Security Risk Management Toolkit: Assessments

READY to go
Mobile Guide

Learn how to develop contingency plans to respond to significant changes in the security threat context and take appropriate actions for the hibernation, relocation, and evacuation of employees.

Actor Mapping and Context Analysis

Note to Learners

The information in this guide is for educational purposes only; it is not intended to be a substitute for professional or specialist security advice. Any reliance you place on such information is therefore at your own risk and the European Interagency Security Forum (EISF) will have no responsibility or liability under any circumstances.

Why is Actor Mapping and Context Analysis Critical?

Mapping the different actors in the operating environment and analyzing the context are both key activities for organizations that are:

- Moving into a new country/area/region
- Starting a new program or project
- Facing a major disruption to the status quo in a familiar operational context

In recent years, NGOs have been ordered out of countries or their staff sentenced or imprisoned, despite the state's urgent humanitarian needs, because someone made a simple social mistake, offended a host government, or started work without properly gaining acceptance by both formal and informal leadership structures. To avoid this from happening, it is critical to start an actor mapping and context analysis as early as possible and continue the process throughout your program's duration.

Who?

Who are the key individuals, groups, organizations, state institutions and other stakeholders that can affect your security and operations?

What?

What is their political and/or social position, power, background, and relation to or interest in the organization?

The Actor Mapping Process

Actor mapping is an exercise to identify all the key individuals, stakeholders, or other organizations that will have an effect on your organization's programs and the operating environment.

Examples of Actors

- Host government ministers, department heads or similar actors
- Opposition figures, groups, or key supporters
- Host government security officials (military, police, other)
- Donors
- UN agencies and their contact points
- Community leaders
- Formal and informal leaders in the operating region
- Other NGOs, both national and international
- Key business individuals who may control local supply and logistics
- Local media
- Beneficiary groups
- Host communities

Key Considerations for Actor Mapping

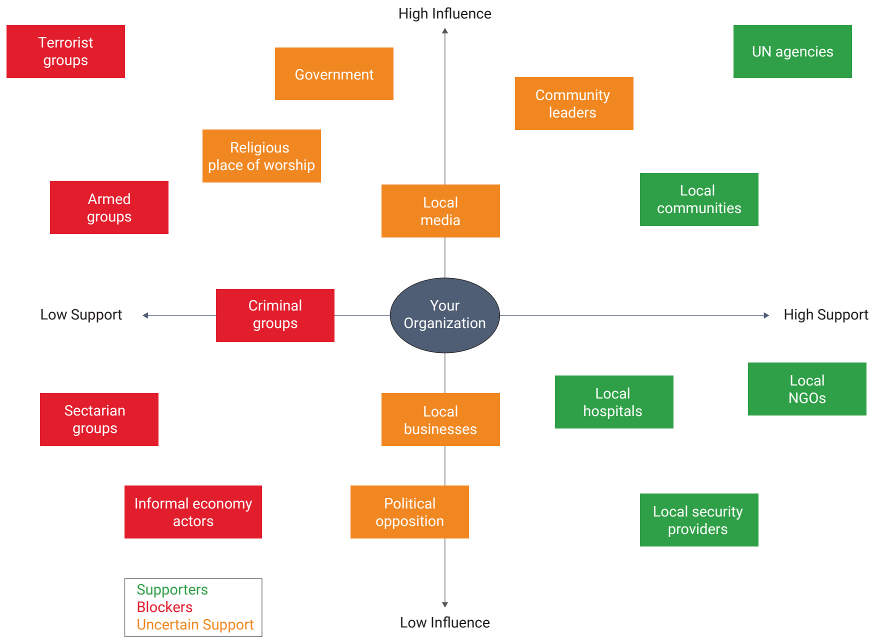
Consider the following during the actor mapping process:

- The declared interests of an individual or group may be very different from their actual interests.
- Once the key actors are identified, it is important to understand how they link together and where interacting with one may influence relations with another.
- Determine how key actors are connected; which actors are allied, and which are in conflict.
- Examine how relationships may be affected by the presence of your organization and any programs to be implemented.

Developing an Actor Map

Once key stakeholders have been identified, it is important to identify the power dynamics and roles of each actor in relation to your organization and its programs. Creating an actor map helps to clarify your relationships with the multiple stakeholders that share your operational space and to determine how they can positively or negatively impact your organization and programs. Use color coding in your map to visualize potential threats, sources of support, and uncertain relationships. As contexts are complex and rapidly evolve, it is important to regularly review your actor map and include different perspectives into the analysis.

