TRAVEL RISK MANAGEMENT
METHODOLOGICAL GUIDE

The risk assessment process is performed at the beginning of the development of a travel. It is used to evaluate and approve any new travel or renewal. If the travel is planned over several months and the safety environment changes during that time, it is necessary to redo the process - in part or in full.

To ensure optimal outcomes, the travel risk assessment should:

- Be conducted by a qualified individual who has the time and resources to do so.
- Integrate data from several sources (Global Affairs Canada, accident and near miss reports, government websites from different countries, newspapers and other media, information from other organizations operating at destination, etc.). Tab 1 of document APPENDIX A – Risk_Management_Support provides some examples.
- Collect information from stakeholders (local and national partners, local authorities, government, etc.).
- Consider the organization's risk tolerance, policies, and procedures in place within the organization, both at headquarters and at destination.
- Include a visit to the place of travel.

Steps to Carry a Travel Risk Assessment

1. Identify the risks related to the travel
2. Analyze the level of the identified risks
3. Treat the risks

Tips for Achieving Robust Travel Risk Management

- Value the information disclosed in informal exchanges.
- Discuss in a climate of trust that encourages the free expression of resource persons.
- During the site visit, note the presence of safety equipment (smoke detectors, evacuation plan, first aid kit, vehicle in good order, etc.) and their condition.
- Discern facts from rumors. Consider these rumors because they may contain information that is true and useful.

1. IDENTIFY THE RISKS RELATED TO THE TRAVEL

To identify risks, you must:

1.1 Understand the safety, and security context of destination

1.2 Identify the activities pursued and their characteristics

1.3 Consider vulnerabilities

1.1 Understand the Safety, Security and Sanitary Context of the Destination

To identify the threats that are present due to the context in which the travel takes place, the context must be established by identifying and documenting the various aspects that make up the destination that may influence the health, safety, and security of individuals during the travel.

By using various sources of information:

- Locate and thoroughly document warnings, advisories, announcements and tips for the country and regions visited.
- Draw a brief portrait of the country, considering the historical context, to gain an understanding of the political, economic, health, cultural, and infrastructural situation, etc.
- Address the following:
  - The **civil and cultural context of** the country and its stability: the political situation, ethnic conflicts, socioeconomic situation, religion, LGBTQ2+ community, gender identity conditions, etc.
  - **Local authorities and forces:** systemic corruption, links to criminal or terrorist groups, lack of security exacerbated by incompetent and nonchalant law enforcement, extortion, "taxing" or paying a right to pass, etc.
  - **Crime**: the crime groups present, the most common types of crime (fraud, harassment, counterfeit money, sexual assault, etc.), the main areas or locations associated with crime, the people targeted by crime, etc.
  - The history of **terrorist events**, the presence of terrorist groups, the level of threat in the country or region,
  - **Infrastructure**: road conditions, major road hazards, adequacy of highways and bridges, quality and safety of roads, railroads and waterways, condition of airports and ferry terminals, condition of energy networks and frequency of outages, cellular and internet coverage, night lighting, etc.
  - **Health and health care** conditions such as overall quality and accessibility, history of pandemic and epidemic diseases, etc.
  - **Geographical** characteristics (topography, hydrography, deforestation, climatology, etc.): the history and probability of occurrence of natural disasters (earthquake, tidal wave, fire, hurricane, landslide, flood, earthquake, heavy rain, etc.), and the presence of minefields or unexploded ordnance, etc.

1.2 Identify the Activities Pursued and their Characteristics

To identify the threats related to the activities pursued, the organization must ask itself about its activities and their characteristics. For example, a person attending a conference in a large urban center may face fewer risks in the same destination than a person taking part in a hike in a remote area.

Consider the following:

- **Travel**: travel schedule, roads used and their condition, means of transport used, season and impacts on infrastructure used, wildlife on the roads, payment of right of way (taxing), robberies, etc.
- **Accommodations**: the security of the area and buildings, locking systems, presence of guards, measures in place in case of fire, lighting of the premises, ability of the structure to withstand natural disasters, proximity to sites that store hazardous materials, possibility of a gas leak, prolonged electrical outages, presence of emergency exits, etc.
- The **regions visited**: the socio-cultural context, the risk levels identified by government sites (AMC for example), the fauna and flora, the geographical environment, etc.

- **Accessibility to health infrastructure**: the distance to travel to access health professionals, the quality of care and infrastructure, the availability of paramedical services and emergency transport, etc.
- **Food and catering**: water quality, food availability and quality, sanitation of establishments, safety of premises, safe access to toilets in restaurants, etc.
- **Communications**: reliability of the cellular network, access to the Internet.

