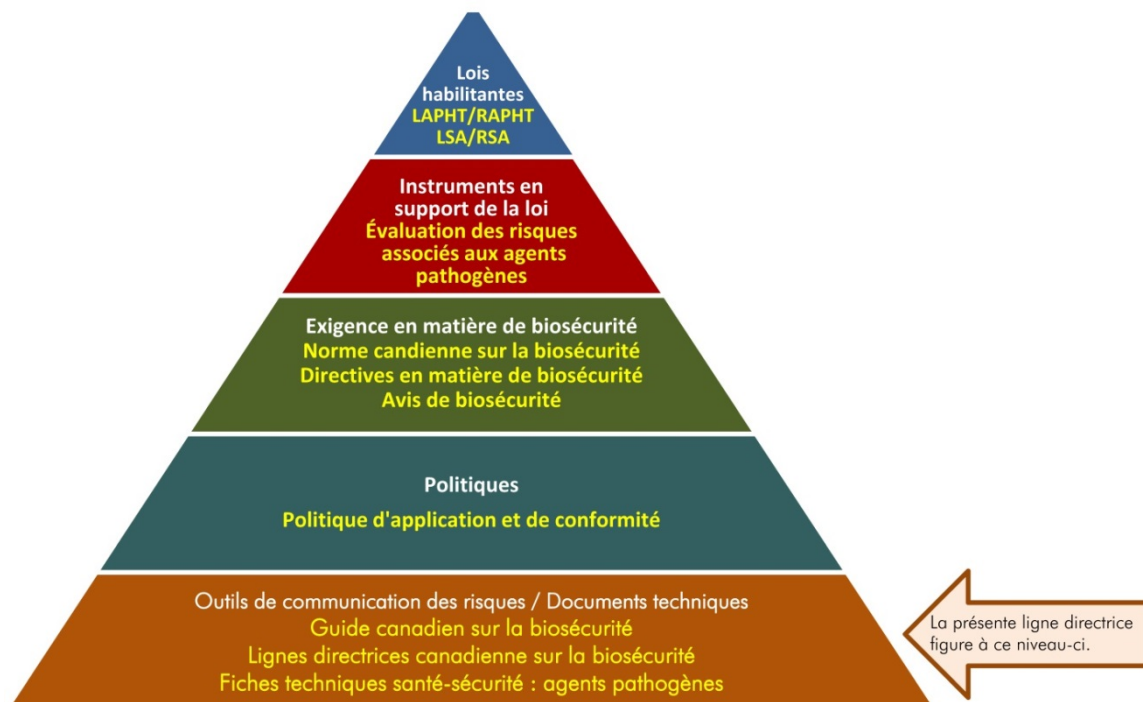
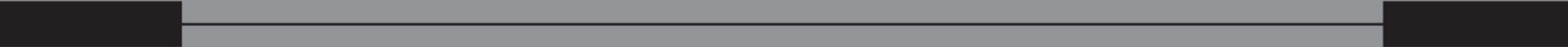


Figure 1 : La hiérarchie des documents en matière de biosécurité et de biosûreté du Gouvernement du Canada

Le présent document d'orientation a été élaboré par l'ASPC et l'ACIA dans le cadre d'une série de publications électroniques qui s'étendent sur les concepts liés à la biosécurité et la biosûreté présentés dans l'édition actuelle du *Guide canadien sur la biosécurité* (GCB), soit le document complémentaire à la *Norme canadienne sur la biosécurité* (NCB). La ligne directrice *Effectuer une évaluation des risques de biosûreté* présente une méthodologie pour l'évaluation des risques de biosûreté dans les installations où sont manipulés et entreposés des agents pathogènes humains, des agents zoopathogènes et des toxines. Cette ligne directrice vise à aider les parties réglementées à satisfaire aux exigences énoncées dans la NCB, mais les informations qu'elle contient ne devraient pas être interprétées comme des exigences. Les parties réglementées peuvent choisir d'adopter de différentes approches pour répondre aux exigences de la NCB.

La ligne directrice *Effectuer une évaluation des risques de biosûreté* est un document en constante évolution et fait continuellement l'objet d'améliorations. L'ASPC et l'ACIA accueillent avec intérêt les commentaires, les clarifications et les suggestions visant l'amélioration des versions subséquentes de ce document. Veuillez envoyer toute information ou suggestion accompagnées de leurs références à l'adresse suivante :

- Adresse courriel de l'ASPC : PHAC.pathogens-pathogenes.ASPC@canada.ca



ABRÉVIATIONS ET SIGLES



ABRÉVIATIONS ET SIGLES

ABCSE	Agent biologique à cote de sécurité élevée
ACIA	Agence canadienne d'inspection des aliments
ASPC	Agence de la santé publique du Canada
GCB	<i>Guide canadien sur la biosécurité</i>
GR	Groupe de risque (c.-à-d., GR1, GR2, GR3, GR4)
NCB	<i>Norme canadienne sur la biosécurité</i>
TI	Technologie de l'information

INTRODUCTION



CHAPITRE 1 - INTRODUCTION

Les termes en **caractères gras** sont définis dans le glossaire du chapitre 4.

1.1 Objectif et portée

La ligne directrice *Effectuer une évaluation des risques de biosûreté* propose une méthodologie pour effectuer une **évaluation des risques de biosûreté** en se fondant sur des directives introduites au chapitre 6 du *Guide canadien sur la biosécurité* (GCB) et sur d'autres directives présentées dans les méthodologies d'évaluation des **risques** aux échelles nationale et internationale^{1,2,3,4,5,6}. Au même titre que la *Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif*, cette ligne directrice aide les **installations** à se conformer aux exigences en matière de **biosûreté** au Canada⁷.

Comme énoncé dans la matrice 4.1 de la *Norme canadienne sur la biosécurité* (NCB), une évaluation des risques de biosûreté doit être effectuée dans les installations où des agents pathogènes, des toxines et d'autres matières infectieuses réglementés ainsi que des **ressources** connexes sont **manipulés ou entreposés**⁸. Les risques de biosûreté associés à ces matières sont définis et des stratégies d'atténuation appropriées sont déterminées afin de protéger les matières et les ressources connexes des **événements de biosûreté** (c.-à-d. vol, mésusage, détournement, libération intentionnelle non autorisée et perte accidentelle). Les installations peuvent décider d'effectuer une seule évaluation des risques de biosûreté au niveau de l'organisation, ou plusieurs évaluations distinctes propres à chaque emplacement ou zone de confinement.

L'information présentée dans cette ligne directrice, y compris les exemples, vise à fournir une méthodologie pour effectuer une évaluation des risques de biosûreté. Il existe plusieurs techniques et méthodologies d'évaluation des risques, et il incombe à l'organisation de déterminer quelle technique ou méthodologie convient le mieux à leur propre situation.

Une évaluation des risques de biosûreté comporte des considérations particulières comparativement à la **biosécurité** et aux autres évaluations des risques. Cependant, les principes, les concepts et l'approche générale sont plutôt similaires. Comme le décrit cette ligne directrice, une évaluation des risques de biosûreté s'intéresse aux événements de biosûreté ayant le potentiel d'entraîner des conséquences néfastes sur la santé publique, la santé animale, ou les deux, ainsi que sur l'organisation. De plus amples renseignements sur la biosécurité et la biosûreté sont disponibles dans le GCB.

L'information et les recommandations présentées dans la ligne directrice *Effectuer une évaluation des risques de biosûreté* n'existent qu'à titre indicatif et ne devraient pas être interprétées comme des exigences. Les parties réglementées peuvent choisir d'adopter de différentes approches pour répondre aux exigences de la NCB.

1.2 Aperçu

La manipulation et l'entreposage des agents pathogènes et des toxines posent un **risque** pour la santé publique, la santé animale, ou les deux. La gestion de ces risques nécessite que le personnel travaillant en laboratoire et dans d'autres zones de confinement où sont manipulés des agents pathogènes, des toxines, des matières infectieuses ou des animaux infectés soit sensibilisé au sujet des pratiques relatives à la biosécurité et la biosûreté et qu'il applique ces pratiques.

Pour gérer les risques de biosûreté, les installations sont tenues d'élaborer un **plan de biosûreté** traitant les risques faisant partie de l'évaluation des risques de biosûreté. La complexité du plan de biosûreté est proportionnelle aux risques que pose la compromission des ressources de l'installation. Le plan de biosûreté inclut les stratégies d'atténuation pour les risques associés à :

- la sécurité physique;
- la compétence et la fiabilité du personnel;
- la responsabilité à l'égard des agents pathogènes, des toxines et des autres matières infectieuses réglementées;
- l'inventaire;
- les interventions en cas d'incident ou d'urgence;
- la gestion de l'information.

Le risque est une fonction de la probabilité qu'un événement survienne et les conséquences de cet événement. La probabilité d'un événement de biosûreté est déterminée par trois facteurs : le motif de l'**adversaire**, la capacité de l'adversaire et la fréquence historique. La conséquence est déterminée par deux facteurs, soit l'effet et la **vulnérabilité** (qui est fondée sur l'efficacité des **mesures d'atténuation**), et évalue la gravité d'un événement de biosûreté. Les mesures d'atténuation efficaces d'une organisation cherchent à prévenir et à détecter les événements de biosûreté, ainsi qu'à y répondre et à s'en rétablir, pour ultimement réduire les risques. Les faiblesses des mesures d'atténuation (c.-à-d. les vulnérabilités) sont corrigées en améliorant les mesures d'atténuation existantes ou en en implémentant de nouvelles.

L'évaluation des risques peut être très subjective. Puisque les données sur les événements de biosûreté sont limitées et grandement variables, cette ligne directrice recommande d'exploiter les connaissances et l'expertise du personnel de l'organisation en assemblant une équipe d'évaluation des risques qui analysera collectivement les risques posés à une organisation.

Cette ligne directrice propose une approche flexible et évolutive aux évaluations des risques de biosûreté. Selon un nombre de facteurs (p. ex. la complexité des activités de l'organisation, les ressources disponibles, ou les contraintes fiscales ou de temps), il incombe à l'équipe d'évaluation des risques de déterminer le niveau de précision nécessaire pour chaque activité comprise dans le processus de l'évaluation des risques de biosûreté. Pour ce faire, il faut agréger les éléments similaires de l'évaluation des risques de biosûreté. Dans cette optique, il est recommandé que les éléments de l'évaluation des risques de biosûreté suivent une structure hiérarchique, commençant par une classe, une catégorie, un groupe ainsi qu'un niveau individuel, du composant ou de l'événement. La charge de travail et la complexité de l'évaluation peuvent être considérablement réduites en effectuant l'évaluation des risques de biosûreté au niveau du groupe ou de la catégorie, ce qui devrait être envisagé à moins qu'il y ait une raison d'évaluer certains éléments de façon individuelle. Les annexes B à E fournissent des exemples d'éléments d'évaluation des risques dans leur structure hiérarchique.

L'évaluation des risques fait partie de la gestion du risque et implique les cinq activités suivantes :

1. Établir un inventaire des ressources
2. Évaluer la probabilité des événements de biosûreté
3. Évaluer les conséquences de chaque événement de biosûreté
4. Analyser les risques
5. Déterminer la **tolérance au risque**

Les trois activités supplémentaires communes à la gestion de risque comprennent : la préparation, l'évaluation des vulnérabilités (qui sont fondées sur l'efficacité des mesures d'atténuation) et le renouvellement et l'amélioration continus. Le tableau 1-1 fournit un aperçu de la façon dont les étapes décrites dans cette ligne directrice se rapportent au processus de gestion des risques présenté dans le GCB et la norme ISO 31000 de l'Organisation internationale de normalisation⁹.

Tableau 1-1 : Rapport entre les étapes décrites dans cette ligne directrice et celles de l'ISO 31000 et du *Guide canadien sur la biosécurité* (GCB)

Les rangées en couleur mettent en évidence les différentes façons dont l'étape de l'évaluation des risques est décomposée dans chaque processus.

ISO 31000		<i>Guide canadien sur la biosécurité</i>	Ligne directrice <i>Effectuer une évaluation des risques de biosûreté</i>
Établir le contexte		Préparation	Préparation
Appréciation du risque	Identification des risques	Déterminer les ressources, les conséquences, les menaces et les vulnérabilités	Inventaire des ressources
			Probabilité
			Conséquence
	Analyse des risques	Évaluer les risques	Analyse des risques
	Évaluation des risques		Tolérance au risque
Traitement des risques		Atténuation	Atténuation
Contrôle et révision		Révision et amélioration continue	Révision et amélioration continue

Comme illustré dans le tableau 1-2, les composantes présentées dans cette ligne directrice sont évaluées selon une échelle à cinq valeurs correspondant aux niveaux :

- très faible (1);
- faible (2);
- modéré (3);
- élevé (4);
- très élevé (5).

Cette échelle sert à évaluer la priorité des ressources, la probabilité des événements de biosûreté, la gravité des conséquences et l'évaluation du niveau de risque.

Tableau 1-2 : Valeurs qualitatives et quantitatives des composantes

Valeur de la composante (quantitative)	1	2	3	4	5
Valeur de la composante (qualitative)	Très faible	Faible	Modéré	Élevé	Très élevé

Cette ligne directrice utilise des termes clés pour évaluer les valeurs des composantes, comme de niveau « très faible » à « très élevé », de « très peu fréquent » à « très fréquent », de « très peu motivé » à « très motivé », de « très limité » à « très sophistiqué », et de « négligeable » à « répandu ». Il incombe à l'organisation de définir le sens de ces termes clés.

1.3 Comment utiliser la Ligne directrice canadienne sur la biosécurité : *Effectuer une évaluation des risques de biosûreté*

Une liste détaillée des abréviations et des sigles utilisés dans cette ligne directrice est offerte au début du document. Chaque mot ou terme est écrit au long à sa première occurrence, suivi de son abréviation ou son sigle entre parenthèses. Par la suite, l'abréviation ou le sigle est utilisé exclusivement dans le reste du document. Au chapitre 10 se trouve un glossaire exhaustif où sont définis les termes techniques. Les termes qui y figurent apparaissent en **caractères gras** à leur première occurrence dans le document. Au chapitre 11 se trouve une liste des ressources citées en référence dans cette ligne directrice. La source des citations dans le texte sont énumérées dans les références à la fin de chaque chapitre.

