OTHER SOLUTIONS
Building Up Confidence

SECURITY PLAN

BEST PRACTICES

2019

AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT

Warning

The best practices listed in this guide are for information purposes only. These best practices are not sufficient measures to ensure the security of goods and people as part of a contract. **The risk assessment and security measures to be implemented are therefore the sole responsibilities of AFD's partner which should outline them in its security plan.** AFD and OTHER SOLUTIONS Consulting shall not be held responsible for any risk assessment or security measures that may prove insufficient or unsuitable for the risks and events.

Definitions and Clarifications

Security aims at mitigating risks of any intentionally malicious act induced by violence, while safety aims at mitigating risks resulting from non-intentional acts (related to health or natural disasters for instance). Readers should be aware of the fact that this guide is mainly focused on security issues. Safety issues related to natural disasters and health are not specifically addressed, except for when it comes to some specifications on medical evacuations. We strongly encourage readers to design specific measures in order to mitigate the impact of these elements based on their prevalence (annual or seasonal) in the contexts of the missions considered.

Contact

OTHER SOLUTIONS Consulting Ltd.
London office
contact@othersolutions.net
+44 (0)2038456691
Company registered in the UK and in Wales 85 48 765 | VAT 169 5909 53
https://othersolutions.net

TABLE OF CONTENT

INTRODUCTION

WHO IS THIS GUIDE INTENDED FOR?

This guide aims to clarify the consideration of security issues and explains best practices useful to the development of security plans. It is intended for all entities wishing to benefit or benefiting from AFD financing to operate in a particular **orange or red zone**[1]: service providers recruited directly by AFD; civil society organizations (CSO) benefiting from AFD funds; construction companies and consultants recruited by a public contracting authority with AFD financing. **It has two complementary uses**:

- CSOs will find here an explanation of what is expected from them when they submit a response to a call for projects (i.e. a risk analysis).

- Any organization wishing to operate in a red or an orange zone will find additional elements related to the design and implementation of mitigation measures in the section following the presentation of the risk matrix.

WHAT IS NOT INCLUDED IN THIS GUIDE

This guide is not intended to replace the security practices of AFD's partners. They are fully responsible for their own security practices.

This guide is not intended to be prescriptive, particularly in terms of security strategies, which can and should vary according to organizations and contexts. Its use is to be differentiated according to the type of project/service considered and its context. In this sense, it does not provide an evaluation grid against which bids will be reviewed.

Finally, while it can support partners' strategy in defining their budgets, for example by alerting them to the costs associated with security management, this guide does not provide specific references in this area.

It is worth noting that:

- AFD is never required to comment on the measures proposed by its service providers or beneficiaries, which remain their sole responsibility.
- AFD agrees to finance the security measures, defined exclusively by its service providers and beneficiaries, for the services and projects it finances, including in the event of a deterioration of the security context the project.
- In hostile environments, AFD can
  - (i) Include security-related admissibility requirements into its own procurement documentation;
  - (ii) Require its counterparties to use procurement documents that include security-related admissibility requirements; and
  - (iii) Provide its beneficiaries with external support for the review of their security plan (in the case of NGOs) or those of recruited companies (in the case of public project owners).

[1] Classification of the French Ministry of Europe and Foreign Affairs

GENERAL PRINCIPLES

This guide builds on best security practices and aims to make them accessible in a simple and clear manner. Although this document has a primarily operational purpose, it is worth going back to some general principles. Any security plan is part of a broader system, which includes:

i) **The organization's internal security policies**. These describe the duties and responsibilities of the organization and its employees with regards to security. Depending on the case, they may include, but are not limited to, the organization's risk appetite, its general organization in security management (lines of authority and responsibilities), its training policy in this area and its general procedures.

ii) **A security strategy**, based on acceptance, protection or deterrence. Generally speaking, the first strategy aims to establish a relationship of trust with the stakeholders present in the project area; the second strategy aims to enhance security by implementing passive protection measures (e. g. walls, barbed wire, visitor screening); the third strategy is based on active protection measures (e. g. armed escort or any other counterthreat measure).

iii) **A security plan valid for the country of operation, and an adapted version in each area where the projects will be implemented**. This plan includes several elements, described below, that can be combined in a risk analysis matrix. They are operationally broken down into **Standard Operating Procedures (SOPs) and Contingency Plans (CPs)**:

- **The SOPs** correspond to probability mitigation measures and typically include procedures that facilitate and standardize communications, travel, accommodation (e.g. securing offices or living places for the organization's staff), money transfer procedures, etc.
- **- The CPs** correspond to probability mitigation measures and must define procedures to guide hibernation, relocation and evacuation processes, as well as crisis management, including family relations, communication with the authorities concerned and the media.

Autonomy of Organizations, Consistency of the Security System

Each organization is free to define its practices according to its means, structure and objectives. It is quite possible that an NGO and private companies may adopt different strategies and procedures in the same context. However, **it is essential that the structure of the various framework documents be consistent, and mitigation measures must reflect the organization's strategy. For instance, SOPs based mainly on armed protection would be difficult to integrate into a security strategy focused on the acceptance of teams by the population.**

Because they include activities that go beyond the projects financed by AFD, this guide does not cover in detail aspects related to internal policies or security strategies.

STRUCTURE OF THE GUIDE

This guide is structured into four parts:

- **The general organization of security**, which briefly addresses the importance of clarity in terms of responsibilities and lines of communication.
- **The risk analysis**, including context analysis, threat and vulnerability analysis.
- **The risk matrix**, summarizes the main points of the analysis, and makes it possible to prioritize the risks and identify the main mitigation measures. Although it is organically part of the risk analysis, it is presented here separately.
- **The probability mitigation measures (Standard Operating Procedures - SOPs) and impact measures (Contingency Plans - CPs).** Precise information on specific SOPs and CPs is presented, including those relating to crisis management, as well as information on security measures prior to the deployment of teams.