1.3 Consider Vulnerabilities

To identify threats related to vulnerabilities, the organization considers the vulnerabilities of the individuals involved in the travel (gender, ethnicity, religion, criminal record, pre-existing conditions, physical and psychological ability to perform a task or continue the activity, etc.) and the vulnerabilities of the organization (see Appendix A).

> In some contexts, disclosure of this information may not be required by the law of the province, state, or country in which the organization is based. Good practice would then be to support travellers in thinking about and becoming aware of their vulnerabilities and empowering them to identify the resulting risks. Travellers then address the risks by identifying behaviors to adopt to preserve their health and safety.

2. ANALYZE THE RISKS IDENTIFIED

For each threat that turns out to be a risk analyze their level. It is necessary to identify the likelihood of the risk occurring and the impact it will have. It is therefore important to analyze the facts and data available to make a fair and objective assessment.

3. TREAT THE RISKS

3.1 Assessing Established Risk Levels

Categorize the risk: Low, Moderate, High, or Very High.

3.1.1 Determine the Risk Management Strategy to be Applied

Refer to your organization's risk management strategy.

For each of the assessed risks, indicate the strategy to be applied (accept, mitigate, reject or transfer[1]) by the organization.

3.2 Identify Measures and Implement Them

To operationalize the identified management strategy, identify the measures to be put in place. The choice of measures depends on several variables such as the human and financial resources available, the capacity

[1] An organization that transfers a risk to a stakeholder must assess whether that partner has the capacity to fulfill its role and responsibilities (see Appendix B) in managing that risk.

of the partner(s), the profile of the people who travel, the vulnerabilities of the organization, the analysis of cost versus benefit, etc.

Examples of Risk Treatment

i. **Risk: Getting hit by a motorcycle in Man Chi Minh, Vietnam (transportation accident)**
Risk level: High (3 x 3 = 9)
Strategy: Mitigation and Transfer
Measures to be implemented:
Training for travellers on cultural codes of conduct (vulnerability).
Instruct to cross only at traffic lights (vulnerability).
Safety training on arrival "How to cross the street in Vietnam" (vulnerability).
Cabs or buses always drop off travellers on the right side of the street (probability).
Travellers are covered by a hospitalization (impact) insurance policy.

ii. **Risk of earthquake in Port-au-Prince, Haiti (natural disaster)**
Risk level: High (3 x 4 = 12)
Strategy: Mitigation and transfer (to insurance)
Measures to be implemented:
Select accommodations with earthquake resistant infrastructure (vulnerability).
Prioritize one-story buildings (vulnerability).
Training for travellers on preventive and reactive behaviors in case of an earthquake (vulnerability and impact).
Travellers are covered by a repatriation (impact) insurance policy.

3.2.1 Assess the Partner's Capabilities

If an organization transfers the management of a risk to a partner and delegates responsibility for implementing certain measures, it must assess whether the partner has the capacity to assume its role and responsibilities.

3.3 Determine the Residual Level of Risk

Identify the new value (between 1 and 4) obtained following the implementation of the measurements.

For risks whose residual level is still beyond the organization's tolerance, identify additional measures to be put in place until an acceptable residual risk level is reached (if possible). It is important to mention that there is no such thing as zero risk.

MAKE THE FINAL DECISION

The risk management process allows for informed decision making. For example, the organization may choose to develop a project in a new destination, approve a travel or authorize a specific activity.

DEFINITIONS AND CONCEPTS

What is a Risk?

Risk = Threat X Vulnerability

What is a threat?

A sign that indicates to another person the intention to harm or injure or that shows the imminence of a danger.

What is vulnerability?

It is the propensity of a physical or moral person (the organization), to suffer the effects of a threat.

Vulnerabilities of an individual

It is about gender identity, age, sexual orientation, religion (conspicuous signs), ethnic origin (skin color), physical condition, mental health. It is also a question of considering experience, training, available financial resources, etc.

Organizational vulnerabilities

Organizations, in general, may have vulnerabilities in the following categories:

- Governance and strategy
- Finance
- Communications and reputation
- Legal framework
- Operations and Human Resources

Appendix A presents a broader range of an organization's vulnerabilities.