Here is an example of an actor map. Keep in mind that this example is not comprehensive, and you may need to include different actors that apply to your context.



Informal economy actors

- Market traders
- Local barons
- Informal transport workers (rickshaws)

Local organizations

- Organization A – development
- Organization B – peacebuilding

Local hospitals

- Senior leadership
- Emergency contacts

Criminal groups

- Drug trafficker
- Human trafficker

Government

- Parliament
- Ministers of health
- Coalitions

UN agencies

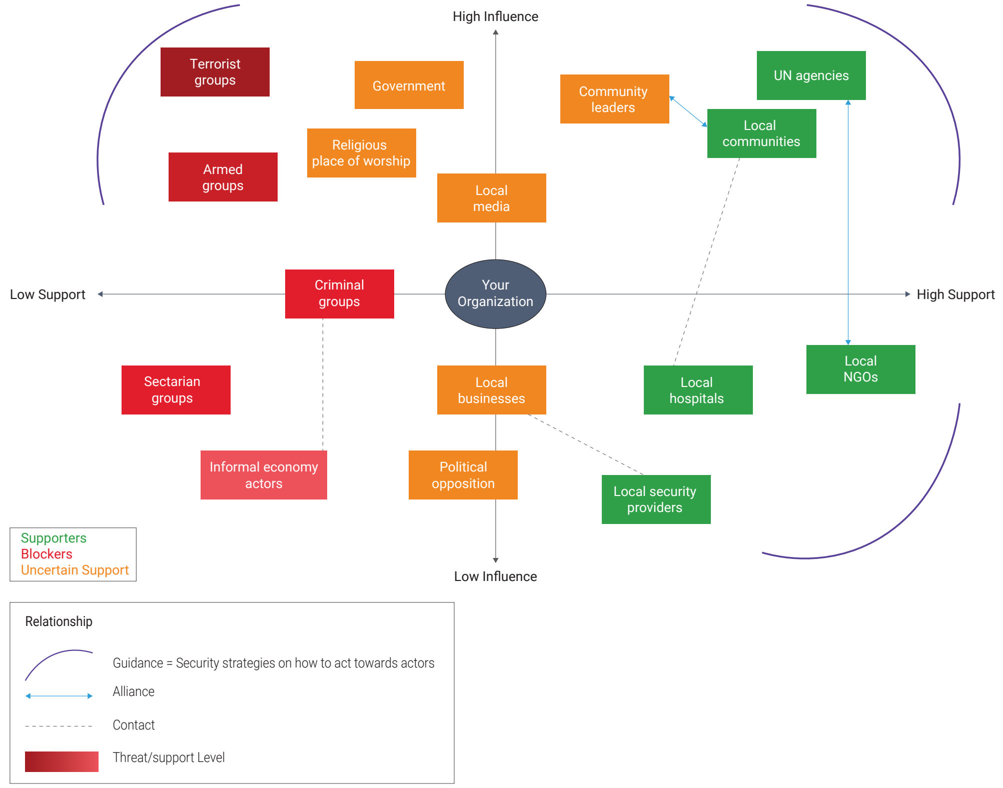
- United Nations Department of Safety and Security (UNDSS)
- United Nations Development Programme (UNDP)
- United Nations High Commissioner for Refugees (UNHCR)

Local communities

- Women and girls
- Older people
- Ethnic groups

Adapting an Actor Map

Actor mapping should be adapted to your organization and its operational context, as well as be adapted to your needs for information and layout preferences. Actor maps can vary at different levels and be enriched by incorporating additional strategic information. However, be careful not to overcomplicate your map too much – actor mapping is supposed to help you visualize a complex setting in a clearer, simpler way and cannot capture every single nuance. Consider this example when developing your actor map.



- Monitor closely
- Determine additional guidance

- Explore partnership
- Maintain good relationships

Initiate/maintain contact

Context Analysis

Once the actor mapping exercise is complete, you will then need to analyze the context by examining the interrelation and impact of multiple factors. This may include:

- History (both recent and distant)
- Cultural and religious traditions that may differ between urban and rural areas
- Racial, tribal, or political alliances
- Socio-economic factors
- Infrastructure conditions
- Level of security or insecurity and contributing factors
- Attitudes towards foreigners (western, diaspora, or regional)
- Attitudes towards aid organizations
- Governance issues
- Corruption
- Impact of arriving NGOs, other than programming, on local social, economic, and power relationships
- Other factors

Writing a Context Analysis

When writing a context analysis, you can use the **PESTLE** method as a tool to remember what factors determine the general environment. During your analysis, try to identify as many actors, dynamics, and factors as possible in each category and consider the potential impact they have on your organization and programs.