The first three components are at the heart of any security plan. While it may include other elements at the discretion of the organizations and depending on the contexts in which they operate, the topics presented are usually integrated into a security plan.

The tools and methods presented below are summarized and introductory.
They are intended to raise awareness on best practices among the users of this guide and should not limit interested parties to the content proposed here. **References** to learn more on the methodology or perspectives are suggested at the end of the document.

The definitions of security strategy are left to the readers' discretion. Choices in this area naturally influence the design and implementation of SOPs and CPs. This guide has been drafted with the necessary flexibility in mind to provide a common basis to a wide range of players.

Missions in orange or red zones are by nature subject to a greater number of **hazards** than in more stable environments. To take this into account, readers are encouraged to **conduct regular reviews** of their analyses, SOPs and PCs, over no more than annual cycles. Finally, we would like to draw everyone's attention to the importance of properly quantifying the budgets associated with the effective implementation of a security plan.

WARNING

Gender differences result in significant differences in terms of threat exposure, vulnerability profiles and risk mitigation measures. It is **strongly recommended** to design, write and implement security plans with mixed teams, so that the diversity of security issues can be analyzed and anticipated as accurately as possible

1. GENERAL ORGANIZATION OF SECURITY

The general organization of security can vary greatly from one organization to another. Depending on the size, specific positions may be created or, conversely, missions may be part of a larger scope of responsibility.

In all cases, clear responsibilities exist at the international (headquarters), national (agency or mission) and local (project location) level. The lines of communication between the different levels of responsibility are clear, formalized and all staff know the person to whom they can refer if necessary.

Level	Main tasks
International (HQ)[2]	A security policy is in place. A crisis management plan is in place, circulated to the relevant people who are trained in its use and who make up the Crisis Management Cell (CMC). A person is in charge of the administrative aspects of security (insurance, especially for medical risks). One or more focal points are clearly identified to provide support to national security teams.
National (Agency, Office or Mission)	A security plan is in place. Security responsibilities are clear and known to all: everyone knows who has the authority to validate movements, to decide on a relocation or temporary suspension of activities. An incident management plan is in place, circulated to the relevant people who are trained in its use and who make up the Incident Management Unit (IMC). A person is in charge of maintaining a monitoring network with the relevant contacts to ensure the continuous update of specific threats. He or she maintains contact with the relevant supporting stakeholders to help the teams whenever necessary (e.g. with the authorities, an embassy or others in the case of hibernation). A person ensures that the equipment (rolling stock, communications equipment, medical kits, etc.) necessary for security management is available and properly maintained.
Local (Project)	A local security plan is in place. A person is in charge of maintaining a monitoring network with the relevant contacts to ensure the continuous update of specific threats. He or she maintains contact with the relevant supporting stakeholders to help the teams whenever necessary (e.g. municipal and traditional authorities, other organizations present, etc.)

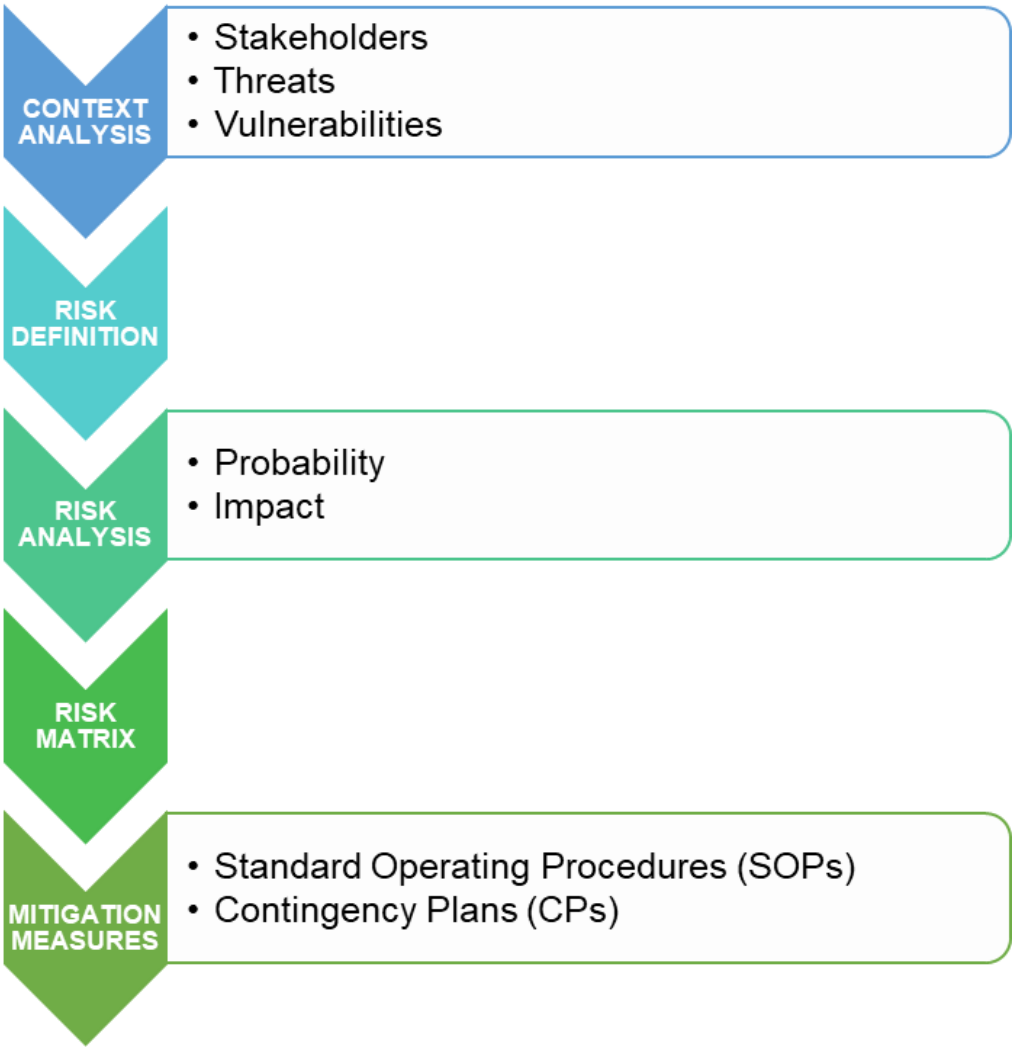
[2] All the references for the international level are naturally solely applicable to international entities