Examples of risks:

i. Threat: Motorcycles which are very numerous and sneak everywhere (Ho Chin Min, Vietnam)
Vulnerability: Lack of understanding of cultural codes of conduct and inexperience of the traveller
Risk: Getting hit by a motorcycle

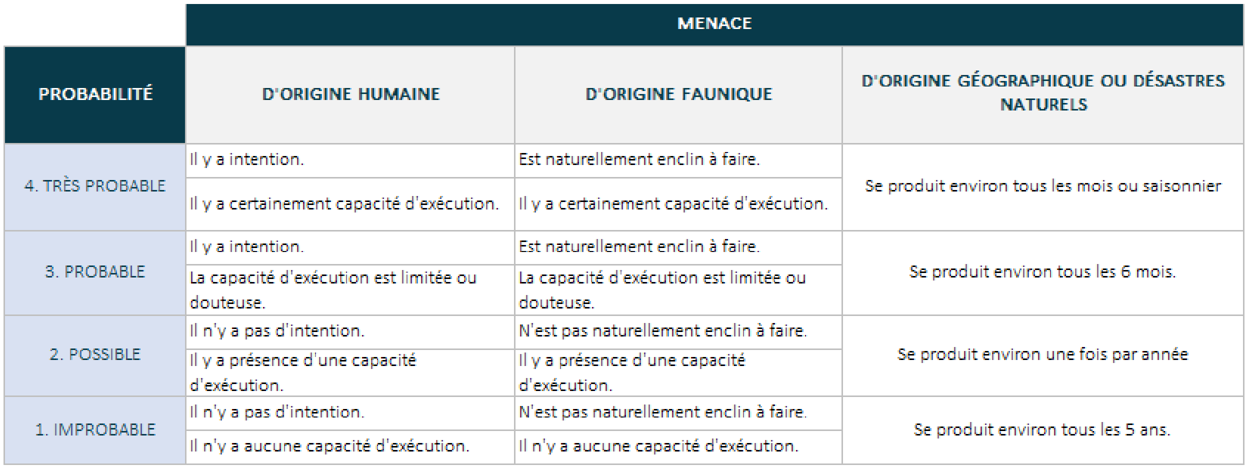
ii. Threat: Earthquake (Port-au-Prince, Haiti)
Vulnerability: Weak infrastructure (housing, roads, workplace, etc.)
Risk: Being a victim of an earthquake

What is the Level of a Risk?

Risk level = Probability of occurrence X Impact

The probability of occurrence

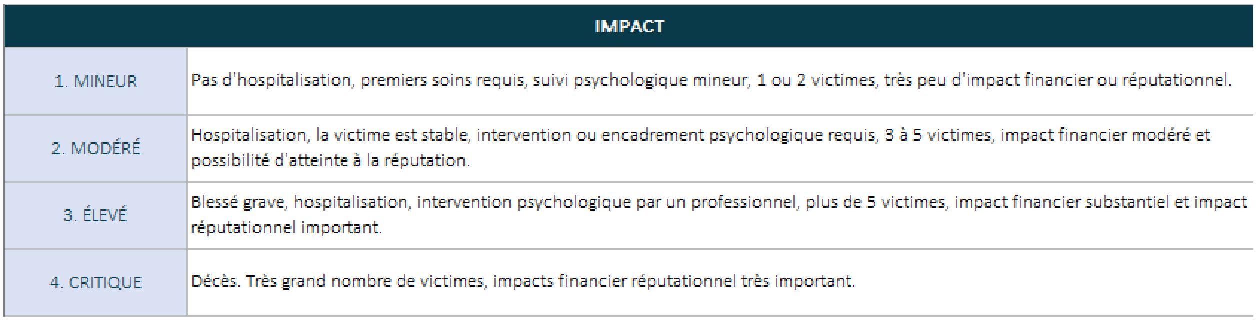
The likelihood indicates the extent to which the risk is likely to occur based on the conditions of the destination, the activities being pursued, and the vulnerabilities identified.



	MENACE		
PROBABILITÉ	D'ORIGINE HUMAINE	D'ORIGINE FAUNIQUE	D'ORIGINE GÉOGRAPHIQUE OU DÉSASTRES NATURELS
4. TRÈS PROBABLE	Il y a intention.	Est naturellement enclin à faire.	Se produit environ tous les mois ou saisonnier
	Il y a certainement capacité d'exécution.	Il y a certainement capacité d'exécution.	
3. PROBABLE	Il y a intention.	Est naturellement enclin à faire.	Se produit environ tous les 6 mois.
	La capacité d'exécution est limitée ou douteuse.	La capacité d'exécution est limitée ou douteuse.	
2. POSSIBLE	Il n'y a pas d'intention.	N'est pas naturellement enclin à faire.	Se produit environ une fois par année
	Il y a présence d'une capacité d'exécution.	Il y a présence d'une capacité d'exécution.	
1. IMPROBABLE	Il n'y a pas d'intention.	N'est pas naturellement enclin à faire.	Se produit environ tous les 5 ans.
	Il n'y a aucune capacité d'exécution.	Il n'y a aucune capacité d'exécution.	

The impact

Impact (or severity) indicates the degree of potential negative consequences. The measurement criteria are: minor, moderate, high, and critical.