Afin de faciliter la lecture du présent texte, nous avons employé le masculin comme genre neutre pour désigner aussi bien les femmes que les hommes.

Références

¹ Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada. Consulté à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosécurité/guide-deuxieme-edition.html>

- 2 Gouvernement du Canada, Centre de la sécurité des télécommunications, Gendarmerie royale du Canada. (2007). *Méthodologie harmonisée d'évaluation des menaces et des risques, Version 1.0.*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.cse-cst.gc.ca/fr/publication/trq-1>
- 3 Congressional Research Service. (2007). *The Department of Homeland Security Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Consulté le 30 mai 2017 à l'adresse <https://fas.org/sgp/crs/homesec/RL33858.pdf>
- 4 Sécurité publique Canada. (2012). *Lignes directrices sur la méthodologie d'évaluation tous risques, 2012-2013*. Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-sssmnt-fr.aspx>
- 5 Salerno, R. M. et Gaudioso, J. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, États-Unis : CRC Press.
- 6 Recherche et développement pour la défense Canada. (2017). *The Chemical, Biological, Radiological/Nuclear Explosive (CBRNE) Consolidated Risk Assessment (CRA) Rating Tool Guide*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805090_A1b.pdf
- 7 Gouvernement du Canada. (2016). *Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif*, Ottawa, ON : Gouvernement du Canada. Consulté à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/directrices/elaboration-plan-biosecurite-exhaustif-apercu.html>
- 8 Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité, 2e éd.*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/deuxieme-edition.html>
- 9 *ISO 31000:2009, Management du risque – Principes et lignes directrices*. (2009). Genève, Suisse : Organisation internationale de normalisation.

PRÉPARATION



CHAPITRE 2 - PRÉPARATION

La préparation est un préambule important de l'évaluation des risques de biosûreté. Elle consiste au moins à rassembler la documentation, à développer une compréhension du contexte de la **menace**, à définir la portée, à assembler une équipe d'évaluation et à établir un calendrier d'évaluation des risques.

2.1 Rassembler la documentation

La documentation concernant le mandat de l'organisation, les plans d'affaires, les plans d'étages, la fonction du programme, les évaluations globales des risques, les évaluations locales des risques (ELR), les évaluations des risques associés à l'agent pathogène, les Fiches techniques santé-sécurité : agents pathogènes (FTSSP) et les évaluations des risques de biosûreté existantes, ainsi que toute autre information pertinente, sera prise en considération lors du processus d'évaluation des risques de biosûreté et devrait être rassemblée préalablement¹.

2.2 Contexte de la menace

Développer une compréhension du contexte de la menace implique de rassembler de la documentation et d'autres renseignements recueillis de diverses sources et de rédiger un aperçu du contexte de la menace actuel pouvant avoir des effets sur l'organisation. Cette activité devrait aussi aller au-delà des événements de biosûreté actuels et historiques; elle devrait tenir compte des événements de biosûreté émergents pouvant se répandre davantage à l'avenir, avec l'évolution de la technologie et du contexte de la menace global. Se tenir au courant des événements de sécurité et de biosûreté locaux, nationaux et internationaux assurera une compréhension approfondie du contexte de la menace.

Consulter des unités de travail pertinentes, comme le service de sécurité au sein des organisations plus grandes, soutiendra cette activité. De même, les unités de sécurité de la technologie de l'information (TI) internes ou externes, qui sont responsables de la sécurité des systèmes et des réseaux informatiques, peuvent documenter des incidents de cybersécurité. Ces rapports contribueront à l'identification des événements de biosûreté et des adversaires potentiels.

Une collaboration entreprise avec des organismes d'application de la loi locaux, provinciaux et fédéraux pourrait constituer une source de statistiques sur les activités criminelles et suspectes à proximité de l'installation d'une organisation. Ces organismes peuvent être tenus de fournir des rapports de police, des cartes thermiques de la criminalité ainsi que l'accès au contenu en ligne à des fins d'évaluation des risques de biosûreté. L'annexe A présente une liste de ressources en ligne offrant des renseignements pertinents sur les menaces pouvant soutenir cette activité.

La portée de l'évaluation des risques de biosûreté devrait tenir compte des ressources de l'organisation et des événements de biosûreté potentiels pertinents inclus dans l'évaluation et indiquer ceux qui en sont exclus (p. ex. catastrophes naturelles et défaillances techniques).

2.3 L'équipe d'évaluation

L'équipe d'évaluation devrait être composée d'individus disposant d'une connaissance approfondie des activités de l'organisation. L'équipe d'évaluation devrait aussi comprendre un individu responsable de diriger l'évaluation des risques de biosûreté, soit souvent l'agent de la sécurité biologique (ASB); des cadres supérieurs responsables de définir la tolérance au risque de l'organisation; et d'autres individus qui mettront à contribution des connaissances pertinentes tout au long de l'évaluation des risques de biosûreté (p. ex. spécialistes de la sécurité, scientifiques, personnel de laboratoire, personnel des ressources humaines et personnel des TI).

La composition de l'équipe d'évaluation devrait être adaptée selon la complexité de l'évaluation des risques de biosûreté.

2.4 Calendrier

Un plan de projet décrivant les étapes et les délais devrait être élaboré. La durée de l'évaluation des risques de biosûreté dépendra de la complexité des activités, des ressources disponibles et des contraintes fiscales et de temps de l'organisation. Le calendrier devrait être suffisamment flexible pour tenir compte des changements imprévus susceptibles de modifier le risque ou les contextes de la menace. Le plan de projet de l'évaluation des risques peut inclure les étapes importantes du projet, la ou les personnes responsables de chaque étape importante, les délais, la durée prévue des tâches, les périodes de révision et les approbations.

Références

- 1 Gouvernement du Canada. Fiches techniques santé-sécurité : agents pathogènes (FTSSP). Ottawa, ON, Canada : Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/fiches-techniques-sante-securite-agents-pathogenes-evaluation-risques.html>

INVENTAIRE DES RESSOURCES



CHAPITRE 3 - INVENTAIRE DES RESSOURCES

3.1 Identification des ressources

L'inventaire des ressources constitue le fondement de l'évaluation des risques de biosûreté et mène à l'implémentation de mesures d'atténuation adéquates visant à contrer les événements de biosûreté. Les ressources peuvent être tangibles, intangibles ou des personnes. Les ressources tangibles peuvent être décrites à l'aide de caractéristiques physiques (p. ex. agents pathogènes, toxines, équipement, animaux et matériel). Les ressources intangibles n'ont pas de caractéristiques physiques (p. ex. information scientifique, connaissances, plan de biosûreté, processus logiques, et même la réputation de l'organisation). Les personnes-ressources comprennent les individus jouant un rôle clé dans l'accomplissement du mandat de l'organisation (p. ex. personnel, étudiants, entrepreneurs, cadres supérieurs et scientifiques).

Une attention particulière devrait être accordée aux ressources pouvant être utilisées à des fins malveillantes, comme causer la maladie chez les populations humaines ou animales ou susciter la peur de tels événements. Parmi ces ressources figurent celles ayant été désignées comme **agents biologiques à cote de sécurité élevée (ABCSE)**, d'autres agents pathogènes humains, agents zoopathogènes et toxines, ainsi que les ressources ayant une **possibilité de double usage**. La NCB exige qu'un inventaire des agents pathogènes et des toxines réglementés et entreposés à long terme (c.-à-d. plus de 30 jours) soit dressé et tenu à jour (matrice 4.10 de la NCB)¹. Il est exigé que les matières à risque plus élevé (c.-à-d. les ABCSE, matières du **groupe de risque 3 [GR3]** et du **GR4**) soient précisément identifiées. Comme indiqué dans le GCB, la quantité des agents pathogènes, des toxines et des ressources connexes peut être exprimée par une unité de mesure spécifique (p. ex. nombre de flacons ou de tubes ou quantité de masse), ou par une plage de valeur (p. ex. nombre d'animaux dans une colonie [10-15])². Ces renseignements permettent de déterminer et de documenter le potentiel de mésusage intentionnel des agents pathogènes ou des toxines et de prioriser les ressources en fonction de leurs propriétés et des conséquences de leur compromission.

Les agents pathogènes et les toxines ayant une possibilité de double usage représentent une préoccupation de premier plan en matière de biosûreté. Les agents pathogènes humains et les toxines ayant été reconnus comme présentant une possibilité de double usage sont appelés des ABCSE et sont qualifiés d'« agents pathogènes précisés » et de « toxines précisées » dans le *Règlement sur les agents pathogènes humains et les toxines (RAPHT)*³. En plus des agents pathogènes et des toxines, l'équipement et les connaissances ayant une

possibilité de double usage devraient également être identifiés. Un arbre décisionnel pour l'identification de la possibilité de double usage dans les recherches en sciences de la vie est inclus dans le *Plan de surveillance administrative à l'égard des agents pathogènes et des toxines dans un contexte de recherche - Éléments requis et lignes directrices* et fournit des directives sur l'identification d'agents pathogènes, de toxines et de ressources connexes, ainsi que des connaissances ayant une possibilité de double usage⁴. Les pratiques exemplaires imposent que les autres facteurs, par exemple la concentration, la quantité et l'état du matériel, soient aussi compris dans l'inventaire.

L'identification des ressources peut être complétée au niveau agrégé ou au niveau du composant (c.-à-d. classe, catégorie, groupe, et individuel ou composant). Les animaux peuvent être identifiés au niveau du groupe (p. ex. une colonie de rats) au lieu d'identifier chaque animal au niveau individuel. Inversement, les agents pathogènes et les toxines peuvent être identifiés au niveau du composant (p. ex. le virus de l'immunodéficiência humaine) au lieu d'identifier ces ressources à un niveau de groupe (p. ex. agent pathogène de GR3 ou toxine, bactérie, virus, ou parasite). Consultez l'annexe B pour un exemple de liste de ressources, dans leur structure hiérarchique, pouvant être comprise dans un inventaire des ressources de biosûreté.

3.2 Priorité des ressources

Identifier les propriétés d'une ressource, tout en tenant compte de la gravité des conséquences résultant de la compromission de cette ressource, aidera l'équipe d'évaluation à établir la priorité des ressources. Prioriser l'inventaire des ressources aidera ensuite l'équipe à établir les mesures d'atténuation nécessaires à la protection des ressources.

Cette ligne directrice propose que la priorité soit établie au moyen d'une échelle (p. ex. de 1 à 5, où la valeur 5 représente une priorité de niveau très élevé et 1 représente une priorité de niveau très faible). Consultez le tableau 3-1 pour un exemple d'inventaire des ressources.

Tableau 3-1 : Exemple d'inventaire des ressources de biosûreté

Classe de la ressource	Catégorie de la ressource	Groupe de la ressource	Composant	ABCSE	Groupe de risque	Quantité	État	Facilité d'utilisation	Emplacement	Possibilité de double usage	Valeur de priorité
Tangible	Biologique	Virus	VIH	Non	3	10 x 1ml tubes	Congelé	Difficile	Congélateur A	Non	Modéré (3)
Intangible	Information	Inventaire	Inventaire d'agent pathogène et de toxine	s.o.	s.o.	1	Électronique	s.o.	s.o.	s.o.	Élevé (4)
Tangible	Biologique	Bactérie	<i>Bacillus anthracis</i>	Oui	3	5 x 1ml tubes	Gelé	Difficile	Congélateur C	Oui	Très élevé (5)
Tangible	Biologique	Bactérie	<i>Bacillus subtilis</i>	Non	1	20 x 1ml tubes	Gelé	Difficile	Congélateur C	Non	Très faible (1)
Tangible	Équipement	Système de libération	Aérosol	s.o.	s.o.	1	s.o.	Facile	Congélateur C	Oui	Modéré (3)
Intangible	Perception/Réputation	Confiance publique	s.o.	s.o.	s.o.	s.o.	s.o.	s.o.	s.o.	s.o.	Très élevé (5)
Personnes	Employé	Scientifique	Professeur	s.o.	s.o.	20	s.o.	s.o.	s.o.	Oui	Très élevé (5)

Références

1 Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada. Consulté à l'adresse

<https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/deuxieme-edition.html>

2 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada. Consulté à l'adresse

<https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/guide-deuxieme-edition.html>

3 *Règlement sur les agents pathogènes humains et les toxines (DORS/2015-44)*. (2015).

4 Gouvernement du Canada. (2015). *Plan de surveillance administrative à l'égard des agents pathogènes et des toxines dans un contexte de recherche -*

Éléments requis et lignes directrices, Ottawa, ON, Canada. Consulté le 30 mai 2017 à l'adresse <https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/programme-delivrance-permis/plan-surveillance-administrative-a-egard-agent-pathogenes-toxines-contexte-recherche-elements-requis-lignes-directrices.html>

PROBABILITÉ



CHAPITRE 4 - PROBABILITÉ

Le Gouvernement du Canada définit la **menace** comme un « événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services »¹. Dans cette optique, déterminer la probabilité implique l'identification des événements de biosûreté ayant le potentiel de compromettre les ressources que possède une organisation. Avant de commencer cette activité, réviser le contexte de la menace examiné à l'étape préparatoire de l'évaluation des risques de biosûreté contribuera à établir le contexte.

L'évaluation des risques de biosûreté est axée sur l'identification des événements de biosûreté qui comprennent des pertes et des événements de nature délibérée (p. ex. vol, mésusage, détournement et libération non autorisée)^{2,3}. Tous les autres événements involontaires (p. ex. accidents, tremblements de terre, ouragans ou inondations) peuvent être pris en compte dans une approche tous risques, mais ils demeurent normalement hors de la portée de l'évaluation des risques de biosûreté. Les événements de biosûreté délibérés peuvent être exécutés par des adversaires externes ou internes, qui devraient être identifiés pour chaque événement de biosûreté.

L'évaluation de la probabilité comprend l'identification d'événements de biosûreté délibérés et de la détermination du motif, des moyens et de la capacité de l'adversaire ainsi que de la fréquence historique.