2. SECURITY **ANALYSIS AND THREATS**

The definition of measures adapted to the risks involved requires that they be precisely defined and prioritized. To this end, it is necessary to conduct a context analysis, the purpose of which is to better identify the threats surrounding the project context and the threats to which it exposes the organization. The graph below summarizes the main steps in defining a security plan, which consists of:

- An analysis of the context;
- A risk analysis;
- Measures to mitigate the impact and probability of each associated risk.

Ideally, all these elements should be included in the security plan.[3]



[3] This graph is adapted from : Von Braabant K. et Humanitarian Outcomes : *Revue des bonnes pratiques, Gestion opérationnelle de la sécurité dans des contextes violents, version révisée Décembre 2010*, p. 9. Also called GPR8 v 2010, French version available here:
https://odihpn.org/wp-content/uploads/2011/03/GPR8_revised_edition_French.pdf

2.1. CONTEXT ANALYSIS

Understanding the context

The context analysis is the prerequisite for any risk analysis. It identifies the stakeholders, threats and vulnerabilities that shape the risks to which the organization is likely to be exposed.

Any security plan must present the context in varying degrees of detail, each organization being free to arrange this section according to its objectives, but it is always necessary to describe the following main points:

Theme	Characteristics
Human aspects	Demography, ethnicity, population (urban/rural, economic migration, displacement), lifestyle (farmers and pastoralists), vehicular and local languages, etc.
Geography	The area and resources, specifically water and energy
History	Main steps in the formation of the political and social scene of the country under consideration and, ideally, of the area under consideration
Politics	Political events affecting the situation: Electoral deadlines Political issues (agrarian reform, nationality code, constitutional reform)
Foreign policy	Integration into regional groups Foreign trade Strategic partnerships and alliance systems Strategic implications
Socio-economic context	Structure of the economy (primary, secondary and tertiary) GDP per capita, average wage, employment, literacy rate, etc. Healthcare system
Conflicts	Description of the main conflict(s) (if any): Stakeholders involved Issues at stake Ideological aspects Economic aspects of the conflict

Context analysis needs to be reviewed regularly, ideally annually, sometimes more in response to sudden events.

Key steps of a context analysis

1. **Document review**: This phase consists of collecting, analyzing and synthesizing as much information as possible available on the country and the area of the mission. Media (especially press and radio), online sources, specialized sites and academic journals can provide considerable material to support the design of the most detailed questionnaire possible for the next steps.

2. **Investigation outside the country of the mission**: Ideally supported by a solid documentary research, it is possible to contact several types of organizations with knowledge of the project area. These may be diplomatic representatives, university research centers, think tanks, international or non-governmental organizations.

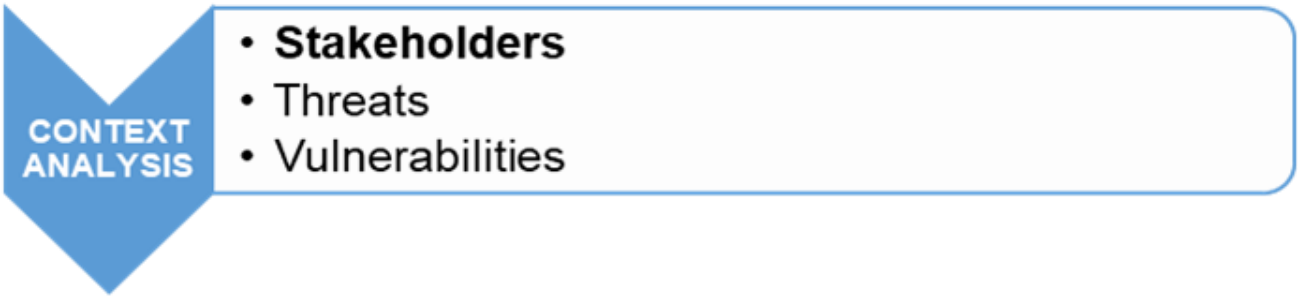
3. **Field survey in the capital of the country:** Building on previous work, the field survey collects the analysis of several types of stakeholders: government authorities, organizations (national and international) active in and/or around the project area, and also allows one to orientate the interviews towards the business and companies in the area (logistics providers, in particular). National university research and civil society players are key and often forgotten resources in this phase.

4. **Field survey at the project site** where possible. At the end of the process, this work makes it possible to contact local actors active in the project area, such as local authorities (Prefecture, Municipality, etc.) or traditional authorities (Sultanate, Lamidats, Chiefs, etc.), and local civil society representatives (NGOs, Research Centres and Universities, etc.). The private sector is also a significant source of information. Finally, it is necessary to come into direct contact with armed stakeholders in some cases.

WARNING

It may not be possible to visit the field before submission. However, it is essential to have completed the first two steps to inform the key elements of the security plan at that time.