P	E	S	T	L	E
Political	Economic	Social	Technological	Legal	Environmental

P

Political

Politics

- Government stability
- Corruption levels
- Censorship
- Political factions and coalitions
- Civil unrest, demonstrations
- Regional and international relationships

E

Economic

Economics

- Economic growth
- Inflation rate and access to basic goods
- Trade restrictions
- Unemployment rate
- Levels of poverty

S

Social

Social

- Population growth
- Age distribution
- Health consciousness
- Cultural behaviors and traditions
- Ethnic, religious composition

T

Technological

Technological

- Levels of innovation and automation
- Internet access and social media culture
- Technological change
- Cybersecurity environment

L

Legal

Legal

- Anti-discrimination laws (ethnicity, gender, religion)
- Employment laws
- Property and access laws
- Health and safety laws

E

Environmental

Environmental

- Weather and climate
- Environmental policies
- Natural hazards
- State of essential resources (water, crops)

Tips for Effective Actor Mapping and Context Analysis

Actor mapping and context analysis may be challenging when responding quickly to a new environment. Identifying all the actors and stakeholders can be difficult enough, without trying to establish power relationships or behind the scenes motivations. Follow these tips throughout the actor mapping and context analysis process.

Find good sources of local knowledge, while being aware of bias.

Research other organizations or individuals who have recently worked in the context and interview them.

Include as many perspectives as possible into the actor mapping and context analysis.

Recognize how different ethnicities, ages, and genders can have a distinct understanding of drivers and relationships of the context.

Update information regularly in the actor mapping and context analysis process (as it becomes known) in the early stages of a new response.

Maintain confidentiality of all outputs in this process to avoid upsetting local sensibilities.

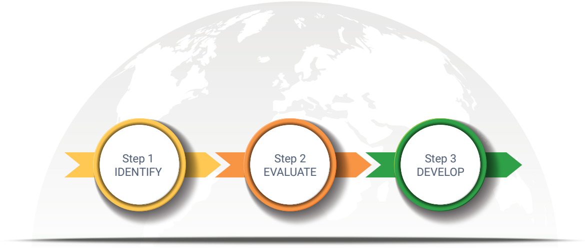
Monitor and carefully manage how the information is employed and shared to avoid being seen as gathering ‘intelligence’ of others.

Security Risk Assessments

Conducting a Basic Security Risk Assessment

All organizations must understand their ‘threshold’ for acceptable risk for their organization and staff. Some organizations are experienced and have the capacity to work in moderate to high-risk environments while others may only have the capacity to work in low to moderate risk areas. It is important to know your organization’s ability to manage risk when determining the threshold for responding to a humanitarian emergency. The threshold for acceptable risk also depends on the type of program, for instance, whether it is critical for lifesaving, for advocacy against existing power structures, or for long-term development.

Follow these three steps to conduct a basic security risk assessment as part of any wider assessment process.



Step 1: IDENTIFY
Identify the threats.

Step 2: EVALUATE
Evaluate the threats and rate your organization’s risk level (vulnerability).

Step 3: DEVELOP
Develop strategies to reduce risk and vulnerability.

Step 1: Identify Threats

Identifying Security Risks and Threats

Conducting security risk assessments is an integral part of designing and implementing sustainable programs. A critical step when starting a new program is to develop a clear understanding of the operational environment (through completing an actor mapping and context analysis) and to identify threats and risks that your organization may face. A comprehensive security risk assessment is essential to develop appropriate mitigation measures, that will enable the safe and sustainable delivery of program objectives.

Threat

Threats are potential sources of harm that could negatively impact your staff, program, organization, assets, or reputation.

What threats exist in the context where you operate that could affect/endanger your staff, assets, organization, reputation, or programming?

Examples of security threats:

- **Physical threats:** crime, terrorism, kidnapping, gender-based violence
- **Organizational threats:** legal challenges, corruption, blackmailing
- **Environmental threats:** natural disasters, health and medical problems, stress

Risk

Risks can be defined as the effects of uncertainty on achieving your objectives. It is often quantified as the probability of facing a threat and its likely impact on your staff, program, organization, assets, or reputation.

How could risks affect your staff, assets, organization, reputation, or programming?