4.1 Identification des événements de biosûreté

Cette activité comprend l'identification des événements de biosûreté qui pourraient entraîner l'accès non autorisé, l'endommagement, la perte ou le mésusage des ressources d'une organisation. Il est également important de tenir compte de l'imprévisibilité des événements délibérés, qui peuvent être exécutés avec peu ou sans avertissement⁴. Cette activité devrait être axée sur les scénarios d'événements de biosûreté cherchant à cibler l'organisation directement. Ces scénarios peuvent être inspirés d'événements étant survenus sur place ou ailleurs (c.-à-d. historiques) ou pouvant survenir prochainement (c.-à-d. hypothétiques). Cette activité ne devrait pas comprendre de scénarios d'événements de biosûreté complexes (p. ex. ceux découlant d'un événement indirect) puisque les résultats possibles sont difficiles à déterminer⁴.

Les événements de biosûreté délibérés peuvent être exécutés à l'aide de moyens physiques ou de la cybertechnologie. L'équipe d'évaluation des risques devrait donc prendre en compte les deux types d'événements.

Il incombe à l'équipe d'évaluation de déterminer le niveau de détail jugé nécessaire pour cette activité. L'équipe d'évaluation peut décider d'agréger les événements de biosûreté possédant des similarités afin de réduire la complexité de l'évaluation des risques de biosûreté. Cela peut être accompli en organisant les événements de biosûreté en une structure hiérarchique (c.-à-d. classe, catégorie, groupe et événement individuel), comme illustré dans la figure 4-1. Cette ligne directrice recommande d'agréger les événements de biosûreté au niveau du groupe tout au plus.

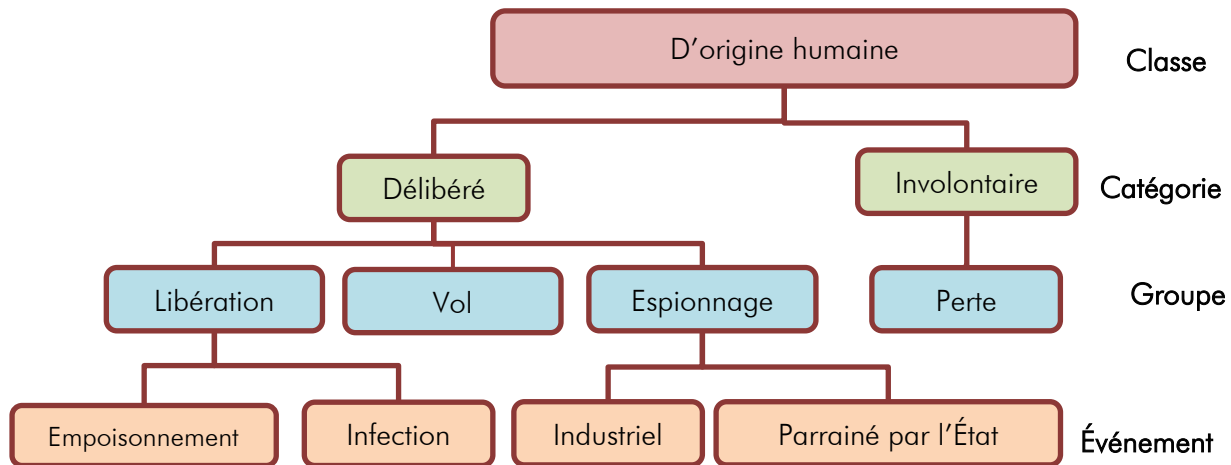


Figure 4-1 : Hiérarchie des événements de biosûreté

4.2 Adversaires

Les adversaires sont des individus ou groupes cherchant à délibérément compromettre les ressources d'une installation. Déterminer la probabilité implique d'identifier les adversaires (externes ou internes) pouvant posséder le motif, les moyens et la capacité d'exécuter un événement de biosûreté^{Error! Bookmark not defined.,Error! Bookmark not defined.,5}. L'occasion existe lorsque des adversaires ont la capacité d'exploiter les faiblesses des mesures d'atténuation.

Les adversaires internes, aussi appelés « menaces internes », sont des individus ayant un accès autorisé aux ressources d'une organisation. Les adversaires internes mécontents et la possibilité que les adversaires internes soient contraints, par du chantage ou des menaces, d'exécuter un événement de biosûreté ou qu'ils se fassent promettre une récompense pour en

exécuter un devraient être pris en compte. Parmi les exemples d'adversaires internes peuvent figurer des membres du personnel, des entrepreneurs, des étudiants et des bénévoles.

Les adversaires externes, aussi appelés « menaces externes », sont des individus, des organisations ou des groupes n'ayant pas d'accès autorisé aux ressources d'une organisation. Parmi les exemples d'adversaires externes peuvent figurer des manifestants, des activistes, des anciens employés, des visiteurs, des criminels opportunistes, des organisations criminelles, des acteurs solitaires, des organisations terroristes et des individus radicalisés.

Le motif de l'adversaire peut être déterminé par les intentions qu'exprime l'adversaire en question (p. ex. un employé mentionne aux autres qu'il libérera les animaux d'expérience) ou par un renseignement suggérant qu'un adversaire a l'intention d'exécuter un événement de biosûreté. Ces renseignements peuvent être fournis par des experts en la matière ou par des agences de sécurité. L'annexe A présente une liste des ressources en ligne pouvant soutenir cette activité.

Pour évaluer le motif de l'adversaire, cette ligne directrice recommande d'utiliser une échelle composée de cinq valeurs, comme suit :

- Très peu motivé (1)
- Peu motivé (2)
- Assez motivé (3)
- Motivé (4)
- Très motivé (5)

Le tableau 4-1 propose les gammes de niveaux utilisées dans l'évaluation du motif, des moyens et de la capacité de l'adversaire.

Dans le même ordre d'idées, les moyens et la capacité de l'adversaire (p. ex. son aptitude à contourner les mesures d'atténuation et à cultiver un agent pathogène ou à extraire une toxine) peuvent être exprimés au moyen d'une échelle composée de cinq valeurs, comme suit :

- Très limité (1)
- Limité (2)
- Assez sophistiqué (3)
- Sophistiqué (4)
- Très sophistiqué (5)

L'identification de l'adversaire peut se faire au niveau agrégé en regroupant les adversaires ayant des motifs similaires. Il est recommandé de mener cette activité en identifiant les adversaires dans une structure hiérarchique, comme présentée à l'annexe D. Cette ligne directrice recommande d'agréger les adversaires de biosûreté au niveau de la catégorie tout au plus.

Tableau 4-1 : Évaluation de l'adversaire

Motif	Valeur du motif	Moyens/Capacité	Valeur des moyens/de la capacité
Très motivé	Très élevé (5)	Très sophistiqué	Très élevé (5)
Motivé	Élevé (4)	Sophistiqué	Élevé (4)
Assez motivé	Modéré (3)	Assez sophistiqué	Modéré (3)
Peu motivé	Faible (2)	Limité	Faible (2)
Très peu motivé	Très faible (1)	Très limité/aucun	Très faible (1)

4.3 Ressources ciblées

Les adversaires cherchent à cibler une ou plusieurs ressources lorsqu'ils exécutent un événement de biosûreté. Dans cette optique, l'équipe d'évaluation devrait identifier toutes les ressources qui pourraient être ciblées.

4.4 Fréquence

L'évaluation de la probabilité tient compte de la fréquence historique d'un événement de biosûreté. Cela peut être accompli en utilisant les données disponibles ou en se basant sur les connaissances des employés et des experts en la matière. L'équipe d'évaluation peut juger utile de consulter les agences externes pour recueillir des données sur la fréquence des événements de biosûreté. L'annexe A présente une liste des ressources en ligne pouvant soutenir cette activité.

L'équipe d'évaluation devrait tenir compte des événements de biosûreté et des événements de sûreté ou de nature criminelle connexes (p. ex. entrée par infraction, vandalisme et

sabotage) étant survenus à proximité de l'installation d'une organisation (c.-à-d. à l'installation même ou à des installations locales similaires ne faisant pas partie de l'organisation) et des événements de biosûreté étant survenus à distance de l'installation (c.-à-d. à des installations similaires aux échelles régionale, nationale et internationale).

Le tableau 4-2 propose une échelle d'évaluation de la fréquence pour cette activité. Ce tableau devrait être utilisé selon l'hypothèse que les événements de biosûreté à proximité de l'installation de l'organisation indiqueraient une probabilité d'occurrence plus élevée. Inversement, les événements de biosûreté dans des endroits éloignés indiqueraient une probabilité d'occurrence plus faible^{Error! Bookmark not defined.}. La gamme de fréquences de l'occurrence des événements de biosûreté (p. ex. moins d'un mois, d'un mois à moins d'un an) devrait être examinée davantage. Il est recommandé que ce tableau soit adapté pour représenter la situation particulière de l'organisation.

La fréquence de la proximité et de la distance peut être déterminée au moyen d'une échelle composée de cinq valeurs, comme suit :

- Très peu fréquent/aucun (1)
- Peu fréquent (2)
- Assez fréquent (3)
- Fréquent (4)
- Très fréquent (5)

Tableau 4-2 : Évaluation de la fréquence d'un événement de biosûreté

Gamme de fréquences	Proximité	Valeur de la proximité	Distance	Valeur de la distance
< 1 mois	Très fréquent	Très élevé (5)	Très fréquent	Très élevé (5)
1 mois < 1 an	Très fréquent	Très élevé (5)	Fréquent	Élevé (4)
1 an < 5 ans	Fréquent	Élevé (4)	Assez fréquent	Modéré (3)
5 ans < 10 ans	Assez fréquent	Modéré (3)	Peu fréquent	Faible (2)
10 ans < 25 ans	Peu fréquent	Faible (2)	Très peu fréquent	Très faible (1)
> = 25 ans	Très peu fréquent/aucun	Très faible (1)	Très peu fréquent/aucun	Très faible (1)

4.5 Calcul de la probabilité

Pour récapituler, le calcul de la probabilité implique l'identification des événements de biosûreté délibérés et la détermination du motif, des moyens et de la capacité de l'adversaire ainsi que de la fréquence historique. Le tableau 4-3 présente un tableau de calcul de la probabilité dont l'équipe d'évaluation peut se servir pour déterminer la probabilité d'un événement de biosûreté en assignant une valeur de un à cinq (c.-à-d. 5 étant très élevé, et 1 étant très faible) au motif, aux moyens et à la capacité de l'adversaire ainsi qu'à la fréquence historique de l'événement de biosûreté. La valeur de la probabilité est une moyenne des quatre éléments, arrondie au nombre entier le plus près.

Tableau 4-3 : Évaluation de la probabilité

Adversaire		Fréquence		Valeur de la probabilité ^a
Motif	Moyens/Capacité	Proximité	Distance	
Très motivé (5)	Très sophistiqué (5)	Très fréquent (5)	Très fréquent (5)	Très élevé (5)
Motivé (4)	Sophistiqué (4)	Fréquent (4)	Fréquent (4)	Élevé (4)
Assez motivé (3)	Assez sophistiqué (3)	Assez fréquent (3)	Assez fréquent (3)	Modéré (3)
Peu motivé (2)	Capacités limitées (2)	Peu fréquent (2)	Peu fréquent (2)	Faible (2)
Très peu motivé/aucun (1)	Capacités très limitées/aucune (1)	Très peu fréquent/aucun (1)	Très peu fréquent/aucun (1)	Très faible (1)

a) La valeur de la probabilité est une moyenne des valeurs des quatre éléments, arrondie au nombre entier le plus près.

Le scénario de risque suivant démontre la façon d'utiliser le tableau de l'évaluation de la probabilité : Un groupe activiste pour la défense des animaux très motivé, mais ayant une capacité limitée, a libéré de façon délibérée des animaux infectés à proximité de l'installation d'une organisation une fois au cours des quinze dernières années. Au cours des cinq dernières années, ce groupe a une fois libéré de façon délibérée des animaux infectés provenant d'une autre installation dans une région du pays plus éloignée.

Exemple d'évaluation de la probabilité

Événement de biosûreté : libération délibérée

Ressource ciblée : animal infecté

Adversaire : groupe activiste pour la défense des animaux

Motif = très motivé (très élevé 5)

Capacité = très limité (très faible 1)

Fréquence (proximité) = peu fréquent (faible 2)

Fréquence (distance) = assez fréquent (modéré 3)

$$\begin{aligned}
 \text{Probabilité} &= (\text{motif} + \text{capacité} + \text{proximité} + \text{distance})/4 \\
 &= (\text{très motivé} + \text{très limité} + \text{peu fréquent} + \text{assez fréquent})/4 \\
 &= (5 + 1 + 2 + 3)/4 = 11/4 = 2,75
 \end{aligned}$$

Ainsi, la valeur de la probabilité est égale à 3 (arrondie au nombre entier le plus près), ou « modéré ».

Le tableau 4-4 présente des exemples supplémentaires d'évaluations de la probabilité d'un événement de biosûreté.

Tableau 4-4 : Exemple d'évaluation de la probabilité d'un événement de biosûreté

Scénario	Catégorie de l'événement de biosûreté	Groupe de l'événement de biosûreté	Classe de l'adversaire	Catégorie de l'adversaire	Adversaire	Ressources ciblées	Évaluation de la probabilité				
							Valeur du motif de l'adversaire	Valeur des capacités de l'adversaire	Valeur de la fréquence (proximité)	Valeur de la fréquence (distance)	Valeur de la probabilité ^a
Un groupe activiste pour la défense des animaux libère de façon intentionnelle un animal infecté	Délibéré	Libération intentionnelle	Externe	Activiste	Groupe activiste pour la défense des animaux	Animal	Très élevé (5)	Très faible (1)	Faible (2)	Modéré (3)	Modéré (3)
Un individu interne contraint commet un vol d'information ou de technologie intangibles	Délibéré	Vol	Interne	Entrepreneur	Personnel d'entretien	Technologie intangible	Modéré (3)	Très faible (1)	Faible (2)	Faible (2)	Faible (2)
Un employé mécontent utilise des ressources pour infecter le personnel	Délibéré	Mésusage	Interne	Personnel	Étudiant	Agent pathogène de GR3 et toxine; Personnel	Élevé (4)	Élevé (4)	Très faible (1)	Modéré (3)	Modéré (3)

a) La valeur de la probabilité est une moyenne des valeurs des quatre éléments, arrondie au nombre entier le plus près.