Stakeholders analysis



The first step in context analysis is to identify the different stakeholders in your environment. There can be several types of stakeholders, the following table gives a non-exhaustive list of different players:

	Type	Examples
Armed stakeholders	Regular armed forces of the country of operation	The National Army, Police forces or any other form of official law enforcement force
	Militias	Mayi Mayi in the DRC, Kamajohs in Sierra Leone.
	Private Security Company (PSC)	Security groups responsible for the security of sensitive sites in the Niger Delta. Companies in charge of the security of living spaces in Nairobi.
	Armed Opposition Groups (AOGs)	Groups organized politically and militarily, contesting the authority of the government at the local or national level with arms.
	Others	Family Katibas in Syria. Criminal and terrorist organizations Small non-organized crime (e.g. in urban areas).
Non-armed stakeholders	Governmental authorities	Ministries, centralized and decentralized administrations
	Traditional authorities	Sultanate Kanem in Chad
	Local authorities	Camp leaders in camps for internally displaced people
	Local population	Different ethnic groups co-existing in the same environment (rural or urban).

	Displaced population	Displaced groups in Iraq from the province of Ninive to Iraqi Kurdistan.

Each of these players has a distinct modus operandi and organization (and sometimes no clearly identifiable organization, as is often the case for petty crime, for instance). Identifying these two aspects helps to clarify any authorizations or re-insurances that may need to be obtained, and to specify the specific threats posed by some of these groups in your environment. Gauging a player's modus operandi, intentions and capacities makes it possible to assess whether a threat related to this stakeholder is credible, and therefore probable, or not.

All these groups have more or less clear intentions, and have more or less significant means. Their intentions depend on their objectives. These can be elementary (survival for displaced populations), difficult to identify (in the case of heterogeneous groups, where objectives are contested internally) or very clear (for instance, the stated ambition of some groups to kidnap nationals of certain nationalities).

Similarly, the resources available to these different groups vary widely. Some armed groups (AOGs) may be completely under-equipped or, on the contrary, have the qualified human resources to use a large arsenal, be it military, administrative or other.

Taking into considerations the intentions and resources of the various actors makes it possible to assess the degree of threat that each can represent. A small group with few weapons that does not seem hostile does not represent a big threat. On the other hand, an AOG with resolutely hostile ambitions and a proven ability to conduct lethal and complex operations is a very strong threat.

Intentions and means can evolve very quickly according to ideological reframes, fights or other factors. Therefore, these two aspects should be assessed dynamically as much as possible. To do so, it is possible to mobilize:

- Diplomatic resources (advice to travelers from the various embassies);
- The national press if it is accessible, the international specialized press;
- Specialized sites (university research, think tanks)
- Contacts with organizations present on site.

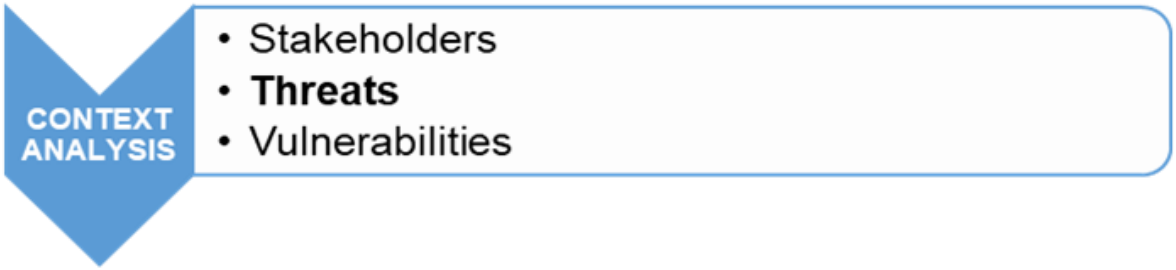
Once consolidated, in order to prepare the risk matrix, these elements can be summarized in broad categories, the table on the following page provides an example of categories. The categories mentioned are generic and the reader is free to adapt them according to his/her needs. For each category, an indicator is defined on a basis of 1 to 5, ranging from a peaceful environment (level 1) to a high level of threats (level 5).

	Conflicts	Tensions	Activism	Crime
Description of the security level	1- No armed conflict for more than 10 years and/or conflict-related problems resolved	1- No socio-political tensions	1- No armed dissident in the country	1- Violent crimes are very rare
	2- No armed conflict for more than 5 years and/or conflict-related problems resolved	2- Tensions in some areas with punctual acts of violence	2- Presence of armed dissidents in the country but not in the areas of operation	2- Violent crimes are limited to specific areas
	3- Ongoing low intensity conflict and/or tensions in regional relations	3- Regular tensions with punctual acts of violence	3- Armed groups launch attacks against local or foreign interests	3- Violent crimes target only nationals
	4- High intensity conflict with no end in sight	4- Tensions with systematic violence and an impact on the stability of the region	4- Armed groups indirectly target civilians and/or the humanitarian aid system. Access negotiations remain possible.	4- Violent crimes target nationals and sometimes foreigners
	5- High intensity armed conflict	5- Civil war or coup d'état	5- Armed groups directly target civilians and/or the aid system. Access negotiations are impossible.	5- Widespread violent crimes.

	Environment	Administration	Gender	Infrastructures
Description of the security level	1- Few environmental risks and/or good emergency infrastructure	1- Good cooperation between organizations and government, with no restrictions on access by other stakeholders	1- The context allows for people to live their life freely regardless of gender or sexual orientation.	1 - Electricity, transportation, communications and healthcare services are of high quality and rarely interrupted.
	2- Localized environmental risks and/or acceptable emergency infrastructure	2- Organizations can operate freely with limited restrictions.	2- The context allows for relative freedom.	2 - Electricity, transportation, communications and healthcare services are of acceptable quality and are interrupted from time to time.
	3- Periodic or seasonal environmental risks and/or fragile emergency infrastructure	3- Organizations are limited to certain areas or face resistance from communities. The government can put in place restrictions.	3- The context is defined by gender-specific prescriptive roles, with an implicit tolerance for diversity.	3 - Electricity, transportation, communications and healthcare services are frequently interrupted and have a low level of security.
	4- Regular environmental risks and/or limited emergency infrastructure	4- Operations are facing clear hostility. Some organizations are targeted by militant groups. The government may threaten to expel you.	4- The context is conservative and defined by gender-specific prescriptive roles, with very limited tolerance for diversity.	4- Electricity, transportation, communications and health services are of poor quality. Breakdowns or disruptions are frequent.
	5- Major environmental risks and/or no emergency infrastructure	5- Organizations cannot respond safely and operations are not sustainable. The government is hostile and organizations can be targeted directly.	5- The context is highly conservative and diversity is not accepted.	5- Electricity, transportation, communications and healthcare services are severely degraded or non-existent

Threat analysis

The security plan must include a brief narrative for the main threats identified, indicating for each one the relevant details (risky areas, people at risk, operating procedures).