Examples of security risks:

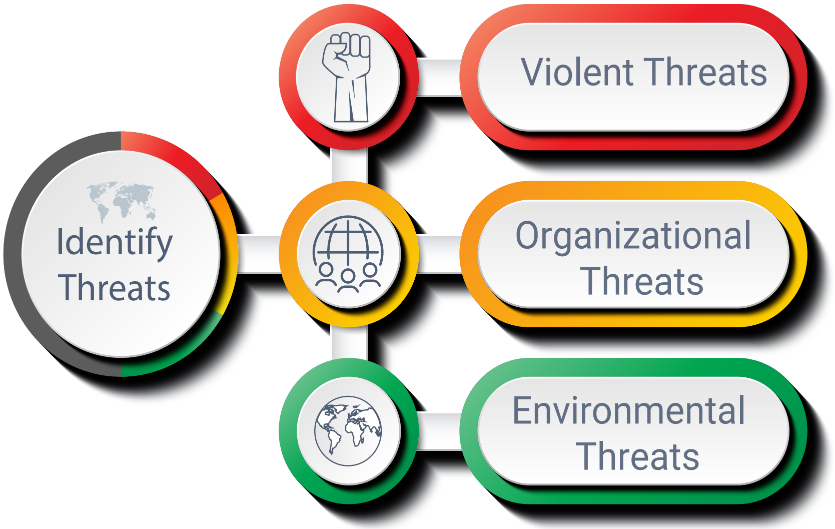
- Program suspension
- Destruction of assets
- Staff injuries or deaths
- Reputational damage
- Office closure
- Rejection by local communities
- Financial risk (theft, corruption, money laundering)
- Loss of projects

Step 1: Identify Threats

There are a wide variety of threats and risks that affect international and national organizations entering a new context.

Many of the different methods used to identify threats, such as actor mapping and context analysis, can require a significant amount of research and time in the region and may not be practical in situations of emergency assessment.

Organizations undertaking an emergency response program should conduct a more detailed risk assessment within the first 10-15 days of deployment and incorporate the results into their overall program strategy. Organizations undertaking any type of program should complete at least a preliminary analysis as part of all the initial assessments for project design and implementation, and then enhance the analysis as more information becomes available over time.



Violent Threats

- Targeted armed attack
- Non-targeted armed conflict
- Kidnapping
- Terrorism
- Explosive violence (landmines, improvised explosive device (IEDs), bombing)
- Carjacking
- Sexual violence
- Civil unrest
- Religious violence
- Crime
- Other types of violence

Organizational Threats

- Reputation risk
- Financial risk (banking system, currency exchange, theft, misappropriation)
- Corruption
- Legal risk (work permits, compliance with domestic legislation, resistance to advocacy)
- Political risk
- Workplace violence or discrimination
- Cultural challenges

Environmental Threats

- Natural hazards (weather, earthquakes, flooding)
- Medical risks (access to suitable medical treatment for staff)
- Health-related issues (food, water, disease, stress)
- Traffic and roadside accidents
- Other accidents
- Fire

Step 2: Evaluating Threats

Step 2: Evaluate the Threats

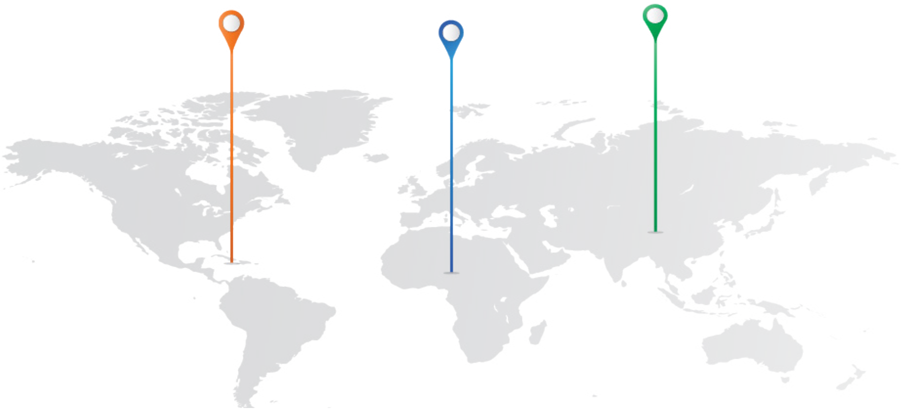
Once you have identified the types of threats your organization will face, you will need to evaluate each threat and rate the level of risk to the staff, the overall organization, and its operations. This will help clarify how severe the risk is and how much priority it must be given.