Références

- 1 Gouvernement du Canada, Secrétariat du Conseil du Trésor du Canada. (2012). *Politique sur la sécurité du gouvernement*. Consulté le 30 mai 2017 à l'adresse <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578>
- 2 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada. Consulté à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/guide-deuxieme-edition.html>
- 3 Salerno, R. M. et Gaudioso, J. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, États-Unis : CRC Press.
- 4 Gouvernement du Canada, Centre de la sécurité des télécommunications, Gendarmerie royale du Canada. (2007). *Méthodologie harmonisée d'évaluation des menaces et des risques, Version 1.0.*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.cse-cst.gc.ca/fr/publication/tra-1>

5 United States Centers for Disease Control and Prevention, Division of Select Agents and Toxins et United States Animal and Plant Health Inspection Service, Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities (2nd Revision)*. Consulté le 30 mai 2017 à l'adresse http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

CONSÉQUENCE



CHAPITRE 5 - CONSÉQUENCE

Les événements de biosûreté peuvent entraîner la mort, la maladie, des effets psychologiques et des effets sur l'organisation. La gravité de ces conséquences peut être atténuée par la mise en œuvre de mesures d'atténuation efficaces. En outre, des mesures d'atténuation efficaces renforceront la résilience et permettront un retour plus rapide aux activités régulières et à l'état de stabilité.

5.1 Effets sur la santé publique, la santé animale et l'organisation

Les événements de biosûreté peuvent avoir des effets physiques et psychologiques. Les effets physiques pourraient causer la mort ou la maladie limitée ou répandue chez les populations humaines ou animales. Les effets psychologiques pourraient susciter un sentiment de peur collectif. Les événements de biosûreté peuvent aussi entraîner des effets de divers degrés sur l'organisation, provoqués par des pertes de propriété intellectuelle et de renseignements exclusifs et par des activités d'intervention et de rétablissement coûteuses.

Les éclosions du syndrome respiratoire aigu sévère (SRAS)^a, du virus Ébola^b et de l'encéphalopathie spongiforme bovine (ESB)^c, bien qu'elles ne découlent pas d'actes délibérés, présentent des scénarios dont les équipes d'évaluation peuvent tenir compte lorsqu'elles déterminent la gravité des effets résultant d'une compromission des ressources d'une organisation. Ces éclosions, parmi d'autres, ont permis de confirmer que dans un monde de plus en plus interconnecté, les événements de biosécurité et de biosûreté ont le potentiel de franchir les frontières géographiques. Les événements de biosûreté de plus longue durée font augmenter les coûts d'intervention et de rétablissement; ainsi, les effets locaux, régionaux, nationaux et internationaux devraient être pris en compte lors de l'évaluation de l'effet.

a L'éclosion du SRAS en 2003, originaire d'une ferme isolée en Asie, a causé la maladie et la mort à l'échelle mondiale, y compris dans certaines régions du Canada (p. ex. Toronto).

b L'éclosion du virus Ébola en 2015 a été majoritairement restreinte au continent Africain et a causé la maladie et la mort chez des milliers d'individus.

c L'éclosion de l'ESB au Royaume-Uni en 2003, aussi connue sous le nom de la « maladie de la vache folle », a causé la mort de 2700 bovins.

Les effets physiques et psychologiques sur la santé publique comprennent les critères suivants :

- Cas de maladie négligeables ou inexistants et aucun décès, ou sentiment de peur collectif négligeable (1)
- Nombre limité de cas de maladie (un seul ou quelques-uns) et aucun décès, ou sentiment de peur collectif faible (2)
- Plusieurs cas isolés de maladie et mortalité minimal, ou sentiment de peur collectif modéré (3)
- Cas de maladie répandus et mortalité modéré, ou sentiment de peur collectif important (4)
- Cas de maladie répandus et mortalité élevé, ou sentiment de peur collectif répandu (5)

Les effets sur la santé animale comprennent les critères suivants :

- Effets négligeables chez le bétail de valeur moyenne à grande (1)
- Maladie limitée chez le bétail de valeur moyenne à grande (2)
- Quelques cas de maladie et un potentiel de mort chez le bétail de valeur moyenne à grande (3)
- Cas de maladie répandu et un potentiel de mort chez le bétail de valeur moyenne à grande (4)
- Mortalité élevé chez le bétail de valeur moyenne à grande (5)

Les effets sur l'organisation comprennent les critères suivants :

- Coûts négligeables associés aux activités d'intervention et de rétablissement; pertes négligeables de propriété intellectuelle, de renseignements exclusifs, reconnaissance pour les travaux de recherche ou de réputation de l'organisation (1)
- Coûts limités associés aux activités d'intervention et de rétablissement; pertes limitées de propriété intellectuelle, de renseignements exclusifs, de reconnaissance pour les travaux de recherche ou de réputation de l'organisation (2)
- Coûts importants associés aux activités d'intervention et de rétablissement; pertes importantes de propriété intellectuelle, de renseignements exclusifs, de reconnaissance pour les travaux de recherche ou de réputation de l'organisation (3)

L'objectif principal de la biosûreté est de prévenir la perte, le vol, le mésusage, le détournement ou la libération intentionnelle d'agents pathogènes, de toxines ou d'autres ressources connexes dans le but de protéger la santé et la sécurité des populations humaines

et animales. L'effet sur l'organisation fait partie de l'intérêt que porte l'organisation à la protection de ses ressources et à la production d'une évaluation des risques exhaustive. Puisque l'effet sur l'organisation, par définition, ne peut que toucher l'organisation, sa valeur d'effet maximale est « modéré » (3).

Les effets sur la santé publique, sur la santé animale et sur l'organisation peuvent être exprimés sous forme d'une valeur de 1 à 5, où 5 représente une valeur de niveau très élevé et 1 représente une valeur de niveau très faible, comme suit :

- Très faible (1)
- Faible (2)
- Modéré (3)
- Élevé (4)
- Très élevé (5)

La valeur de l'effet équivaut à la valeur la plus élevée des trois éléments évalués (c.-à-d. l'effet sur la santé publique, sur la santé animale ou sur l'organisation). Par exemple, si les effets d'un événement de biosûreté ont été évalués aux niveaux « modéré » sur la santé publique, « très faible » sur la santé animale et « faible » sur l'organisation, la valeur de l'effet sera fixée au niveau « modéré » puisque ce dernier représente la valeur la plus élevée des trois. Un événement de biosûreté particulier (p. ex. espionnage et sabotage) pourrait n'avoir aucun effet sur la santé publique ou la santé animale; cependant, ses effets sur l'organisation pourraient être importants et entraîner une importante perte de propriété intellectuelle, de renseignements exclusifs, de reconnaissance pour les travaux de recherche et de réputation ainsi que des pertes financières.

Le tableau 5-1 présente une matrice des effets, et le tableau 5-2 présente des exemples supplémentaires soutenant cette activité.

Tableau 5-1 : Évaluation des effets

Santé publique (physique ou psychologique)	Santé animale	Organisation	Valeur de l'effet ^b
- Cas de maladie répandus et mortalité élevée, ou - Sentiment de peur collectif répandu	Mortalité élevée chez le bétail de valeur moyenne à grande^a	La valeur maximale de l'effet sur l'organisation est « modéré » (3)	Très élevé (5)
- Cas de maladie répandus et mortalité modérée, ou - Sentiment de peur collectif important	Maladie répandue et potentiel de mort chez le bétail de valeur moyenne à grande^a	La valeur maximale de l'effet sur l'organisation est « modéré » (3)	Élevé (4)
- Plusieurs cas isolés de maladie et mortalité minimale, ou - Sentiment de peur collectif modéré	- Un peu de maladie et de potentiel de mort chez le bétail de valeur moyenne à grande^a - Mort répandue chez les autres animaux	- Coûts importants à modérés associés aux activités d'intervention et de rétablissement, ou - Pertes importantes de propriété intellectuelle, de renseignements exclusifs, de reconnaissance pour les travaux de recherche ou de réputation de l'organisation	Modéré (3)
- Nombre limité de cas de maladie (un seul ou quelques-uns) et aucun décès, ou - Sentiment de peur collectif limité	- Maladie limitée chez le bétail de valeur moyenne à grande^a - Maladie répandue et potentiel de mort chez les autres animaux	- Coûts limités associés aux activités d'intervention et de rétablissement, ou - Pertes limitées de propriété intellectuelle, de renseignements exclusifs, de reconnaissance pour les travaux de recherche ou de réputation de l'organisation	Faible (2)
- Cas de maladie négligeables ou inexistants et aucun décès, ou - Sentiment de peur collectif négligeable	- Effets négligeables chez le bétail de valeur moyenne à grande^a - Un peu de maladie et de potentiel de mort chez les autres animaux	- Coûts négligeables associés aux activités d'intervention et de rétablissement, ou - Pertes négligeables de propriété intellectuelle, de renseignements exclusifs, de reconnaissance pour les travaux de recherche ou de réputation de l'organisation	Très faible (1)

a) L'Agence canadienne d'inspection des aliments (ACIA) a classé les animaux selon la valeur économique de l'industrie à laquelle ils appartiennent pour le Canada comme suit :

1. Industries où le bétail a la plus grande valeur : bovine, équine, porcine, avicole, des crustacés, des poissons à nageoires (sauvages ou en élevage).
2. Industries où le bétail a une valeur moyenne : ovine et caprine, apicole, des mollusques, des autres ruminants en élevage (cervidés, bisons).
3. Industries où le bétail a la plus petite valeur et autres animaux de faible valeur : des lagomorphes (lapins), animaux de compagnie (chiens, chats, etc.), des reptiles, des amphibiens, des rongeurs, des primates non humains.

b) La valeur de l'effet équivaut à la valeur la plus élevée des trois éléments évalués.

Tableau 5-2 : Évaluation de l'effet

Scénario	Catégorie de l'événement de biosûreté	Groupe de l'événement de biosûreté	Classe de l'adversaire	Catégorie de l'adversaire	Ressources ciblées	Évaluation de l'effet			
						Valeur de la santé publique	Valeur de la santé animale	Valeur de l'organisation	Valeur de l'effet ^{a)}
Un groupe activiste pour la défense des animaux libère de façon intentionnelle un animal infecté	Délibéré	Libération	Externe	Activiste	Animal	Élevé (4)	Élevé (4)	Modéré (3)	Élevé (4)
Un individu interne contraint commet un vol d'information ou de technologie intangibles	Délibéré	Vol	Interne	Personnel	Technologie intangible	Sans objet	Sans objet	Modéré (3)	Modéré (3)
Un employé mécontent utilise des ressources pour infecter le personnel	Délibéré	Mésusage	Interne	Personnel	Agent pathogène de GR3 et toxine; Personnel	Modéré (3)	Modéré (3)	Faible (2)	Modéré (3)

a) La valeur de l'effet équivaut à la valeur la plus élevée des trois colonnes précédentes (effets sur la santé publique, sur la santé animale et sur l'organisation).

5.2 Vulnérabilités et efficacité des mesures d'atténuation

L'évaluation des risques de biosûreté implique d'évaluer les mesures d'atténuation existantes d'une organisation afin de déterminer s'il existe des vulnérabilités (c.-à-d. des mesures d'atténuation faibles) procurant aux adversaires l'occasion d'exécuter un événement de biosûreté¹.

Des mesures d'atténuation efficaces peuvent être mises en œuvre à chacune des étapes de la gestion des incidents (c.-à-d. prévention, détection, intervention et rétablissement). La prévention a pour objectif d'éliminer ou de réduire le risque d'occurrence d'un événement de biosûreté. La détection est axée sur l'identification précoce de l'événement de biosûreté, permettant ainsi une intervention rapide. L'intervention est l'action entreprise durant l'événement de biosûreté ou immédiatement avant ou après celui-ci afin d'atténuer ses conséquences. Le rétablissement comprend les activités exercées pour réparer les dommages ou rétablir les conditions à un niveau acceptable après l'occurrence d'un événement de biosûreté^{2,3,4}.

Une mesure d'atténuation peut avoir un seul ou plusieurs objectifs dans la sécurisation des ressources d'une organisation. L'évaluation de l'efficacité des mesures d'atténuation repose sur l'analyse de leur effet avant l'événement de biosûreté (c.-à-d. prévention) et de leur effet après l'événement de biosûreté (c.-à-d. détection, intervention et rétablissement). Cette évaluation est mieux dirigée par les spécialistes en sûreté de l'équipe d'évaluation¹.

L'efficacité d'une mesure d'atténuation peut être évaluée au moyen d'une échelle de cinq valeurs, comme suit :

- Très efficace (1)
- Efficace (2)
- Assez efficace (3)
- Inefficace (4)
- Très inefficace ou aucune mesure d'atténuation (5)

L'équipe d'évaluation devrait évaluer chaque mesure d'atténuation sur son efficacité d'atténuation des effets de l'événement avant l'événement de biosûreté (c.-à-d. prévention) et après l'événement de biosûreté (c.-à-d. détection, intervention et rétablissement). La valeur la plus élevée des deux sera la valeur de la vulnérabilité. Par exemple, si le personnel de sécurité est jugé « efficace » (c.-à-d. vulnérabilité de niveau « faible » [2]) avant l'événement et « assez efficace » (c.-à-d. vulnérabilité de niveau « modéré » [3]) après l'événement, la valeur de la vulnérabilité sera fixée à « modéré » (3). Il est possible qu'une mesure d'atténuation ne soit pas toujours applicable avant ou après l'événement de biosûreté. Dans de tels cas, la valeur de vulnérabilité est déterminée selon l'élément auquel la valeur a été assignée. Le tableau 5-4 présente un exemple d'une évaluation de mesure d'atténuation sur le filtrage de sécurité d'une organisation. Le tableau 5-3 peut servir de repère à l'équipe d'évaluation pour cette activité.

Tableau 5-3 : Évaluation de la vulnérabilité

Efficacité de la mesure d'atténuation		Valeur de la vulnérabilité ^a
Avant l'événement de biosûreté	Après l'événement de biosûreté	
Sans objet	Sans objet	Aucune
Très inefficace ou aucune mesure d'atténuation	Très inefficace ou aucune mesure d'atténuation	Très élevé (5)
Inefficace	Inefficace	Élevé (4)
Assez efficace	Assez efficace	Modéré (3)
Efficace	Efficace	Faible (2)
Très efficace	Très efficace	Très faible (1)

a) La valeur de la vulnérabilité équivaut à la valeur la plus élevée des deux éléments évalués.