As part of the document review, upstream identification of the most prevalent threats in the area of operation, based in particular on the resources mentioned above, is necessary.

In connection with the table of levels (see p. 15-16) and in order to prepare the risk matrix, the table on the following page provides a non-exhaustive list of threats associated with each category that may be encountered in degraded security environments.

	Conflicts	Tensions	Activism	Crime	Environment	Administrative	Gender	Infrastructures
Examples of threats	Air strikes	Demonstrations	Suicide attacks	Burglary	Earthquakes	Restrictions on visas	Rape	Insufficient communication network
	Artillery/ mortar fire	Mob movements	Targeted improvised explosives	Robbery	Animal bites or attacks	Interference	Harassment or verbal aggression	Inadequate medical structures
	Crossfire	Riots	Artillery/ Mortar fire	Armed robbery	Electrical problems	Aid diversion	Harassment or physical aggression	Poor condition of the roads
	Mines and UXOs	Lootings	Ambushes	Crime	Fire (accidental)	Fraud / Corruption	Discrimination	
	Ambushes	Coup d'Etat	Arrest / Detention / Interrogation	Car-jacking	Fire (natural)	Direct targeting	Intimidation	
	Improvised traps		Kidnapping	Arson	Epidemics	Threats or intimidation	Blackmail	
	Checkpoints		Indirect improvised explosives	Kidnapping	Extreme weather conditions	Harassment / Aggression	Harassment (On line or not)	
	Direct targeted fire		Armed raids	Murder	Diseases	Access or movement restrictions	Non-verbal harassment	
	Arrest / Detention /		Sexual violence	Abduction	Car accident	Blackmail	Lynching	
	Armed raids		Direct threat	Fraud / Corruption	Plane crash	Surveillance (online or not)	Restrictions	
			Abduction		Flooding	Arrest / Detention /	Kidnapping	
							Arrest / Detention	

WARNING

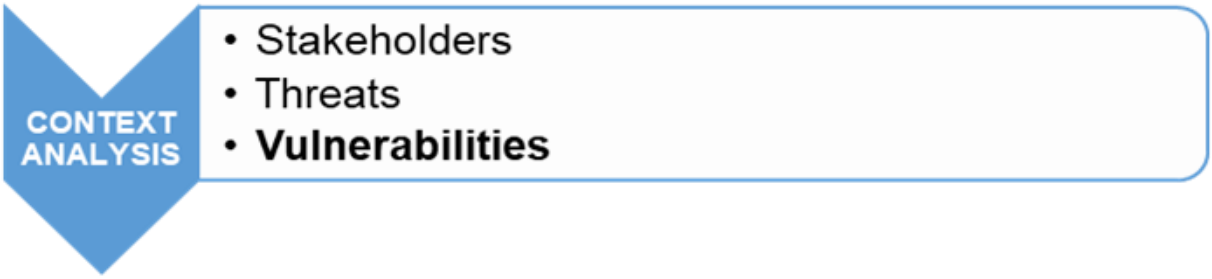
A distinction must be made between internal and external threats. External threats are located in the environment and do not depend on the activity related to a project. Petty crime, for example, is endemic in some places. Internal threats, on the other hand, are linked to the organizations in charge of the implementation a project, whose presence may lead to insecurity previously unknown in your area of operation. The arrival of four-wheel drive vehicles in a context where they are seen as a novelty may, for example, lead to robbery on the roads. More finely, it is necessary to watch out for the threats induced by any new presence. For example, in some areas, local recruitment policy must ensure that it respects the balance between different local groups. The over-representation of one of these groups could fuel community tensions and draw unwanted attention to the organization.

Once the 8 to 10 most likely threats have been identified, it is important to understand them more precisely by specifying for each threat how it is carried out. The following table presents the main questions to be asked for each threat, with examples for illustration.

Question	Example
- Is there a history or chronology available for each threat to identify specific aspects (e. g. neighborhoods known to harbor petty crime, roads with high accident rates, etc.)?	Favelas in Brazil or slums in Nairobi are known for their precariousness and the prevalence of petty crime (armed robbery). In some cities, the proximity of railway or bus stations is also a place of petty crime (pickpockets).
- What are the targets for each threat? Are they targeting groups, isolated people with a specific profile (gender, nationality, sexual orientation, apparent wealth), etc.?	In some contexts, known and repeated threats against staff of certain nationalities (North American countries and Western Europe) have led organizations to assign their non-Caucasian staff to these areas. In some Central and East African countries, the LGBTQ community is subject to unusual distrust, exposing them to high threats of physical violence. Any ostentatious wealth is generally likely to attract malicious attention.
- What is the known modus operandi of the threat actors?	In some countries, criminals deliberately throw themselves against vehicles used by NGO staff. Given the security strategies of NGOs, identified and understood by the criminals, the objective is to force NGOs to provide prompt

	compensation which amounts to a form of extortion. In other countries, the presence of a targeted man for various reasons (wealth, belonging to the diplomatic staff or decision-maker of a large company) may make him vulnerable to being drugged and then having his belongings stolen.

Vulnerabilities analysis



Just because a threat exists does not mean that you are exposed to it. For example, the risk of a car being attacked by "road cutters" on a road (the threat) depends on the frequency with which the car travels (the vulnerability). The absence of any car trip corresponds to zero vulnerability, a high frequency of car movement to high vulnerability.