IMPACT	
1. MINEUR	Pas d'hospitalisation, premiers soins requis, suivi psychologique mineur, 1 ou 2 victimes, très peu d'impact financier ou réputationnel.
2. MODÉRÉ	Hospitalisation, la victime est stable, intervention ou encadrement psychologique requis, 3 à 5 victimes, impact financier modéré et possibilité d'atteinte à la réputation.
3. ÉLEVÉ	Blessé grave, hospitalisation, intervention psychologique par un professionnel, plus de 5 victimes, impact financier substantiel et impact réputationnel important.
4. CRITIQUE	Décès. Très grand nombre de victimes, impacts financier réputationnel très important.

Calculate the level of risk

The level of a risk is established by multiplying the ratings (1 to 4) associated with the probability and impact.

Examples of risk level calculations:

i. **Risk: Getting hit by a motorcycle in Ho Chi Minh, Vietnam**
Threat: The motorcycles which are very numerous and sneak everywhere.
Vulnerability: Lack of understanding of cultural codes of conduct and inexperience of the traveller.
Probability: It is likely that one of our travellers will get caught (2).
Impact: If our traveller gets caught, the physical and financial impacts are high (3).
Risk level: Moderate (2 x 3 = 6).

ii. **Risk: Being a victim of an earthquake in Port-au-Prince, Haiti**
Threat: Earthquake
Vulnerability: Weak infrastructure (housing, roads, workplace, etc.).
Probability: Port-au-Prince is considered an active seismic zone and an earthquake is likely (3).
Impact: If our traveller experiences an earthquake, the physical, psychological, and financial impacts are critical in view of the possible severity of the injuries (4).
Risk level: High (3 x 4 = 12)

APPENDIX A - EXAMPLES[2] OF ORGANIZATIONAL VULNERABILITIES

- **Business processes:** Threats associated with the design or implementation of business processes.
- **Capital Assets:** Threats associated with an organization's capital assets, including durable assets (e.g., buildings, ships, scientific equipment, fleet), but excluding information technology infrastructure.
- **Communications:** Threats associated with an organization's approach and culture to communication, consultation, transparency, and information sharing, both internally and externally.
- **Conflict of interest:** Threats associated with perceived or potential conflicts (private interests and the public interest).
- **Financial Management:** Threats associated with the structures and processes designed to ensure sound management of the organization's financial resources and compliance with financial management policies and standards.
- **Funding:** Threats associated with the commitment of various donors and stakeholders to funding the organization's operations and programming.
- **Governance and strategic direction:** Threats to leadership, decision-making and management capacity.
- **Human Resource Management:** Threats associated with turnover, organizational culture, recruitment, retention, staffing processes and practices, succession planning, talent management and employee capacity building.
- **Information Management:** Threats to capacity and sustainability related to information management procedures and practices.
- **Information Technology:** Threats associated with information technology capacity and sustainability, including technology infrastructure and application use.
- **Knowledge Management:** Threats associated with the recording and management of knowledge, including intellectual property, information, organizational and operational records, and scientific data.
- **Legality:** Threats associated with the management of activities related to legislation, advice, and litigation, including the development and renewal of laws, regulations, policies, treaties, and international agreements according to established legal standards.
- **Organizational Transformation and Change Management:** Threats associated with a significant change in an organization's structure or behavior related to its mandate, operating environment, leadership, or strategic direction.
- **Policy Development and Implementation:** Threats associated with the development, implementation, and compliance with government policies and internal policies and procedures.
- **Privacy:** Threats to the protection of personal information.

[2] Inspired by the website, Risk Taxonomy Guide, https://www.canada.ca/fr/secretariat-conseil-tresor/organisation/gestion-risque/taxonomies.html, (May 11, 2020).

- **Program Design and Delivery:** Threats associated with the design and delivery of specific programs that may impact the overall goals of the organization.
- **Project Management:** Threats associated with the processes and practices of preparing and managing large projects in support of the organization's overall mandate as well as risks associated with specific projects that may require long-term management.
- **Political situation:** Threats associated with the political situation and the operating environment of the organization.
- **Reputation:** Threats to an organization's reputation and credibility with partners, stakeholders, and the public.
- **Occupational health and safety:** Threats associated with the safety of the work environment in which the organization's employees operate and the health of employees.
- **Resource Management:** Threats associated with the availability of resources to enable an organization to achieve its mandate and the ability of the organization to manage those resources.
- **Stakeholders and Partnerships:** Threats associated with the demographics, characteristics and activities of an organization's partners and stakeholders.
- **Values and Ethics:** Threats associated with an organization's culture and its ability to uphold the spirit and intent of its values and ethics code.

The organization may identify other threats specific to its organizational culture.