# La gestion des risques d’un séjour

# GUIDE MÉTHODOLOGIQUE

Le processus d’évaluation des risques est accompli en amont du développement d’un séjour. Il sert à l’évaluation et l’approbation de tout nouveau séjour ou à une reconduction. Si la planification du séjour s’étend sur plusieurs mois et que le contexte de sécurité évolue au cours de cette période, il est nécessaire de refaire le processus – en partie ou entièrement.

Afin d’assurer des résultats optimaux, l’évaluation des risques liés aux séjoursdevrait :

* Être menée par une personne qualifiée et qui dispose du temps et des ressources pour la réaliser;
* Intégrer les données issues de plusieurs sources (Affaires mondiales Canada, rapport d’accidents et d’événements évités de justesse, sites Internet gouvernementaux de différents pays, journaux et autres médias, informations issues d’autres organisations qui opèrent à destination, etc.);
* Collecter de l’information auprès des parties prenantes (partenaires locaux et nationaux, autorités locales, gouvernement, etc.);
* Tenir compte de la tolérance au risque de l’organisation, des politiques et des procédures en place au sein de l’organisation, tant au siège social qu’à destination;
* Inclure une visite des lieux de séjour.

## Les étapes pour réaliser une évaluation des risques

1. Identifier les risques
2. Analyser et évaluer les risques identifiés
3. Tenir compte des vulnarbilités

## Conseils pour réaliser une robuste gestion des risques d’un séjour

* Accorder de la valeur à l’information divulguée lors d’échanges informels;
* Discuter dans un climat de confiance qui favorise la libre-expression des personnes ressources;
* Lors de la visite terrain, relever la présence de l’équipement de sécurité (détecteurs de fumée, plan d’évacuation, trousse de premiers soins, véhicule en bon ordre, etc.) et de leur état;
* Discerner les faits des rumeurs. Considérer tout de même ces rumeurs car celles-ci pourraient contenir de l’information s’avérant vraie et utile.

# Identifier les risques

Pour identifier les risques vous devez :

* 1. Comprendre le contexte de la sécurité de la destination;
	2. Identifier les activités poursuivies et leurs caractéristiques;
	3. Tenir compte des vulnérabilités.

## Comprendre le contexte de sécurité de la destination

Pour identifier les menaces présentes en raison du contexte dans lequel le séjour se déroule, il faut en établir le contexte en déterminant et documentant les divers aspects qui composent la destination qui peuvent exercer une influence sur la santé et la sécurité des individus pendant le séjour.

En ayant recours à diverses sources d’information :

* Repérer et documenter avec rigueur les avertissements, avis, annonces et conseils pour le pays et les régions visitées;
* Dresser un portrait sommaire du pays en tenant compte du contexte historique afin d’acquérir une compréhension de la situation politique, économique, sanitaire, de la culture, des infrastructures, etc.;
* Traiter des aspects suivants :
* Le **contexte civil** **et culturel** du pays et sa stabilité : la situation politique, les conflits ethniques, la situation socioéconomique, la religion, la communauté LGBTQ2+, les conditions liées à l’identité de genre, etc.,
* Les **autorités et forces locales :** la corruption systémique, les liens avec des groupes criminalisés ou terroristes, le manque de sécurité exacerbé par l’incompétence et la nonchalance des forces de l’ordre, l’extorsion, le « taxage » ou le paiement d’un droit de passage, etc.,
* La **criminalité**: les groupes criminalisés présents, les types de crimes les plus courants (fraude, harcèlement, fausse monnaie, agression sexuelle, etc.), les principales régions ou lieux associés aux crimes, les personnes visées par les crimes, etc.,
* L’historique des **évènements terroristes**, la présence de groupes terroristes, le niveau de menace dans le pays ou la région,
* **Infrastructures** : conditions routières, risques routiers importants, adéquation des autoroutes et ponts, qualité et sécurité des routes, chemins de fer et voies navigables, état des aéroports et gares maritimes, état des réseaux énergétiques et fréquence des pannes, couverture des réseaux cellulaires et internet, éclairage de nuit, etc.,
* Les conditions **sanitaires et des soins de santé** telles que la qualité générale et l’accessibilité, l’historique des maladies pandémiques et épidémiques, etc.,
* Caractéristiques **géographiques** (topographie, hydrographie, déforestation, climatologie, etc.) : l’historique et la probabilité d’occurrence de catastrophes naturelles (tremblement de terre, raz-de-marée, feux, ouragans, éboulements, glissements de terrain, inondations, séisme, pluies importantes, etc.), et la présence de champs de mines ou de munitions non explosées, etc.