Threat analysis helps to understand vulnerability factors, distinguishing between those over which it is possible to have an element of control and those over which it is impossible. With regard to the threats identified, the security plan must indicate the internal and external factors of vulnerability.

Some vulnerability factors are context-specific and out of control. The presence of armed groups is an illustration of this. Others, on the other hand, are subject to changes. In contexts where certain nationalities or physical profiles are more particularly targeted (French or American nationals in certain regions of the Middle East or the Sahel, Caucasians in Yemen), it is important to identify the related vulnerability, it can be neutralized by recruitment measures specific to the concerned area.

A review of the history of incidents, locations and targets can help identify and differentiate these types of vulnerabilities, which must be mentioned in the security plan before mitigation measures are subsequently defined.

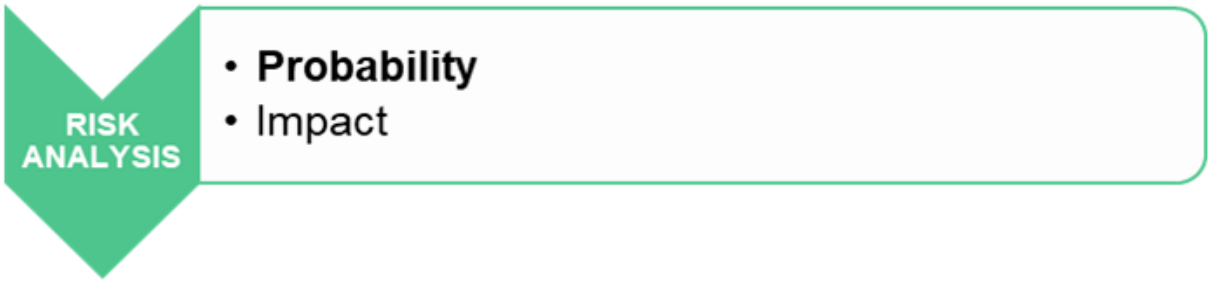
2.2. Risk analysis

Warning

The risk analysis will have to be included in the proposal in answer to an RCCP.

The combination of threats and vulnerabilities translates into risks. The presence of mines (threat) on roads used by an organization with inadequate resources (vulnerability) can lead to an explosion of the vehicle, resulting in significant damage to the organization's staff and property, or even its reputation (risks). Risk analysis consists of identifying risks and prioritizing them. This analysis will then make it possible, in the next phase and within a risk matrix (point 3.), to identify appropriate mitigation measures. The risk matrix does not have to be integrated into the RCCP.

Likelihood



Probability is measured on a scale of 1 to 5, from least likely to most likely. It is assessed over a defined timeline, usually one year, sometimes less depending on the volatility of the context. For instance, when power is contested, the likelihood of violent demonstrations is higher right before electoral deadlines (campaign, organization of the vote, counting and proclamation of results). This probability is lower outside these periods.

Importantly, while some risks are likely to remain constant over a relatively long period of time, such as malaria in some regions, others may change as political, social, economic or military situations change. It is therefore necessary to specify when the risk is seasonal, such as petty crime during the lean season, i.e. when food reserves are depleted while waiting for the next harvest, and which corresponds to agricultural cycles. More generally, it is important to update the risk analysis on a regular basis - between 6 months and a year in degraded security contexts - to take into account the emergence - or even disappearance - of certain risks over time.

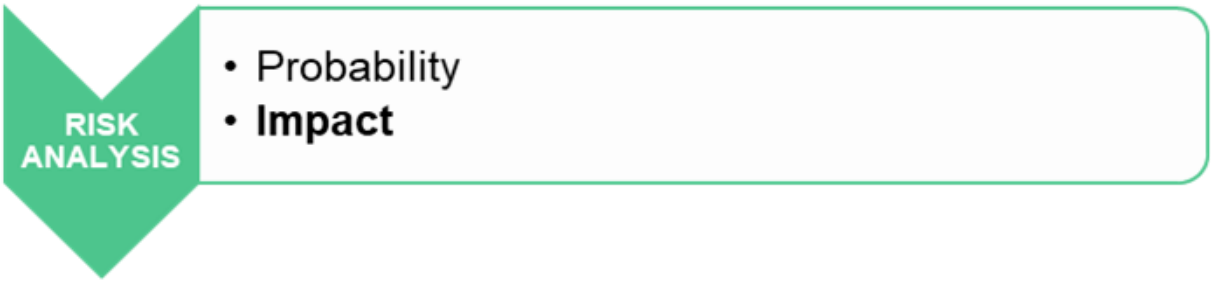
The following table provides a more detailed methodology for assigning the probability of occurrence to a specific risk.

Likelihood	Definition	*Intention* *Capacity* *(see p. 15)*	History	Level

Very unlikely	The event is considered to have no realistic probability of occurring.	Unknown	None	Has never occurred over the last 12 months.	1
Unlikely	The event is considered to have a reasonable probability of occurring.	Potential	Low	Has rarely occurred over the last 12 months.	2
Possible	The event is considered to have an average probability of occurring.	Possible	Average	Has occurred several times over the last 12 months	3
Likely	The event is considered to have a very high probability of occurring.	Probable but not explicit	Significant	Has occurred many times over the last 12 months.	4
Very likely	It is expected that the event will occur.	Clear intention	High	Has occurred regularly over the last 12 months.	5

In addition to natural hazards, threats associated with the presence of armed groups, from petty crime to AOGs, should be specified. The notions of intention and capacity in this table refer to the concepts presented in the stakeholders analysis p.14.

Impact



The impact is also measured from 1 to 5, ranging from least to most impactful. The impact is measured by taking into account the following elements:

- Impact on people (diseases, physical attacks, attacks leaving physical or psychological traumas, death);
- Impact on property (theft of money, inputs, vehicles, etc.; destruction of property, looting, etc.);
- Impact on activities (from temporary suspension to indefinite stoppage);
- Impact on reputation (e.g. loss of customers, suspension of enforcement, legal proceedings, etc.).