Threat	Location	Who/what will be at risk?	What will the impact be?
List the threats identified in Step 1 and complete for each of them	Is the threat confined to one or more areas or across the entire affected region? Be specific.	• International staff • National staff • Community members • Marked vehicles • Aid supplies	What could be the gravity of the impact? Consider different scenarios and think about the material as well as immaterial implications (damage to the reputation in the community or with the government).
Example			
Vehicle accidents	Routes to field location (roads, highways)	• Driver and passengers • Users of the road • Marked vehicles	• Loss of assets • Reduction in mobility of teams • Reduction in ability to work • Physical injuries to involved staff, drivers, and users of the road • Loss of life

Rating Risks: Consider How Threats Vary in Different Contexts

Many organizations use a rating system for potential risks ranging from very low, low, medium, high to very high. The risk rating is derived from a combination of the **probability that an incident will occur** and the **gravity of the impact it will cause**.

The first step to rating a risk is to consider how threats may vary in different contexts.



Threats may vary in level geographically. It may be necessary to evaluate the risk by locality rather than nationally or regionally. For instance, a border area may have a higher probability of facing armed conflict while this may be less likely in provinces closer to the capital. Depending on the scale of the emergency situation you may have one overall risk rating for the area or several within the affected zone for each type of risk.

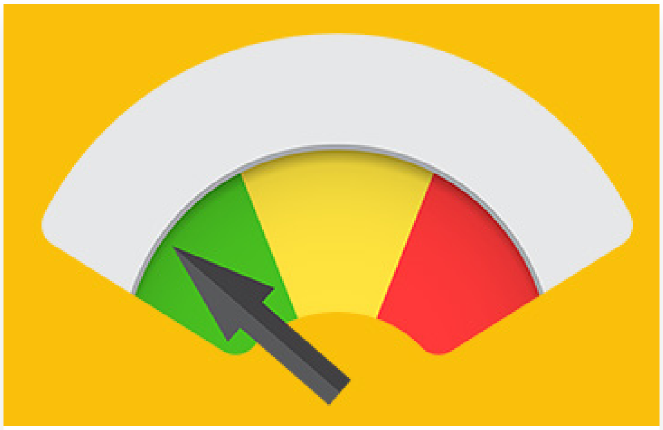
Threats may vary due to different levels of staff vulnerabilities. For example, sometimes national staff may be at less risk in a specific area than international staff. Ethnicity, gender, and experience can also affect the vulnerability of staff.

In a new situation/area where humanitarian response has not recently taken place, use data from similar interventions and current information from local sources to identify potential threats.

Rating Risks: Determine the Risk Rating for Each Threat

The second step to rating a risk is to determine the security risk level for each identified threat. Use this table to rate each threat. Where possible, use previously reported incidents on different threats to justify your rating. The definitions for each security risk level should be agreed across the organization to make it possible to compare different contexts.

Impact	Negligible	Minor	Moderate	Severe	Critical
	• No serious injuries • Minimal loss or damage to assets • No delays to programs	• Minor injuries • Some loss or damage to assets • Some delays to programs	• Non life-threatening injuries • High stress • Loss or damage to assets • Some program delays and disruptions	• Serious injuries • Major destruction of assets • Severe disruption to programs	• Death or Severe injury • Complete destruction or total loss of assets • Loss of programs and projects
Probability					
Very Unlikely Every 4+ years	**Very low**	**Very low**	**Very low**	**Low**	**Low**
Unlikely Every 2-3 years	**Very low**	**Low**	**Low**	**Medium**	**Medium**
Moderately Unlikely Every year	**Very low**	**Low**	**Medium**	**High**	**High**
Likely Once per year	**Low**	**Medium**	**High**	**High**	**Very High**
Very Likely Daily	**Low**	**Medium**	**High**	**Very High**	**Very High**