## Identifier les activités poursuivies et leurs caractéristiques

Pour identifier les menaces liées aux activités poursuivies, l’organisation doit se questionner sur ses activités et leurs caractéristiques. En effet, dans une même destination, une personne qui participe à une conférence dans un grand centre urbain pourrait faire face à moins de risques qu’une personne qui prend part à une randonnée en région éloignée.

Considérer les aspects suivants:

* Les **déplacements**: l’horaire des déplacements, les routes empruntées et leur état, le moyen de transport utilisé, la saison et les impacts sur les infrastructures empruntées, la faune présente sur les routes, le paiement de droit de passage (taxage), les braquages, etc.;
* Les **hébergements** : la sécurité du quartier et des bâtiments, les systèmes de verrouillage, la présence de gardiens, les mesures en place en cas d’incendie, l’éclairage des lieux, la capacité de la structure à résister aux catastrophes naturelles, la proximité de sites qui entreposent des matières dangereuses, la possibilité d’une fuite de gaz, les pannes électriques prolongées, la présence de sorties de secours, etc.;
* Les **régions visitées** : le contexte socioculturel, les niveaux de risque identifiés par les sites gouvernementaux (AMC par exemple), la faune et la flore, l’environnement géographique, etc.;
* L’**accessibilité aux infrastructures de santé** : la distance à parcourir pour avoir accès à des professionnels de la santé, la qualité des soins et des infrastructures, la disponibilité des services paramédicaux et du transport d’urgence, etc.;
* L’**alimentation et la restauration** : la qualité de l’eau, la disponibilité des aliments et leur qualité, la salubrité des établissements, la sécurité des lieux, l’accès sécuritaire aux toilettes dans les restaurants, etc.;
* **Communications** : la fiabilité du réseau cellulaire, l’accès à l’internet.

## Tenir compte des vulnérabilités

Pour identifier les menaces liées aux vulnérabilités, l’organisation tient compte des vulnérabilités des personnes qui prennent part au séjour (genre, ethnie, religion, casier judiciaire, conditions préexistantes, capacité physique et psychologique d’accomplir une tâche ou de poursuivre l’activité, etc.) et des vulnérabilités de l’organisation.

Dans certains contextes, la divulgation de ces informations pourrait ne pas être obligatoire au sens de la loi de la province, de l’état ou du pays d’attache de l’organisation. La bonne pratique serait alors d’accompagner les voyageuses et voyageurs dans une réflexion et une prise de conscience de leurs vulnérabilités et de les habiliter à identifier les risques qui en résultent. Les personnes qui voyagent traitent ensuite les risques en identifiant des comportements à adopter pour préserver leur santé et leur sécurité.

# Analyser lEs RISQUEs identifiés

Pour chacune des menaces qui s’avère être un risque, évaluer son niveau. Il faut identifier la probabilité que le risque se concrétise et l’impact qui en découlera. Il est donc important d’analyser les faits et les données disponibles pour réaliser une évaluation juste et objective.

# Traiter les risques

## 3.1 Évaluer les niveaux de risques établis

Catégoriser le risque : Faible, Modéré, Élevé ou Très élevé.

## 3.1.1 Déterminer la stratégie de gestion des risques à appliquer

Se référer à la stratégie de gestion des risques de votre organisation.

Pour chacun des risques évalués, indiquer la stratégie à appliquer (accepter, atténuer, rejeter ou transférer[[1]](#footnote-2)) par l’organisation.

## Identifier les mesures et les implanter

Dans le but d’opérationnaliser la stratégie de gestion identifiée, identifier les mesures à mettre en place. Le choix des mesures dépend de plusieurs variables telles que les ressources humaines et financières disponibles, la capacité du ou des partenaires, le profil des personnes qui voyagent, les vulnérabilités de l’organisation, l’analyse du coût versus le bénéfice, etc.

## Exemples de traitement des risques

1. **Risque : Se faire happer par une moto à Homme Chi Minh, Vietnam (accident de transport)**

**Niveau de risque** : Élevé (3 x 3 = 9)

**Stratégie** : Atténuation et transfert

**Mesures à mettre en place** :

Formation aux voyageuses et voyageurs sur les codes de conduite culturels (vulnérabilité).

Consigne de traverser seulement aux feux de circulation (vulnérabilité).

Formation sécurité à l’arrivée « Comment traverser la rue au Vietnam » (vulnérabilité).

Les taxis ou autobus débarquent toujours les voyageuses et voyageurs du bon côté de la rue (probabilité).

Les voyageuses et voyageurs sont couverts par une police d’assurance pour hospitalisation (impact).

1. **Risque de séisme à Port-au-Prince, Haïti (catastrophe naturelle)**

**Niveau de risque** : Élevé (3 x 4 = 12)

**Stratégie** : Atténuation et transfert (aux assurances)

**Mesures à mettre en place** :

Sélectionner des hébergements aux infrastructures résistantes aux séismes (vulnérabilité).