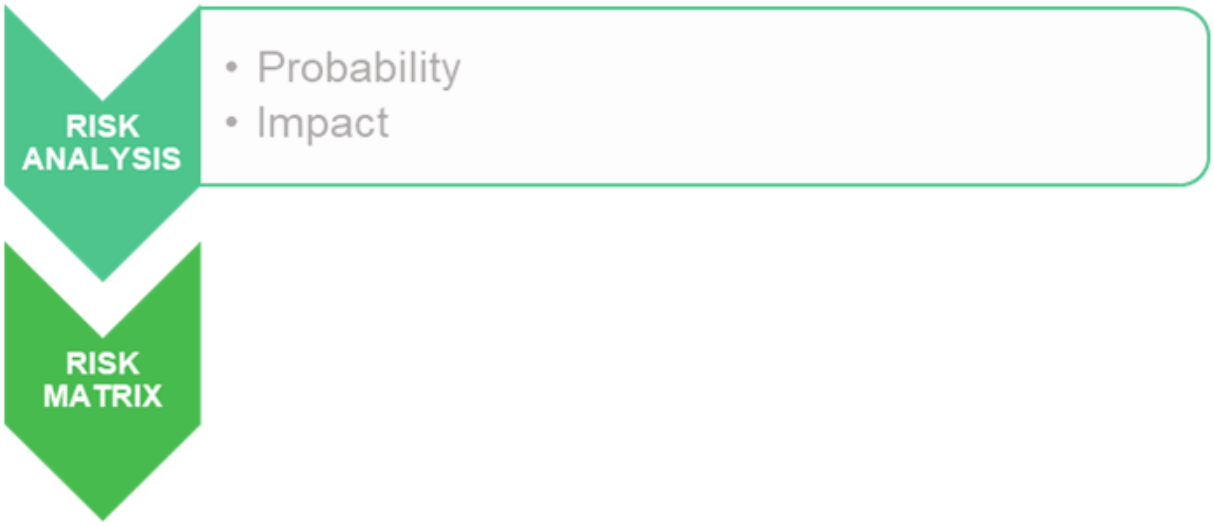
Warning

In general, a high impact combines one or more of these elements. For example, an organized gang robbery can have an impact on people (injuries) and property (money and stolen equipment). One exception is kidnapping: regardless of any combination of elements, its occurrence directly qualifies the impact at its highest level and entails the implementation of a crisis unit.

The following table provides a more detailed methodology for assigning the impact to a specific risk.

Impact	People	Goods	Programs	Reputation	Level
Insignificant	No injuries	No damage	Minor disruptions	Insignificant	1
Minor	Light injuries / possible stress	Possible damage or loss	Some delays	Limited and in some areas only	2
Limited	Non-fatal injuries /high level of stress	Some losses	Delays	Widespread and in some areas only	3
Major	Severe injuries/traumas	Significant losses	Severe disruptions	Limited and across the whole country	4
Critical	Disabling injuries/deaths	Major or complete loss	Suspension of activities	Across the whole country and widespread	5

3. THE RISK MATRIX



The risk matrix is a summary document that:

- Repeats the context analysis and risk analysis,
- Assigns quantitative values to risks (probability and impact)
- Identifies the main lines of mitigation measures (probability and impact)
- Assesses the residual risk once these measures are implemented.

The tables on the following pages give a possible format for a risk matrix, with some clarifications in addition to the points discussed above.

Step	*1*	*2*	*3*	*4*
#	**CONTEXT**			
	Category	**Indicator**	**Description**	**Threat**
1	***Conflict***	***3- Ongoing low intensity conflict and/or tensions in regional relations***	*Since March 15 2013 several AOGs are present in the region of YYY, where the United Nations' mission is deployed. The attacks have been particularly violent in the West and in the South due to high concentration of armed groups*	***1.1. Crossfire***
				1.2.
				1.3
				1.4
				1.5
2	**Tensions**			
3	**Activism**			
4	**Crime**		-	
5	**Environment**			
6	**Administrative**			
7	**Gender**			
8	**Infrastructure**			

Step 1: The categories given here are generic and the reader is free use them as such or adapt them. The elements in italics are given for as an example and are fictitious.
Step 2: Mention the level corresponding to the category.
For the first two steps, you will find the tables on p.16-18 useful for reference.
Step 3: The description corresponds to the indicator. The fictional example given here recaps the key information from the context analysis.
Step 4: Threats should not be presented in detail. Generic category names are provided on p. 19

Step	*5*	*6*	*7*	*8*		*9*
Threat (cf. *Step 4*)	**RISK QUALIFICATION**			**GROSS RISK ASSESSMENT**		
	Description (perpetrator, causes, motivation, location, time…)	**Specific vulnerabilities**	**Risk**	**Probability from 1 to 5**	**Impact from 1 to 5**	**Level of risk from 1 to 25**
1.1. Crossfire	*In area of operation from 'XXX to YYY shots between AOGs and the regular army can happen any time. Strong inter-community between pastoralists and farmers.*	*Areas XXX and YYY are priority for the implementation of the project. To conduct our operations, we must travel there often.*	*Binge present during fights between the AOGs and the regular army, or during inter-community fights.* *Lost bullets can hit unintended targets.*	***3***	***3***	***9***
1.2.						
1.3.						
2						
3						
4		-				
5						
6						
7						
8						

Steps 5 to 7: A brief recap helps give context to the threat and vulnerability, facilitating the identification of the risk.
Step 8: The quantified indicators from the probability and impact analyses summarized on pages 22 and 23, respectively, should be indicated here.
Step 9: The gross risk indicator, i.e. before mitigation measures, simply multiplies the probability indicator by the impact indicator.