Le résultat de cette activité peut prendre la forme d'un tableau énumérant chacune des mesures d'atténuation existantes au niveau agrégé ou au niveau du composant. L'identification et l'agrégation des mesures d'atténuation suivent l'ordre d'une structure hiérarchique, commençant par une classe, une catégorie, un groupe et un composant. L'agrégation devrait se faire au niveau du groupe ou du composant. Le tableau 5-4 présente un exemple des résultats pour cette évaluation jusqu'au niveau du groupe. Une mesure d'atténuation protégera une ou plusieurs ressources; dans cette optique, l'équipe d'évaluation devrait identifier toutes les ressources protégées par une mesure d'atténuation en particulier. Consultez l'annexe E pour un exemple de liste de mesures d'atténuation de biosûreté aux niveaux de la classe, de la catégorie, du groupe et du composant.

Tableau 5-4 : Exemple d'évaluation de la vulnérabilité

Ressource(s) protégée(s)	Événement(s) de biosûreté associé(s)	Classe de la mesure d'atténuation	Catégorie de la mesure d'atténuation	Groupe de la mesure d'atténuation	Évaluation de la vulnérabilité		
					Valeur avant l'événement de biosûreté	Valeur après l'événement de biosûreté	Valeur de la vulnérabilité ^a
Personnel, agents pathogènes, toxines, matières infectieuses, prions, renseignements, équipement	Vol, mésusage, libération, espionnage, adversaire interne	Programme de sécurité	Compétence du personnel	Filtrage de sécurité	Faible (2)	Sans objet	Faible (2)
Personnel, agents pathogènes, toxines, matières infectieuses, prions, renseignements, équipement	Vol, mésusage, libération, espionnage, adversaire interne	Programme de sûreté	Contrôle d'accès	Gardes de sécurité	Très faible (1)	Faible (2)	Faible (2)
Personnel, agents pathogènes, toxines, matières infectieuses, prions, renseignements, équipement	Vol, mésusage, libération, espionnage, adversaire interne	Programme de sûreté	Formation et sensibilisation	Formation sur la menace interne	Très élevé (5)	Sans objet	Très élevé (5)
Équipement, agents pathogènes, toxines, animaux	Vol, perte, adversaires internes et externes	Sécurité physique et programme de sécurité	Système de contrôle d'accès	Registre sur les entrées et les sorties	Très faible (1)	Très faible (1)	Très faible (1)
Personnel, agents pathogènes, toxines, matières infectieuses, prions, renseignements, équipement	Mésusage, libération, détournement, adversaires internes et externes	Programme de sécurité	Plan d'intervention d'urgence	Procédure de rétablissement en cas de libération	Sans objet	Faible (2)	Faible (2)

a) La valeur de la vulnérabilité équivaut à la valeur la plus élevée des deux éléments évalués.

5.3 Calcul de la conséquence

La valeur de la conséquence est le produit de la valeur de l'effet multiplié par la valeur de la vulnérabilité. Le tableau 5-5 combine les effets (tableau 5-2) et la vulnérabilité (tableau 5-4) en un seul tableau et démontre la façon dont plusieurs mesures d'atténuation peuvent être appliquées à chaque effet.

Tableau 5-5 : Exemple d'évaluation de la conséquence

RESSOURCE	Effet	Valeur de l'effet	Mesure d'atténuation	Valeur de la vulnérabilité
Animaux	Élevé sur la santé publique; Élevé sur la santé animale; Modéré sur l'organisation	Élevé (4)	Système de contrôle d'accès	Très faible (1)
			Gardes de sécurité	Faible (2)
Technologie/secr et commercial intangibles	Modéré sur l'organisation	Modéré (3)	Plan d'intervention d'urgence	Faible (2)
			Formation sur la menace interne ^a	Très élevé (5)
Agent pathogène de GR3; personnel de l'organisation	Modéré sur la santé publique; Faible sur l'organisation	Modéré (3)	Filtrage de sécurité	Faible (2)
			Formation sur la menace interne ^a	Élevé (4)
			Système de contrôle d'accès	Très faible (1)

a) Dans cet exemple fictive, la formation sur la menace interne est plus efficace pour la protection des agents pathogènes de GR3 et le personnel de l'organisation qu'à la protection de la technologie et des secrets commerciaux.

Références

- 1 Gouvernement du Canada, Centre de la sécurité des télécommunications, Gendarmerie royale du Canada. (2007). *Méthodologie harmonisée d'évaluation des menaces et des risques, Version 1.0.*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.cse-cst.gc.ca/fr/publication/trq-1>
- 2 Sécurité publique Canada. (2017). *Un cadre de sécurité civile pour le Canada - Troisième édition.* Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 2 juin 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-fr.aspx>
- 3 Sécurité publique Canada. (2013). *Renforcer la résilience face au terrorisme : Stratégie antiterroriste du Canada.* Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 2 juin 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/rsln-cgnt-trrrsm/index-fr.aspx>
- 4 Sécurité publique Canada. (2015). *La lutte contre la prolifération des armes chimiques, biologiques, radiologiques et nucléaires.* Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 2 juin 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/ntnl-scr/cntr-trrrsm/cntr-prlfrtn/index-fr.aspx>

DÉTERMINER LE NIVEAU DE RISQUE ET CRÉER LE REGISTRE DES RISQUES



CHAPITRE 6 - DÉTERMINER LE NIVEAU DE RISQUE ET CRÉER LE REGISTRE DES RISQUES

Le niveau de risque de biosûreté est fondé sur une analyse du risque associé à chaque ressource (ou chaque groupe de ressources partageant des caractéristiques similaires), soit une fonction de la probabilité d'un événement impliquant la ressource et de la conséquence de cet événement. Même s'il est assez improbable qu'ils surviennent, les événements ayant les conséquences les plus graves représentent les risques de biosûreté les plus élevés, suivis des événements ayant des conséquences modérées et étant plus susceptibles de survenir.

Ce chapitre présente la méthode de calcul du risque de biosûreté en utilisant les valeurs déterminées aux chapitres 3, 4 et 5, qui traitent de l'évaluation de la probabilité et des conséquences (tout en tenant compte des mesures d'atténuation existantes) des événements de biosûreté.

6.1 Calcul du risque

Le risque de biosûreté est déterminé selon l'analyse de chaque scénario de risque de biosûreté. Pour élaborer des scénarios de risque, il faut combiner les résultats de tous les tableaux d'événements de biosûreté en un seul tableau des résultats. Pour calculer le risque, il faut multiplier la valeur de la probabilité par la valeur de la conséquence (c.-à-d. effet et vulnérabilité) déterminées pour chaque scénario de risque de biosûreté. Le résultat de chaque calcul du risque indiquera une valeur de 1 à 125. Ces valeurs peuvent ensuite être regroupées en cinq niveaux de risque, allant de « très faible » à « très élevé », comme illustré au tableau 6-1. Le calcul du risque est présenté à la section 6.2.

Tableau 6-1 : Niveau de risque

Gamme de risque	1 – 4	5 – 18	19 – 34	35 – 74	75 – 125
Niveau de risque	Très faible	Faible	Modéré	Élevé	Très élevé

6.2 Registre des risques

Le registre des risques est un outil de gestion du risque commun servant à documenter les résultats de l'analyse du risque et de la planification d'interventions au risque. Il constitue une liste de tous les scénarios de risque et les niveaux de risque, présenté dans un format facile à

réviser, à modifier et à mettre à jour. Le tableau 6-2 présente un registre des risques créé à partir des scénarios de risque figurant dans cette ligne directrice.

Tableau 6-2 : Registre des risques

RESSOURCE	PROBABILITÉ			CONSÉQUENCE				NIVEAU DE RISQUE ^a
	Événement de biosûreté	Adversaire	Valeur de la probabilité	Effets	Valeur de l'effet	Efficacité de la mesure d'atténuation	Valeur de la vulnérabilité	
Animaux	Libération	Externe, activiste	Modéré (3)	Élevé sur la santé publique; Élevé sur la santé animale; Modéré sur l'organisation	Élevé (4)	Système de contrôle d'accès	Très faible (1)	Faible (12)
						Gardes de sécurité	Faible (2)	Modéré (24)
Technologie/secret commercial intangibles	Vol	Interne, personnel	Faible (2)	Modéré sur l'organisation	Modéré (3)	Plan d'intervention d'urgence	Faible (2)	Faible (12)
						Formation sur la menace interne	Très élevé (5)	Modéré (30)
Agent pathogène; personnel de l'organisation	Mésusage	Interne, personnel	Modéré (3)	Modéré sur la santé publique; Faible sur l'organisation	Modéré (3)	Filtrage de sécurité	Faible (2)	Modéré (18)
						Formation sur la menace interne ^b	Élevé (4)	Élevé (36)
						Système de contrôle d'accès	Très faible (1)	Faible (9)

a) Le niveau de risque est calculé en multipliant les valeurs de la probabilité, de l'effet et de la vulnérabilité.

b) Dans cet exemple fictive, la formation sur la menace interne est plus efficace pour la protection des agents pathogènes de GR3 et le personnel de l'organisation qu'à la protection de la technologie et des secrets commerciaux.

TOLÉRANCE AU RISQUE



CHAPITRE 7 - TOLÉRANCE AU RISQUE

La tolérance au risque désigne la volonté d'une organisation d'accepter ou de rejeter un niveau de **risque résiduel** donné, soit le risque restant après l'évaluation des mesures d'atténuation¹. La tolérance au risque est fondée sur le postulat selon lequel le risque zéro n'existe pas à moins que toute menace potentielle soit complètement éliminée (p. ex. la cessation des activités impliquant des agents pathogènes)². La tolérance au risque implique de définir le seuil ou le niveau de risque acceptable de l'organisation. Il incombe à la haute direction de déterminer le niveau acceptable de risque résiduel pour son organisation et d'assurer qu'il y ait suffisamment de ressources disponibles pour atténuer les risques jugés supérieurs au seuil de tolérance au risque².

Dans la figure 7-1, le seuil de tolérance au risque de l'organisation a été établi à « modéré ». Le résultat de cette décision signale des risques considérés comme de niveaux « élevé » et « très élevé ». Les risques supérieurs au seuil de tolérance au risque commandent la mise en œuvre de mesures d'atténuation supplémentaires. L'équipe d'évaluation des risques devrait identifier les mesures d'atténuation améliorées ou nouvelles, réévaluer la valeur de la vulnérabilité comme le démontre la section 5.2 et recalculer le risque comme le démontre la section 6.2 jusqu'à ce qu'il devienne inférieur au seuil de tolérance au risque. Dans le cadre des recommandations concernant les mesures d'atténuation, ces résultats devraient être documentés et communiqués aux cadres supérieurs dans le rapport d'évaluation des risques final.

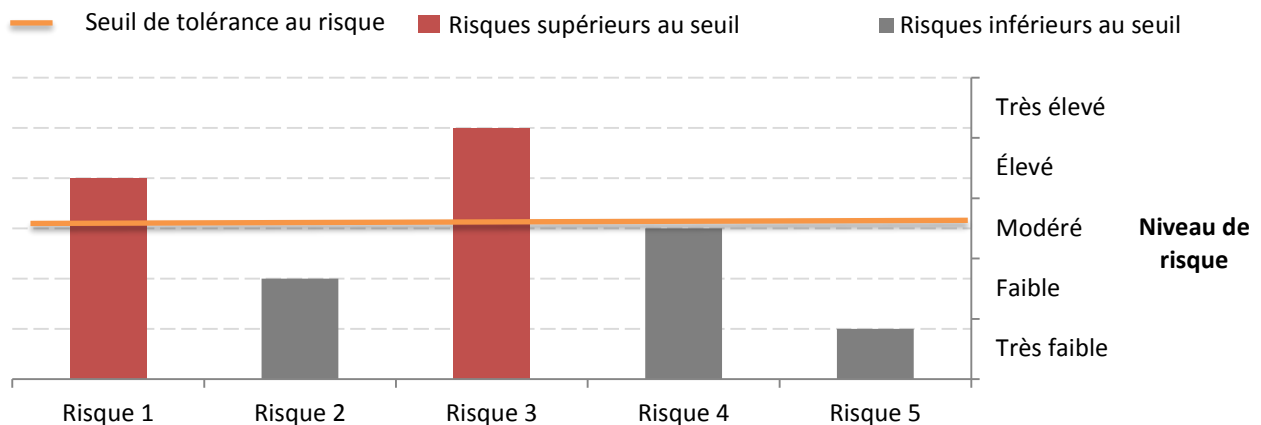


Figure 7-1 : Seuil de tolérance au risque

Selon le seuil de tolérance au risque, les risques inférieurs au seuil de tolérance au risque sont jugés acceptables ou non. Cependant, les risques dont la valeur se situe à l'une des extrémités d'un niveau de risque devraient être soigneusement examinés, comme le démontre

le tableau 7-1 pour l'élément marqué d'un « a », compte tenu surtout de la subjectivité des données d'entrée. Par exemple, un risque de niveau « modéré » pourrait s'être fait attribuer le score de 32, soit une valeur située à l'extrémité supérieure du niveau de risque « modéré » (voir le tableau 6-1). Dans cette situation, la haute direction pourrait choisir de traiter ce risque au moyen de mesures d'atténuation, même s'il est inférieur au seuil de tolérance au risque. Au fil de l'évolution du programme de biosûreté et de l'augmentation du nombre de risques de biosûreté atténués, le seuil de tolérance au risque peut être graduellement abaissé dans le but de réduire le niveau de risque global de l'organisation. Un tel abaissement graduel peut faire partie d'une plus vaste stratégie à long terme de l'organisation. L'acceptation des risques peut être documentée dans le registre des risques dans une colonne supplémentaire, comme le démontre le tableau 7-1.