Prioriser les bâtiments d’un étage (vulnérabilité).

Formation aux voyageuses et voyageurs sur les comportements préventifs et réactifs en cas de séisme (vulnérabilité et impact).

Les voyageuses et voyageurs sont couverts par une police d’assurance pour rapatriement (impact).

## Évaluer les capacités de l’organisation partenaire

L’organisation qui transfert la gestion d’un risque à un partenaire et délègue la responsabilité d’implanter certaines mesures doit évaluer si ce dernier a la capacité d’assumer son rôle et ses responsabilités.

## Déterminer le niveau résiduel des risques (onglet 5. Évaluation et traitement)

Identifier la nouvelle valeur (entre 1 et 4) obtenue à la suite de l’implantation des mesures pour obtenir le niveau de risque résiduel.

Pour les risques dont le niveau résiduel est toujours au-delà de la tolérance de l’organisation, identifier des mesures additionnelles à mettre en place et ce, jusqu’à l’obtention d’un niveau de risque résiduel acceptable (si possible). Il est important de mentionner que le risque zéro n’existe pas.

# PRendre la décision finale

Le processus de gestion des risques permet de prendre des décisions de façon éclairée. Par exemple, l’organisation peut choisir de développer un projet dans une nouvelle destination, d’approuver un séjour ou autoriser la tenue d’une activité spécifique.

# définitions et concepts

## Qu’est-ce qu’un risque ?

**Risque = Menace X Vulnérabilité**

### Qu’est-ce qu’une menace?

Signe par lequel on indique à autrui l’intention que l’on a de faire du mal ou de nuire ou par lequel se manifeste l’imminence d’un danger.

### Qu’est-ce que la vulnérabilité ?

C’est la propension d’une personne physique ou morale (l’organisation), à subir les effets d’une menace.

#### Les vulnérabilités d’une personne physique

Il s’agit de l’identité de genre, de l’âge, de l’orientation sexuelle, de la religion (signes ostentatoires), de l’origine ethnique des individus (couleur de la peau), de leur condition physique, de leur santé mentale. Il s’agit aussi de considérer l’expérience, la formation, les ressources financières disponibles, etc.

#### Les vulnérabilités organisationnelles

Les organisations, de manière générale, peuvent avoir des vulnérabilités dans les catégories suivantes :

* Gouvernance et stratégie;
* Finances;
* Communications et réputation;
* Cadre légal;
* Opérations et ressources humaines.

L’[annexe A](#_annexe_a_–) présente un plus large éventail des vulnérabilités d’une organisation.

### Exemples de risques:

1. Menace : Les motos qui sont très nombreuses et se faufilent partout (Ho Chin Min, Vietnam)

Vulnérabilité : L’incompréhension des codes de conduites culturels et l’inexpérience de la voyageuse ou du voyageur

**Risque : Se faire happer par une moto**

1. Menace : Séisme (Port-au-Prince, Haïti)

Vulnérabilité : Faiblesse des infrastructures (lieu d’hébergement, routes, lieu de travail, etc.)

**Risque : Être victime d’un séisme**

## Qu’est-ce que le niveau d’un risque ?

**Niveau de risque = Probabilité d’occurrence X Impact**

### La probabilité d’occurrence

La probabilité indique dans quelle mesure le risque est susceptible de survenir d’après les conditions de la destination, les activités poursuivies et les vulnérabilités identifiées.



### L’impact

L’impact (ou la gravité) indique le degré de conséquences négatives potentielles. Les critères de mesure sont : mineur, modéré, élevé et critique.



### Calculer le niveau de risque

Le niveau d’un risque est établi en multipliant les cotes (1 à 4) associées à la probabilité et à l’impact.

Exemples de calculs de niveaux de risque :

1. **Risque : Se faire happer par une moto à Ho Chi Minh, Vietnam**

Menace : Les motos qui sont très nombreuses et se faufilent partout.

Vulnérabilité : L’incompréhension des codes de conduites culturels et l’inexpérience de la voyageuse ou du voyageur.

Probabilité : Il est probable qu’un de nos voyageurs se fasse happer (2).

Impact : Si notre voyageur se fait happer, les impacts physiques et financiers sont élevés (3).

**Niveau de risque : Modéré** (2 x 3 = 6).

1. **Risque : Être victime d’un séisme à Port-au-Prince, Haïti**

Menace : Séisme

Vulnérabilité : Faiblesse des infrastructures (lieu d’hébergement, routes, lieu de travail, etc.).

Probabilité : Port-au-Prince est considérée zone sismique active et un séisme est probable (3).

Impact : Si notre voyageur vit un séisme, les impacts physiques, psychologiques et financiers sont critiques aux vues de la sévérité possible des blessures (4).