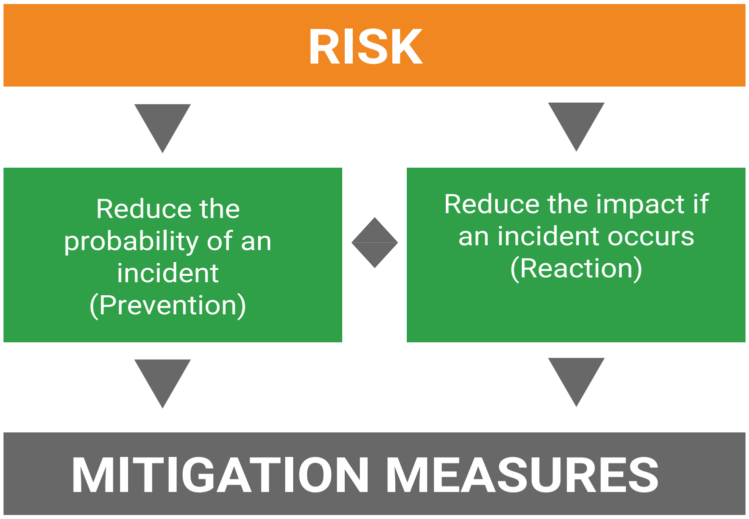


Step 3: Mitigating Risks

Step 3: Develop Strategies to Reduce Risk and Vulnerability

Once the threats that may affect your organization's operations or development programs have been identified and evaluated, and the risks rated, it is important to recommend risk mitigation measures to address these vulnerabilities. The goal of security risk management is not to put up barriers to delivering programs but to enable organizations to stay engaged and implement projects despite the level of risk. While no two situations are identical, actions can be taken to reduce exposure to risk. Developing security strategies is a critical step in ensuring that your organization has taken all reasonable steps to minimize the risk **before** committing staff, resources, and the organization's reputation to a response. This is an essential component of the duty of care.

Mitigation strategies should reflect the organization's preferred risk management strategies such as acceptance, protection, or deterrence. Measures to reduce risk should focus on both **prevention** (reduce the probability) and **reaction** (reduce the impact). By doing this, your organization can reduce the level of residual risk from the level originally assigned to each threat identified and thereby improve its ability to deliver emergency response programs.


RISK
Reduce the probability of an incident (Prevention)
Reduce the impact if an incident occurs (Reaction)
MITIGATION MEASURES

Key Considerations for Mitigating Security Risks

Consider these tips when developing mitigation measures for security risks.

Develop mitigating measures that reflect the risk assessment. For example, if a particular threat is identified as being very unlikely but with a critical impact, implementing measures that only focus on reducing the probability will have a limited effect on reducing the overall risk.

Determine good prevention strategies to reduce threats of office fire, thefts, or vehicle accidents.

Identify threats that are largely unpreventable such as natural disasters, infrastructure failure, or political risk, and focus on reaction measures to reduce their impact on staff and programs.

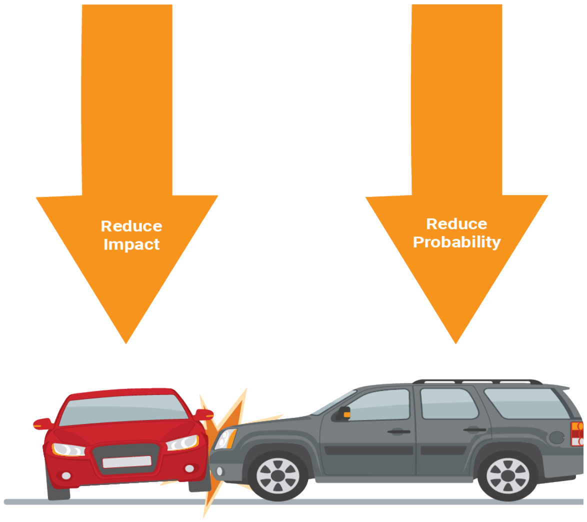
When possible, identify reliable early warning systems that can assist your organization in mitigating the risk.

Set up reaction measures that will improve your organization's preparedness, such as the provision of first aid kits, first aid training, stockpiling emergency supplies, or personal security training.

Identify risks that will transfer to local implementing partners. If your organization chooses to work through local partners as a means of reducing its own exposure to risk, especially in challenging contexts, make sure that you understand resultant risks to local partners and how they might differ from those your organization faced. Just because the partner organization is local, it does not mean that they will not be exposed to risks.

Reducing Exposure to Risk

Here is an example of how you could reduce your exposure to risks for a vehicle accident.



Reduce Probability

- Ensure vehicles are well maintained
- Enforce speed limits
- Provide driver training
- Avoid travel after dark outside towns
- Avoid congested high-risk routes
- Avoid travel in extreme weather

Reduce Impact

- Ensure seatbelts are always worn
- Have first aid kits and train staff
- Have a fire extinguisher
- Keep emergency contact numbers
- Use safety warning triangles at the accident scene
- Have insurance for the vehicle and driver (if needed)
- Have medical insurance and provide counseling (for major accidents) for drivers/passengers