Tableau 7-1 : Évaluation de l'acceptation des risques ajoutée à un registre des risques

RESSOURCE	PROBABILITÉ			CONSÉQUENCE				NIVEAU DE RISQUE	ACCEPTATION DU RISQUE
	Événement de biosûreté	Adversaire	Valeur de la probabilité	Effets	Valeur de l'effet	Mesure d'atténuation	Valeur de la vulnérabilité		
Animaux	Libération	Externe, activiste	Modéré (3)	Élevé sur la santé publique; Élevé sur la santé animale; Modéré sur l'organisation	Élevé (4)	Système de contrôle d'accès	Très faible (1)	Faible (12)	Accepté
						Gardes de sécurité	Faible (2)	Modéré (24)	Accepté
Technologie/secr et commercial intangibles	Vol	Interne, personnel	Faible (2)	Modéré sur l'organisation	Modéré (3)	Plan de gestion de l'intervention d'urgence	Faible (2)	Faible (12)	Accepté
						Formation sur la menace interne	Très élevé (5)	Modéré (30) ^a	Pas accepté
Agent pathogène de GR3; personnel de l'organisation	Méusage	Interne, personnel	Modéré (3)	Modéré sur la santé publique; Faible sur l'organisation	Modéré (3)	Filtrage de sécurité	Faible (2)	Modéré (18)	Accepté
						Formation sur la menace interne ^b	Élevé (4)	Élevé (36)	Pas accepté
						Système de contrôle d'accès	Très faible (1)	Faible (9)	Accepté

a) Risque dont la valeur se situe à l'extrémité supérieure de la gamme de risque « modéré ». Même si le risque est inférieur au seuil de tolérance au risque, la haute direction a décidé de l'atténuer.

b) Dans cet exemple fictive, la formation sur la menace interne est plus efficace pour la protection des agents pathogènes de GR3 et le personnel de l'organisation qu'à la protection de la technologie et des secrets commerciaux.

Références

- 1 Sécurité publique Canada. (2012). *Lignes directrices sur la méthodologie d'évaluation tous risques, 2012-2013*. Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdss/ll-hzrds-rsk-sssmnt-fr.aspx>
- 2 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/guide-deuxieme-edition.html>

ATTÉNUATION ET RÉVISION



CHAPITRE 8 - ATTÉNUATION ET RÉVISION

8.1 Atténuation

L'évaluation des risques de biosûreté permet d'orienter le plan de biosûreté, qui documente les mesures d'atténuation mises en place pour traiter les risques. Les risques supérieurs au seuil de tolérance au risque devraient être contrôlés au moyen de mesures d'atténuation supplémentaires ou améliorées. Une analyse coûts-avantages peut contribuer à déterminer les mesures d'atténuation dans lesquelles une organisation devrait concentrer ses efforts, son temps et son argent.

Les contraintes financières et les limites en matière de ressources peuvent poser des défis à la gestion des risques inacceptables. Comme point de départ, la haute direction peut choisir d'axer les mesures d'atténuation sur les risques ayant les plus grandes conséquences d'abord, puis de contrôler les risques restants au fur et à mesure que les ressources deviennent disponibles. Dans d'autres cas, si les risques sont jugés trop élevés ou trop coûteux à atténuer, le projet ou le programme de l'organisation pourrait devoir être modifié ou annulé.

Les recommandations concernant les mesures d'atténuation devraient être documentées dans le rapport final de l'évaluation des risques de biosûreté. De plus amples renseignements sur les mesures d'atténuation sont disponibles dans la ligne directrice canadienne sur la biosécurité : *Élaboration d'un plan de biosûreté exhaustif*¹.

8.2 Révision

Il est recommandé de régulièrement réviser l'évaluation des risques de biosûreté et de la mettre à jour lorsque nécessaire afin de répondre aux changements pouvant influencer le niveau de risque (p. ex. contexte de la menace, règlements et politiques, après l'occurrence d'un événement de biosûreté, renouvellement d'un programme, vulnérabilités récemment découvertes, construction d'une nouvelle installation et ajouts à l'inventaire des ressources d'une organisation ou suppressions de celui-ci)².

Références

1 Gouvernement du Canada. (2016). *Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif*, Ottawa, ON :

Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/directrices/elaboration-plan-biosecurite-exhaustif-apercu.html>

2 Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2e éd., Ottawa, ON, Canada : Gouvernement du Canada. Disponible à l'adresse

<https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/guide-deuxieme-edition.html>

RAPPORT DES RÉSULTATS



CHAPITRE 9 - RAPPORT DES RÉSULTATS

Une fois l'évaluation des risques de biosûreté complétée, les résultats et les recommandations pour la haute direction et les décideurs devraient être présentés dans un rapport d'évaluation des risques de biosûreté exhaustif. La décision de rédiger un rapport d'évaluation des risques de biosûreté est laissée à la discrétion de l'équipe d'évaluation puisque l'évaluation des risques de biosûreté est complète; cependant, résumer les résultats et mettre l'accent sur les risques plus élevés facilitera la communication et la compréhension de l'évaluation des risques de biosûreté. Le rapport devrait résumer l'évaluation des risques de biosûreté et présenter les scénarios représentant les risques les plus élevés et les recommandations visant l'atténuation des risques inacceptables. Ce rapport et l'évaluation des risques de biosûreté en soi pourraient contenir des renseignements de nature délicate et sont considérés comme des ressources à évaluer dans le processus de l'évaluation des risques.

Voici les dix sections proposées pour le rapport d'évaluation des risques de biosûreté :

1. Résumé du rapport
2. Objectif
3. Portée
4. Contexte
5. Contexte de la menace
6. Inventaire des ressources
7. Résultats de l'évaluation des risques
8. Tolérance au risque
9. Recommandations
10. Annexe :
 - a) Inventaire des ressources
 - b) Tableau des événements de biosûreté
 - c) Tableau de la probabilité
 - d) Tableau de la conséquence
 - e) Registre des risques
 - f) Calendrier
 - g) Membres de l'équipe

9.1 Résumé du rapport

Le résumé du rapport devrait apparaître au début du rapport et brièvement décrire l'objectif, la portée, le contexte, le contexte de la menace, les scénarios représentant les risques les plus élevés et les mesures recommandées pour atténuer ces risques.

9.2 Objectif

L'objectif devrait au moins présenter un court énoncé décrivant ce que le rapport de l'évaluation des risques de biosûreté tente d'accomplir. Par exemple : « Ce rapport présente les résultats de l'évaluation des risques de biosûreté du Laboratoire X et fournit des recommandations concernant les mesures d'atténuation pour les risques inacceptables ».

9.3 Portée

La portée devrait au moins inclure les éléments suivants :

- Le ou les sites compris dans l'évaluation
- Les événements de biosûreté et la période de temps évalués (c.-à-d. les événements de biosûreté qui devaient perdurer à court terme et à long terme)
- Les événements de biosûreté et la période de temps non évalués
- La classe ou le groupe de ressource visé par l'évaluation
- La classe ou le groupe de ressource non visé par l'évaluation

9.4 Contexte

Le contexte fait partie intégrante de la section d'introduction du rapport d'évaluation des risques de biosûreté. Cette section devrait au moins inclure les éléments suivants :

- Le mandat de l'organisation
- Les objectifs de l'organisation
- Une description de la raison pour laquelle l'évaluation des risques de biosûreté doit être effectuée ou mise à jour (p. ex. ajout de nouvelles ressources, évolution du contexte de la menace, relocalisation de l'installation)

9.5 Contexte de la menace

Le profil du contexte de la menace développé dans la section de préparation de l'évaluation des risques de biosûreté peut être modifié pour inclure tout résultat important découvert au cours du processus de l'évaluation des risques de biosûreté. La section du contexte de la menace devrait documenter les menaces qui devaient perdurer à court terme et à long terme, ainsi que les menaces émergentes.

9.6 Inventaire des ressources

L'inventaire des ressources décrit les ressources visées par l'évaluation des risques de biosûreté. Cette section devrait au moins résumer et identifier les ressources les plus importantes. Toute autre ressource identifiée devrait être documentée dans l'annexe.

9.7 Résultats de l'évaluation des risques

Les résultats de l'évaluation des risques de biosûreté devraient être axés sur les scénarios de risque supérieurs au seuil de tolérance au risque. Des représentations graphiques ou tabulaires des scénarios de risque enrichiront cette section. Un aperçu du registre des risques peut être utilisé comme aide visuel.

9.8 Tolérance au risque

Un court énoncé sur la tolérance au risque qu'a établie la haute direction devrait être inclus. Cet énoncé devrait au moins révéler le seuil de tolérance au risque choisi pour définir le niveau maximal du risque acceptable, ainsi que le raisonnement ayant mené à la décision.

9.9 Recommandations

Les recommandations permettront ultimement d'orienter le plan de biosûreté de l'organisation; ainsi, cette section devrait proposer des mesures d'atténuation. Cette section devrait au moins :

- identifier les scénarios de risque supérieurs au seuil de tolérance au risque;
- identifier les mesures d'atténuation inadéquates nécessitant plus d'attention; et,

- proposer des mesures d'atténuation supplémentaires pour réduire le niveau de risque de l'organisation.

Les recommandations peuvent aussi inclure une estimation des ressources requises à la mise en œuvre des mesures d'atténuation. Dans certains cas, cela peut exiger des dépenses ou de simples modifications des procédures de sécurité, ou de la formation et de la sensibilisation supplémentaires pour le personnel.

9.10 Annexe

L'annexe précise l'information sommaire du rapport d'évaluation des risques de biosûreté. L'annexe devrait au moins présenter tous les résultats développés au cours du processus de l'évaluation des risques, y compris les suivants :

- Inventaire des ressources
- Tableau des événements de biosûreté
- Tableau de la probabilité
- Tableau de la conséquence
- Registre des risques

L'annexe peut aussi inclure le matériel préparé à la première étape du processus de l'évaluation des risques de biosûreté, y compris les suivants :

- Calendrier de l'évaluation des risques de biosûreté
- Membres de l'équipe de l'évaluation des risques

GLOSSAIRE



CHAPITRE 10 - GLOSSAIRE

Il est important de souligner que bien que certaines des définitions fournies dans le glossaire ci-dessous soient universellement acceptées, plusieurs d'entre elles ont été créées spécifiquement pour répondre aux besoins de la NCB, du GCB ou de la *Ligne directrice canadienne sur la biosécurité : Effectuer une évaluation des risques de biosûreté*. Par conséquent, certaines définitions pourraient ne pas s'appliquer aux installations qui ne sont pas visées par la NCB.

Adversaire (pluriel : adversaires)	Un individu, une organisation ou un groupe qui a les capacités et le motif d'exécuter un événement menaçant. Un adversaire peut être interne ou externe, agissant seul ou sous l'ordre d'une organisation ou d'un état.
Agents biologiques à cote de sécurité élevée (ABCSE)	Sous-ensemble d'agents pathogènes humains et de toxines qui présentent un risque accru en matière de biosûreté en raison de la possibilité qu'on les utilise comme arme biologique. Au paragraphe 10 du <i>Règlement sur les agents pathogènes humains et les toxines</i> , les ABCSE sont identifiés comme des agents pathogènes et des toxines « précisés ». Les ABCSE comprennent donc tous les agents pathogènes du groupe de risque 3 et du groupe de risque 4 qui se retrouvent sur la <i>Liste des agents pathogènes humains et animaux et des toxines réglementés à l'exportation</i> , publiée par le Groupe d'Australie et sujette à modifications, à l'exception du virus Duvenhage, du virus rabique et de tous les autres du genre <i>Lyssavirus</i> , du virus de la stomatite vésiculaire ainsi que du virus de la chorioméningite lymphocytaire. Les ABCSE comprennent aussi toutes les toxines qui se trouvent à la fois à l'annexe 1 de la <i>Loi sur les agents pathogènes humains et les toxines</i> et sur la <i>Liste des agents pathogènes humains et animaux et des toxines réglementés à l'exportation</i> et qui sont présentes en quantités supérieures aux quantités seuils énoncées au paragraphe 10(2) du <i>Règlement sur les agents pathogènes humains et les toxines</i> .
Agent pathogène	Microorganisme, acide nucléique ou protéine ayant la capacité de causer une maladie ou une infection chez l'humain ou l'animal. Des exemples d'agents pathogènes humains figurent aux annexes 2 à 4 et à la partie 2 de l'annexe 5 de la <i>Loi sur les agents pathogènes humains et les toxines</i> , mais ils ne constituent pas une liste exhaustive; des exemples d'agents zoopathogènes peuvent être trouvés à l'aide du Système automatisé de référence à l'importation sur le site Web de l'Agence canadienne d'inspection des aliments.
Biosécurité	Ensemble des principes, des technologies et des pratiques liés au confinement mis en œuvre pour prévenir l'exposition involontaire à des agents pathogènes ou à des toxines, ou leur libération accidentelle.
Biosûreté	Ensemble des mesures qui visent à prévenir la perte, le vol, le mésusage, le détournement ou la libération intentionnelle d'un agent pathogène humain, d'une toxine ou d'autres ressources connexes (p. ex. le personnel, l'équipement, les matières non infectieuses et les animaux).

Cadres supérieurs	Autorité ultimement responsable de la délégation des pouvoirs appropriés en matière de biosécurité. Les cadres supérieurs sont chargés de s'assurer que le programme de biosécurité dispose de ressources suffisantes, que les exigences légales sont respectées, que l'ordre de priorité des problèmes à l'égard de la biosécurité et de la biosûreté est bien établi et que ces problèmes sont corrigés adéquatement.
Évaluation des risques de biosûreté	Évaluation des risques qui consiste à répertorier et à classer par ordre de priorité les agents pathogènes, les toxines, les matières infectieuses et les autres ressources connexes (p. ex. l'équipement, les animaux, les renseignements) présents dans une installation, à définir les menaces et les risques associés à ces matières, ainsi qu'à déterminer les stratégies d'atténuation appropriées afin de prévenir le vol, le mésusage, le détournement ou la libération intentionnelle de ces matières.
Événement de biosûreté	Acte délibéré qui implique des agents pathogènes ou des toxines, à des renseignements ou à de l'équipement ou qui y est associé, qui pourrait causer la maladie ou du tort aux gens, aux animaux ou aux deux ainsi qu'à l'organisation.
Groupe de risque (GR)	Groupe dans lequel les matières biologiques sont classées en fonction de leurs caractéristiques inhérentes, comme la pathogénicité, la virulence, le risque de propagation et l'existence d'un traitement prophylactique ou thérapeutique efficace. Le groupe de risque énonce le risque pour la santé du personnel et du public ainsi que la santé des animaux et des populations animales.
Incident	Événement ou situation pouvant causer une blessure, du mal, une infection, une intoxication, une maladie ou un dommage. Les incidents peuvent mettre en cause des matières infectieuses, des animaux infectés ou des toxines. Le déversement, la libération et la perte de matières infectieuses ou de toxines ainsi que l'exposition à celles-ci, la fuite d'un animal, les cas où un employé se blesse ou développe une maladie, l'accès non autorisé à la zone de confinement, une panne de courant, un incendie, une explosion, une inondation ainsi que toutes les autres situations de crise (p. ex. séisme, ouragan) sont des exemples d'incidents. Les accidents et ceux évités de justesse sont considérés comme des incidents.
Installation	Structure, bâtiment ou aire définie à l'intérieur d'une structure ou d'un bâtiment dans lesquels sont manipulées ou entreposées des matières infectieuses ou des toxines. Il peut s'agir d'un laboratoire de recherche, d'un laboratoire de diagnostic, d'une aire de production à grande échelle ou d'une zone où on héberge des animaux. Ce terme désigne également une succession de pièces ou un bâtiment contenant plusieurs de ces aires.
Inventaire	Liste des ressources biologiques d'une zone de confinement répertoriant les agents pathogènes, les toxines et les matières infectieuses entreposés à l'intérieur comme à l'extérieur de la zone de confinement.
Libération	Rejet de matières infectieuses ou de toxines hors du système de confinement.