**Niveau de risque : Élevé** (3 x 4 = 12)

# annexe a – exemples[[2]](#footnote-3) de vulnérabilités organisationnelles

* **Processus opérationnels :** Menaces associées à la conception ou à la mise en œuvre des processus opérationnels.
* **Immobilisations :** Menaces associées aux immobilisations d'une organisation, y compris les biens durables (p. ex., immeubles, navires, matériel scientifique, parc), mais excluant l'infrastructure de la technologie de l’information.
* **Communications :** Menaces associées à l'approche et à la culture d'une organisation en matière de communication, de consultation, de transparence et de mise en commun des renseignements, tant à l'interne qu'à l'externe.
* **Conflit d'intérêts :** Menaces associées aux conflits perçus ou potentiels (intérêts privés et l'intérêt public).
* **Gestion financière :** Menaces associées aux structures et aux processus destinés à assurer une saine gestion des ressources financières de l’organisation et sa conformité aux politiques et normes en matière de gestion financière.
* **Financement :** Menaces associées à l’engagement des divers bailleurs de fonds et parties prenantes en matière de financement des opérations et de la programmation de l’organisation.
* **Gouvernance et orientation stratégique :** Menaces associées aux façons de faire en matière de leadership, de prise de décisions et de capacité de gestion.
* **Gestion des ressources humaines :** Menaces associées au roulement de personnel, à la culture organisationnelle, au recrutement, à la rétention du personnel, aux processus et pratiques de dotation, à la planification de la relève, à la gestion des talents et au renforcement des capacités des employés.
* **Gestion de l'information :** Menaces associées à la capacité et à la viabilité relativement aux procédures et aux pratiques de gestion de l'information.
* **Technologie de l'information :** Menaces associées à la capacité et à la viabilité en matière de technologie de l'information, dont l'infrastructure et l'utilisation des applications technologiques.
* **Gestion du savoir :** Menaces associées à la consignation et à la gestion du savoir, notamment en ce qui a trait à la propriété intellectuelle, à l'information, aux dossiers organisationnels et opérationnels ainsi qu’aux données scientifiques.
* **Légalité :** Menaces associées à la gestion des activités se rapportant à la législation, aux avis et aux litiges, y compris l'élaboration et le renouvellement des lois, règlements, politiques, traités et accords internationaux selon les normes juridiques établies.
* **Transformation organisationnelle et gestion du changement :** Menaces associées à un changement important de la structure ou du comportement d'une organisation se rapportant à son mandat, à son contexte opérationnel, à son leadership ou à son orientation stratégique.
* **Élaboration et mise en œuvre des politiques :** Menaces associées à l'élaboration, à la mise en œuvre et au respect des politiques gouvernementales et des politiques et procédures internes.
* **Confidentialité :** Menaces associées à la protection des renseignements personnels.
* **Conception et exécution des programmes :** Menaces associées à la conception et à l'exécution de programmes particuliers susceptibles d'avoir des répercussions sur les objectifs généraux de l'organisation.
* **Gestion de projet :** Menaces associées aux processus et aux pratiques de préparation et de gestion de grands projets, à l'appui du mandat général de l'organisation ainsi qu'à des risques liés à des projets particuliers susceptibles de nécessiter une gestion à long terme.
* **Situation politique :** Menaces associées à la situation politique et au contexte de fonctionnement de l'organisation.
* **Réputation :** Menaces associées à la réputation et à la crédibilité d'une organisation auprès de ses partenaires, des intéressés et de la population.
* **Santé et sécurité au travail :** Menaces associées à la sécurité de l’environnement de travail dans lequel évolue les employés de l’organisation ainsi qu’à la santé des employés.
* **Gestion des ressources :** Menaces associées à la disponibilité des ressources permettant à une organisation de réaliser son mandat ainsi que la capacité de l’organisation à gérer ces ressources.
* **Parties intéressées et partenariats :** Menaces associées au profil démographique, aux caractéristiques et aux activités des partenaires et des parties intéressées d'une organisation.
* **Valeurs et éthique :** Menaces associées à la culture d'une organisation et à sa capacité de respecter l'esprit et l'intention de son code de valeurs et d'éthique.

L’organisation pourrait identifier d’autres menaces spécifiques à sa culture organisationnelle.

1. Une organisation qui transfère un risque à une partie prenante doit évaluer si ce partenaire a la capacité de satisfaire à son rôle et ses responsabilités (voir Annexe B) en lien avec la gestion de ce risque. [↑](#footnote-ref-2)
2. Inspirés du site web, Guide sur la taxonomie des risques, <https://www.canada.ca/fr/secretariat-conseil-tresor/organisation/gestion-risque/taxonomies.html>, (11 mai, 2020). [↑](#footnote-ref-3)