Maladie	Trouble structural ou fonctionnel touchant un humain ou un animal vivant, ou une partie du corps de ceux-ci. Les maladies sont causées par une infection ou une intoxication et se manifestent généralement par des signes et des symptômes caractéristiques.
Manipulation ou entreposage	Englobent la possession, la manipulation, l'utilisation, la production, l'entreposage, le transfert, l'importation, l'exportation, la libération, le rejet ou l'abandon d'agents pathogènes, de toxines ou de matières infectieuses ainsi que l'accès à de telles substances. La manipulation et l'entreposage englobent donc toutes les activités réglementées comportant les agents pathogènes humains et les toxines énoncés au paragraphe 7(1) de la <i>Loi sur les agents pathogènes humains et les toxines</i> .
Matière infectieuse	Tout isolat d'un agent pathogène ou toute matière biologique qui contient des agents pathogènes humains ou des agents zoonotiques et, donc, qui représente un risque pour la santé humaine ou animale.
Menace	Événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services.
Mesure d'atténuation	Mesure mise en œuvre dans le but de prévenir et de repérer un événement ainsi que d'y répondre et de s'en rétablir.
Plan de biosûreté	Plan qui vise la mise en œuvre des stratégies d'atténuation pour les risques associés à : la sécurité physique; la compétence et la fiabilité du personnel; la responsabilisation relative aux agents pathogènes, aux toxines et autres matières infectieuses réglementées; l'inventaire; les interventions en cas d'incident et d'urgence; et la gestion de l'information.
Possibilité de double usage	Propriété d'un agent pathogène ou d'une toxine, d'une connaissance ou d'un équipement de pouvoir être utilisés autant pour mener des activités scientifiques légitimes (p. ex. à des fins commerciales ou médicales, aux fins de recherche) que pour créer sciemment une arme biologique ayant la capacité de causer du tort (p. ex. le bioterrorisme).
Ressources (singulier : ressource)	Ensemble des agents pathogènes, des matières infectieuses, des toxines et des ressources connexes que possède une installation, y compris le matériel, l'équipement, les matières biologiques non infectieuses, les animaux, la connaissance et les renseignements (p. ex. les protocoles, les résultats de recherche) ainsi que le personnel d'une installation.
Risque	Probabilité qu'un événement indésirable (p. ex. accident, incident, bris de confinement) survienne et conséquences de cet événement.
Risque résiduel	Le risque restant après la mise en œuvre de mesures d'atténuation.
Tolérance au risque	Le niveau de risque acceptable pour une organisation.
Toxine (microbienne)	Substance toxique produite par un microorganisme, ou dérivée de celui-ci, qui peut avoir des effets graves sur la santé humaine ou animale. Les toxines sont énumérées à l'annexe 1 et à la partie 1 de l'annexe 5 de la Loi sur les agents pathogènes humains et les toxines.
Vulnérabilité (pluriel: vulnérabilités)	Faiblesse relative aux barrières de sécurité physiques, aux pratiques opérationnelles (p. ex. la formation en matière de biosûreté), à la sécurité du personnel, à la sécurité du transport, à la sécurité de l'information ainsi qu'à la gestion des programmes d'une installation.

RÉFÉRENCES



CHAPITRE 11 - RÉFÉRENCES

- Congressional Research Service des États-Unis. (2007). *The Department of Homeland Security Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Consulté le 30 mai 2017 à l'adresse <https://fas.org/sgp/crs/homesecc/RL33858.pdf>
- Centers for Disease Control and Prevention des États-Unis, Division of Select Agents and Toxins et United States Animal and Plant Health Inspection Service, Agriculture Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities (2nd Revision)*. Consulté le 30 mai 2017 à l'adresse <https://stacks.cdc.gov/view/cdc/22411>
- Gouvernement du Canada, Centre de la sécurité des télécommunications, Gendarmerie royale du Canada. (2007). *Méthodologie harmonisée d'évaluation des menaces et des risques, Version 1.0.*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.cse-cst.gc.ca/fr/publication/tra-1>
- Gouvernement du Canada, Secrétariat du Conseil du Trésor du Canada. (2012). *Politique sur la sécurité du gouvernement*. Consulté le 30 mai 2017 à l'adresse <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578>
- Gouvernement du Canada. Fiches techniques santé-sécurité : agents pathogènes (FTSSP). Ottawa, ON, Canada : Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/fiches-techniques-sante-securite-agents-pathogenes-evaluation-risques.html>
- Gouvernement du Canada. (2016). *Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif*, Ottawa, ON : Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/directrices/elaboration-plan-biosecurite-exhaustif-aperçu.html>
- Gouvernement du Canada. (2015). *Plan de surveillance administrative à l'égard des agents pathogènes et des toxines dans un contexte de recherche - Éléments requis et lignes directrices*, Ottawa, ON, Canada. Consulté le 30 mai 2017 à l'adresse <https://www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire/programme-delivrance-permis/plan-surveillance-administrative-a-egard-agents-pathogenes-toxines-contexte-recherche-elements-requis-lignes-directrices.html>
- Gouvernement du Canada. (2016). *Guide canadien sur la biosécurité*, 2^e éd., Ottawa, ON, Canada : Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/guide-deuxieme-edition.html>
- Gouvernement du Canada. (2015). *Norme canadienne sur la biosécurité*, 2^e éd., Ottawa, ON, Canada : Gouvernement du Canada. Disponible à l'adresse <https://www.canada.ca/fr/sante-publique/services/normes-lignes-directrices-canadiennes-biosecurite/deuxieme-edition.html>

ISO 31000:2009, Management du risque – Principes et lignes directrices. (2009). Genève, Suisse : Organisation internationale de normalisation.

Loi sur la santé des animaux (L.C. 1990, ch. 21). (2015).

Loi sur les agents pathogènes humains et les toxines (L.C. 2009, ch. 24). (2015).

Recherche et développement pour la défense Canada. (2017). *The Chemical, Biological, Radiological/Nuclear Explosive (CBRNE) Consolidated Risk Assessment (CRA) Rating Tool Guide*, Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805090_A1b.pdf

Règlement sur la santé des animaux (C.R.C., ch. 296). (2015).

Règlement sur les agents pathogènes humains et les toxines (DORS/2015-44). (2015).

Salerno, R. M. et Gaudioso, J. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, États-Unis : CRC Press.

Sécurité publique Canada. (2012). *Lignes directrices sur la méthodologie d'évaluation tous risques, 2012-2013*. Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 30 mai 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdss/ll-hzrds-rsk-sssmnt-fr.aspx>

Sécurité publique Canada. (2013). *Renforcer la résilience face au terrorisme : Stratégie antiterroriste du Canada*. Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 2 juin 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/rsln-cgnst-trrrsm/index-fr.aspx>

Sécurité publique Canada. (2015). *La lutte contre la prolifération des armes chimiques, biologiques, radiologiques et nucléaires*. Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 2 juin 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/ntnl-scr/cntr-trrrsm/cntr-prlfrtn/index-fr.aspx>

Sécurité publique Canada. (2017). *Un cadre de sécurité civile pour le Canada - Troisième édition*. Ottawa, ON, Canada : Gouvernement du Canada. Consulté le 2 juin 2017 à l'adresse <https://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-fr.aspx>

RESSOURCES



ANNEXE A - RESSOURCES

Les hyperliens suivants, qui étaient exacts au moment de la publication de ce document, sont externes à l'ASPC. L'ASPC ne garantit aucunement qu'ils demeurent actifs ou que leur contenu soit mis à jour et exact.

RESSOURCES DU GOUVERNEMENT FÉDÉRAL	
Service canadien du renseignement de sécurité (SCRS) www.csis.gc.ca	Le SCRS a pour rôle d'enquêter sur les activités qui pourraient constituer une menace pour la sécurité du Canada et d'en faire rapport au gouvernement du Canada. Le SCRS publie des documents non classifiés portant sur des questions liées à la sécurité nationale et au renseignement, soit : des rapports annuels, des « regards sur le monde : avis d'experts », des « études hors-série : questions prioritaires », des tendances nationales et internationales en matière de sécurité, des perspectives ainsi que des menaces et risques potentiels. Publications analytiques et sur les menaces : www.csis.gc.ca/pblctns/index-fr.php
Gendarmerie royale du Canada (GRC) www.rcmp-grc.gc.ca	La GRC est le service de police national du Canada. Elle offre des services complets de police fédérale à tous les Canadiens et des services de police à contrat aux territoires, aux provinces, aux municipalités et aux communautés autochtones. Guide de sensibilisation au terrorisme et à l'extrémisme violent : www.grc.gc.ca/qc/pub/sn-ns/sn-ns-fra.htm Système de Signalement des incidents suspects (SIS) : www.rcmp-grc.gc.ca/fr/signalement-des-incidents-suspects-sis Groupes extrémistes et activistes : www.grc.gc.ca/qc/pub/sn-ns/ge-eg-fra.htm
Sécurité publique Canada (SP) publicsafety.gc.ca	Sécurité publique Canada assure la coordination de tous les ministères et organismes fédéraux qui ont pour mission de veiller à la sécurité nationale et à la protection des Canadiens et des Canadiennes. La Base de données canadienne sur les catastrophes comprend des renseignements détaillés sur plus de 1 000 catastrophes naturelles, incidents technologiques et conflits (nationaux et internationaux) qui ont eu lieu depuis 1900 au pays ou à l'étranger. www.securitepublique.gc.ca/cnt/rsrscs/cndn-dsstr-dtbs/index-fr.aspx La Passerelle d'information canadienne sur les infrastructures essentielles (Passerelle IE) est un espace de travail protégé par un mot de passe pour les intervenants du milieu des infrastructures essentielles publiques et privées et comprend des produits de sécurité nationale et de gestion des urgences développés par des organismes fédéraux. cigateway.ps.gc.ca La lutte contre la prolifération des armes chimiques, biologiques, radiologiques et nucléaires : www.securitepublique.gc.ca/cnt/ntnl-scr/cntr-trrrsm/cntr-prlfrtn/index-fr.aspx Entités terroristes inscrites : www.securitepublique.gc.ca/cnt/ntnl-scr/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-fr.aspx Le Centre canadien de réponse aux incidents cybernétiques (CCRIC), fonctionnant au sein de Sécurité publique Canada, publie des bulletins sur les cybermenaces et des alertes et

	produit des sommaires trimestriels des événements cybernétiques ayant touché les affaires et les infrastructures essentielles au Canada. www.securitepublique.gc.ca/cnt/ntnl-scr/cbr-scr/ccirc-ccirc-fr.aspx Le Centre des opérations du gouvernement (COG), fonctionnant au sein de Sécurité publique Canada, offre une intervention d'urgence intégrée tous risques en cas d'incident, y compris une connaissance de la situation à l'échelle nationale, des produits d'avertissement, des évaluations du risque, des politiques nationales en matière de gestion des interventions des urgences et des exercices. Les produits non confidentiels accessibles aux partenaires des secteurs public et privé sont disponibles dans la Passerelle IE. www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr-fr.aspx
Centre de la sécurité des télécommunications (CST) www.cse-cst.gc.ca	Le CST est responsable d'offrir des conseils et des directives en matière de renseignements électromagnétiques et de cybersécurité. Les 10 mesures de sécurité des TI : www.cse-cst.gc.ca/fr/node/1297/html/24674
Affaires mondiales Canada (AMC) www.international.gc.ca	AMC produit des rapports spéciaux sur les maladies infectieuses, des avis aux voyageurs et des contrôles à l'importation et à l'exportation. Guide des contrôles à l'exportation du Canada: www.international.gc.ca/controls-controles/about-a_propos/expor/guide.aspx?lang=fra
Agence de la santé publique du Canada (ASPC)	Autorité nationale en matière de biosécurité et de biosûreté pour les agents pathogènes humains, les toxines et un sous-ensemble d'agents pathogènes d'animaux terrestres. Information et lignes directrices sur la biosécurité et la biosûreté en laboratoire: www.canada.ca/fr/sante-publique/services/biosecurite-biosurete-laboratoire.html
Agence canadienne d'inspection des aliments (ACIA)	L'ACIA décide des niveaux de bioconfinement, des méthodes et des protocoles nécessaires pour travailler sans danger avec des agents zoopathogènes et zoonotiques, des produits chimiques dangereux et des phytoravageurs justiciables de quarantaine et protège le personnel des laboratoires, la population canadienne et l'environnement. Bureau du Confinement des biorisques et sécurité : www.inspection.gc.ca/animaux/confinement-des-biorisques-et-securite/fra/1300121579431/1315776600051
AUTRES RESSOURCES	
STRATFOR www.stratfor.com	Rapports sur la connaissance de la situation, analyses et prédictions des contextes de la menace à long-terme et analyse des événements.
World Economic Forum www.weforum.org	Prévision de risque mondial www.weforum.org/fr/agenda
Crime Reports crimereports.com	Cartes interactives des incidents criminels parmi les régions participantes, y compris le Canada.

Centers for Disease Control and Prevention des États-Unis www.cdc.gov	<i>Historical trends related to bioterrorism: An Empirical Analysis:</i> wwwnc.cdc.gov/eid/article/5/4/pdfs/99-0406.pdf <i>Biosafety in Microbiological and Biomedical Laboratories (5th Ed.).</i> Washington, DC, États-Unis : United States Government Printing Office. www.cdc.gov/biosafety/publications/bmbl5/index.htm
Department of Homeland Security, Federal Emergency Management Agency des États-Unis	<i>Risk Management Series: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.</i> www.fema.gov/es/media-library/assets/documents/2150
Université de Bradford	<i>Preventing Biological Threats: What You Can Do; et Biological Security Education Handbook: The Power of Team-Based Learning</i> www.bradford.ac.uk/social-sciences/peace-studies/research/publications-and-projects/guide-to-biological-security-issues/
OUTILS ET MÉTHODOLOGIES D'ÉVALUATION DES RISQUES CONNEXES	
Valeur de la ressource, menace/danger, vulnérabilité et risque www.fema.gov	Une méthodologie pour évaluer le risque de terrorisme et des catastrophes naturelles, comme développée par la Federal Emergency Management Agency (FEMA) des États-Unis. www.fema.gov/pdf/plan/prevent/rms/428/fema428_ch1.pdf
Méthodologie d'évaluation tous risques www.publicsafety.gc.ca	L'évaluation tous risques aidera à déterminer, à analyser et à établir l'ordre de priorités de tout un éventail de menaces malveillantes ou non. Le processus tient compte des vulnérabilités associées à des risques précis. Il permet aussi de déterminer les conséquences possibles d'une menace et les moyens d'atténuer les risques. www.securitepublique.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ll-hzrds-rsk-sssmnt-fr.aspx Sécurité publique Canada
Biorisk Assessment Models (BioRams) www.sandia.gov/	Logiciel BioRams servant à évaluer les événements de biosûreté, tout en mettant l'accent sur le bioterrorisme, développé par Sandia National Laboratories. www.biosecurity.sandia.gov/BioRAM/ Sandia National Laboratories
Modèle pour l'évaluation des risques et des vulnérabilités	brs.dk/eng/inspection/contingency_planning/rva/Pages/vulnerability_analysis_model.aspx Danish Emergency Management Agency
Outil harmonisé d'évaluation des menaces et des risques (EMR) www.cse-cst.gc.ca/ www.rcmp-grc.gc.ca/fr	L'EMR est une publication non classifiée, publiée sous l'autorité du chef du Centre de la sécurité des télécommunications (CST) et du Commissaire de la Gendarmerie royale du Canada (GRC). www.cse-cst.gc.ca/fr/publication/tra-1 Centre de la sécurité des télécommunications; Gendarmerie royale du Canada
Programme d'évaluation de la résilience régionale (PERR) publicsafety.gc.ca	Programme d'évaluation de la résilience régionale est un programme d'évaluation des risques exhaustif pour les propriétaires et les exploitants d'infrastructures canadiennes critiques. www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx

Organisation internationale de normalisation (ISO) www.iso.org/fr/home.html	CAN/CSA-ISO 31000-10 (R2015) <i>Management du risque – Principes et lignes directrices</i>
Association canadienne de normalisation (CSA) www.csagroup.org/fr/	CAN/CSA-IEC/ISO 31010-10 (R2015) <i>Gestion des risques – Techniques d'évaluation des risques</i>
Hazard, Risk and Vulnerability Analysis (HRVA) Toolkit	www2.gov.bc.ca/gov/content/safety/emergency-preparedness-response-recovery/local-emergency-programs/hazard-risk-and-vulnerability-analysis Emergency Management British Columbia (EMBC). Gouvernement de la Colombie-Britannique www2.gov.bc.ca

RESSOURCES DE BIOSÛRETÉ



ANNEXE B - RESSOURCE DE BIOSÛRETÉ

Voici un exemple de liste de ressources pouvant être comprise dans l'évaluation des risques de biosûreté.

Classe	Catégorie	Groupe	Composant/Individu
Tangible	Matières biologiques	GR1	<i>Bacillus subtilis</i>
			<i>Bacillus lichenformis</i>
			Virus adéno-associés
		GR2	<i>Actinobacillus pleuropneumoniae</i>
			Virus de l'Hépatite D
			<i>Sporothrix schenckii</i>
		GR3	<i>Mycobacterium tuberculosis</i>
			<i>Penicillium marneffei</i>
			Virus rabique
		GR4	Virus de l'herpès B
			Virus Hendra
			Virus de la fièvre de Lassa
		Toxine	Du choléra
			Diphthérique
		ABCSE	Toxine de type Shiga (vérotoxine)
			<i>Bacillus anthracis</i>
			Virus de Lassa
	Équipement	Équipement d'entreposage pour matières biologique	Congélateur verrouillable
			Coffre-fort
		Équipement de production	Fermenteur
		Système de dissémination d'aérosol	Pulvérisateur
		Sécurité physique	Système de détection d'intrusion
			Système électronique de contrôle de l'accès
			Capteurs de bris de verre
			Télévision en circuit fermé
			Alarmes sonores
			Serrures
			Déchiquiteurs
			Alarme/détecteur d'incendie
	Logiciel	Sécurité	Alarmes
			Serveur pour le système de détection d'intrusion
			Système électronique de contrôle de l'accès

	Technologies de l'information (TI)	Matériel	Ordinateurs et périphériques
			Point d'accès au réseau
			Imprimante de réseau
			Dispositif de stockage électronique externe
			Stockage en réseau
			Stockage infonuagique
Intangible	Animal	Colonie de primates	
		Colonie de souris	
	Information	Inventaire	Agent pathogène et toxine
			Autorisations d'accès et registres
			Plans de l'édifice et de l'étage (plans d'ingénierie)
			Système de gestion de la base de données
		Information scientifique et exclusive	Processus
			Techniques
			Séquence génique
		Sécurité	Évaluation des risques de biosûreté
			Plan de biosûreté
			Procédures opératoires normalisées
	Perception/réputation	Morale des employés	
		Confiance des employés	
		Confiance du public	
		Avantage concurrentiel	
Personne	Personnel	Scientifique	Professeur
			Professeur agrégé
		Étudiant	De premier cycle
			Au cycle supérieur
			Postdoctoral
		Soutien administratif	Adjoint exécutif
		Exécutif	Directeur
			Directeur général
			Doyen
		Gestionnaire/superviseur	Production
			Projet
		Personnel des technologies de l'information (TI)	Soutien aux logiciels et à l'équipement
			Spécialistes de la sécurité des TI
		Sûreté et sécurité	Agent de la sécurité
			Agent de la sécurité biologique

EFFECTUER UNE ÉVALUATION DES RISQUES DE BIOSÛRETÉ

	Entrepreneur	Personnel d'entretien	Superviseur d'entretien
			Personnel d'entretien
		Personnel des installations	Gestionnaire des installations
			Personnel des installations
		Sûreté	Garde de sécurité/commissionnaire

ÉVÉNEMENTS DE BIOSÛRETÉ



ANNEXE C - ÉVÉNEMENTS DE BIOSÛRETÉ

Voici un exemple de liste d'événements de biosûreté pouvant être comprise dans l'évaluation des risques de biosûreté.

Classe	Catégorie	Groupe	Événement
D'origine humaine	Délibéré	Mésusage	
		Libération non autorisée	Empoisonnement
			Maladie/infection
		Détournement	En transit
			Piratage de la chaîne logistique
		Extorsion	Cyberextorsion
			Rançon
			Kidnapping
			Récompense
		Subversion	Lobbying
			Propagande
			Politique
		Sabotage	Destruction
			Vandalisme
			Maliciels
			Déni de services
			Incendie
			Chaîne logistique (p. ex. équipement, services)
		Explosif	Bombe
		Espionnage	Industriel (p. ex. écoute électronique, introduction par effraction, coercition, piratage sophistiqué, écoute clandestine)
			Parrainé par l'État (p. ex. écoute électronique, introduction par effraction, coercition, piratage sophistiqué, écoute clandestine)
		Terrorisme	Local
			International
		Criminel	Vol
	Accidentel	Perte	

ADVERSAIRES



ANNEXE D - ADVERSAIRES

Voici un exemple de liste d'adversaires pouvant être comprise dans l'évaluation des risques de biosûreté.

Classe de l'adversaire	Catégorie de l'adversaire	Groupe de l'adversaire	Adversaire
Interne	Personnel	Scientifique	Professeur
			Professeur agrégé
		Étudiant	De premier cycle
			Au cycle supérieur
			Postdoctoral
		Administration	Adjoint exécutif
		Analyste	Analyste de programme
		Cadre supérieur	Directeur
			Directeur général
			Doyen
		TI	Soutien aux logiciels et à l'équipement
			Spécialiste de la sécurité des TI
		Personnel de bureau	
		Sûreté et sécurité	Chef de la sécurité
			Agent de la sécurité biologique
	Entrepreneur	Personnel d'entretien	
		Personnel des installations	
		Garde de sécurité/commissionnaire	
Externe	Terroriste	International	
		Local	
		Individu radicalisé	
	Parrainés par les États	Pirate informatique	Pirate d'élite
			Pirate amateur
		Service du renseignement	
		Militaire	

Classe de l'adversaire	Catégorie de l'adversaire	Groupe de l'adversaire	Adversaire
		Département/Agence/Ministère	
		Entreprise d'État	
	Non-parrainés par les États	Organisation	Concurrent
		Groupe activiste et militant	Animal
			Environnemental
			Écologique
			Pirates
			Anarchiste
			Hyper-nationaliste
			Anti-mondialisation
	Personnes agissant seules		
	Visiteur	Citoyen canadien	
		Étranger	
	Criminel	Syndicat du crime	
		Acteur solitaire	

MESURES D'ATTÉNUATION DE BIOSÛRETÉ



ANNEXE E - MESURES D'ATTÉNUATION DE BIOSÛRETÉ

Voici un exemple de liste de mesures d'atténuation de biosûreté pouvant être comprise dans l'évaluation des risques de biosûreté.

Classe	Catégorie	Groupe	Composant
Sécurité physique	Barrières de sécurité	Portes	À parement métallique
			À âme vide
			En verre
			En aluminium
			En acier
			À âme pleine en bois
		Fenêtres	À double vitrage
			Trempées
			En feuille
			À barreaux
			Résistantes aux explosions
	Contrôles d'accès	Serrures	Clés mécaniques
			Système électronique programmable pour le contrôle des accès (cartes-clés électroniques)
			Clavier à touches aléatoires
			Ouverture à distance
			Biométrie
			Clé de chiffre
			Clavier
			Série de serrures à clé passe-partout
			Cadenas
			Pênes demi-tour
			Pênes dormants

EFFECTUER UNE ÉVALUATION DES RISQUES DE BIOSÛRETÉ

	Surveillance et contrôle	Télévision en circuit fermé	Caméra (HD, vision nocturne, 360)
			Champ de vue des caméras (angles morts, chevauchement)
			Entreposage des medias enregistrés (court terme, long terme)
		Technologie d'inviolabilité	Étiquettes
			Seaux
			Label
		Détection d'intrusion	Détection de mouvement à infrarouges
			Détection du mouvement
			Interrupteur magnétique
			Mouvement acoustique
			Acoustique
			Détecteur de verre brisé
			Logiciel
			Champ de détection du capteur (angles morts, chevauchement)
Sécurité des renseignements	Formation et sensibilisation	Formation	Politiques en matière de TI
			Politique sur les dispositifs de stockage électronique amovibles
Sécurité du personnel	Procédures opératoires normalisées	Surveillance et contrôle	Reconnaissance visuelle
			Surveillance par CCTV
		Patrouilles	Gardes de sécurité
		Protection	Cadre supérieur
Programme de sécurité	Politiques sur la sécurité	Compétence et fiabilité du personnel	Habilitation de sécurité en vertu de la Loi sur les agents pathogènes humains et les toxines
			Programme d'évaluation de la fiabilité du personnel continu
			Historique de casier judiciaire
			Preuve d'attestation d'études
			Vérification des références
			Vérification de solvabilité
			Dépistage de drogues
		Entreposage du matériel	Politique du bureau dégagé
			Politique du bureau fermé
			Classification des documents (p. ex. exclusif, confidentiel, restreint)
			Gestion de l'inventaire (entreposage à long terme)

EFFECTUER UNE ÉVALUATION DES RISQUES DE BIOSÛRETÉ

		Diffusion de l'information	Politique sur les appareils d'enregistrement électroniques (cellulaires, diffuseurs de médias), coffres-forts dans les zones de sécurité
		Sécurité durant le déplacement et le transport	Matières réglementées
	Contrôles d'accès	Procédures de contrôle des visiteurs	Ouverture/fermeture de session (heures d'ouverture)
			Ouverture/fermeture de session (après les heures d'ouverture)
			Vérification de l'identité
			Accompagnateur du visiteur (accompagnement et supervision)
			Pièces d'identité du visiteur
		Procédures de contrôle du personnel	Politique anti-talonnage
		Identification du personnel	Politique sur l'interdiction d'accès (cartes d'identité, clés)
			Cartes d'identité
		Politique sur le doublage des clés	
		Registres du système de contrôle d'accès	Registres des accès autorisés et refusés du système électronique de contrôle de l'accès
	Intervention en cas d'incident et d'urgence	Enquêtes sur les incidents/Procédure d'intervention	Libération
			Équipement et ressources intangibles
		Déclaration des incidents	Comportement suspect (travail après les heures de travail, demandes d'accès à l'information injustifiée, non-conformité volontaire, changements de comportement)
			Formulaire de rapport d'incident ou PON
		Intervention aux incidents	Discordances dans l'inventaire (d'agents pathogènes ou de toxines)
			Défaillance de l'équipement
			Carte d'identité perdue ou volée
			Ordinateur portable perdu ou volé
			Expulsion d'individus non autorisés

	Formation et sensibilisation	Sensibilisation	Formation sur la menace interne
			Traitement de l'information de nature délicate
			Politiques sur la sécurité de la technologie de l'information
			Sensibilisation à la sécurité
			Transfert de ressources tangibles et intangibles
			Besoin de savoir
		Procédures de sécurité pour la formation	Individus suspects
			Colis suspect
			Appareils d'enregistrement électroniques