Step	*10*	*11*	*12*		*13*
Threat (*Step 4*)	**MITIGATION MEASURES**		**RESIDUAL RISK ASSESSMENT**		
	Of the likelihood	**Of the impact**	**Residual likelihood**	**Residual impact**	**Level of residual risk**
1.1. Crossfires	*The number of movements is reduced. All movements are validated after consultation with stakeholders (AOGs, Army, Communities). The vehicles are equipped with redundant means of communication (GSM and Satellite and/or Radio) and regular updates are made during the movement to reassess the situation.*	*Staff are equipped with bulletproof vests. The vehicles are equipped with a "trauma kit" (compression dressings, tourniquets, in particular). Teams are trained for their use.*	***2***	***2***	***4***
1.2.					
1.3.					
2					
3					
4	-				
5					
6					
7					
8					

Step 10: Measures to mitigate the likelihood of the risk occurring are mentioned, and should be the subject of a detailed SOP.
Step 11: Measures to mitigate the impact of the risk are mentioned, and should be the subject of a detailed CP.
Steps 12 to 14: Same procedure as for steps 8 and 9, the final result gives the level of residual risk and allows one to assess the acceptability of the risk

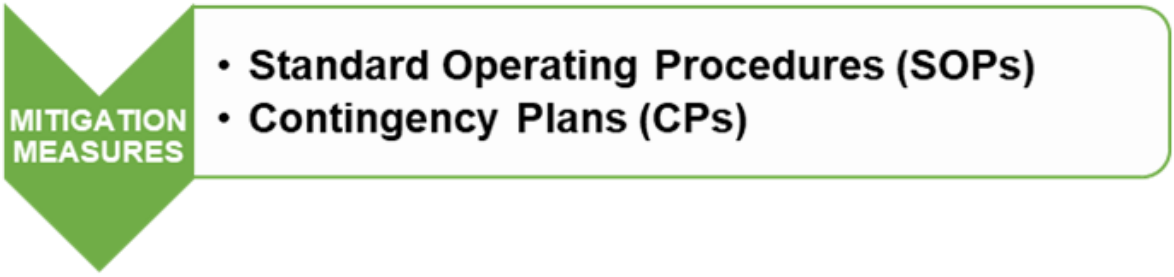
.

WARNING

Steps 10 and 11 must also make it possible to identify the elements that will have to be included in a possible budget dedicated to security.

4. GENERAL SECURITY MEASURES

Once the risks have been specified and ranked, it becomes possible to identify the levers that will reduce the probability of occurrence or impact. The first are the Standard Operating Procedures (or SOPs). The second is the Contingency Plans (CPs).



General principles for definition and implementation

SOPs and CP respect several general principles

Mitigation measures are defined nationally (capital city and general country aspects) **and locally** (base and specific aspects of the local context).
In all cases**, collegial work during the drafting includes mixed gender (men and women) and National/International teams,** in particular to take into account gender aspects and different risk exposures (e.g. setting up office hours to allow national staff to return home safely before nightfall).

The dissemination of documents should be a particular focus. Although in principle they only summarize general elements, they can be misinterpreted (e.g. leading to suspicions of espionage). The mailing list for each plan or procedure must be specific and targeted to the key people concerned. For instance, drivers must be familiar with the Movement and Communication SOP, but are less concerned by the SOP on the living areas of expats.

Some of the measures envisaged need to be included in a training, such as Communication SOPs if they include the use of specific equipment (HF, VHF or satellite telephone).

It is recommended that drills be conducted on these measures, for instance the SOPs on Security of the premises. Staff will really get to grips with the content of these documents if they take part in evacuations of the premises (siren-type alert or other, grouping at the assembly site, fire-fighting drills for fire extinguishers for trained staff, who must be identified).

Very importantly, SOPs and CPs must be **budgeted**, taking into account in particular the following elements (not exhaustive):
- Possible purchase of equipment (radios, fire extinguishers, etc.)
-Staff training (especially if it is outsourced, such as first aid or firefighting).

Finally, mitigation measures must be **updated** to take into account changes in the context, as well as risk analysis. The cyclicity of updates may vary, but **it is recommended not to exceed one year between two reviews, and to adapt it systematically in case of significant events** (political changes, significant changes in the security environment, etc.).

WARNING

It is possible to use companies specialized in risk management to draft all or some of the elements of the security plan presented above. However, it is strongly recommended to maintain regular contact with the provider concerned; and to specify in the document whether the drafting of the plan has been outsourced, and to which organization.

4.1. PRIOR SECURITY MEASURES

The drafting and implementation of the security plan in the country and the area of operation will feed into the departure preparation procedures for expatriate staff. The following are standard recommendations and are not intended to be included in the security plan as such, although they may be mentioned.

Before leaving, it is advisable to decide whether or not to open the post to family status, and the staff concerned must be informed of this during the job proposal.

It is essential to ensure that all expatriate staff **have consulted a doctor** prior to departure, have their **vaccination records up to date**, and are informed of the main health and hygiene rules in the destination country.

Before departure, the security referent at headquarters must give an **individualized security briefing** to the person concerned, with the aim of informing him or her at least on:

- The organization's security policy and roles and responsibilities.

- The general security situation in the country and specific to the area of operation, presenting the risks analyzed and the mitigation measures implemented;

- The code of conduct in force;

- The importance of registering locally with your local embassy or consulate (ARIANE procedure for France and equivalents);

- The security plan, a complete or substation-specific version of which must be provided;

- Reception procedures upon arrival.

It is also recommended **to provide personal security training as well as first aid training** for all staff travelling to orange or red zones.

Immediately **upon arrival, the security referent in the country of operation must give a detailed briefing to the person concerned**, providing details on the points mentioned above. A guided tour of the city, offices and living areas is also recommended. In addition, it is necessary to hand him/ her:

- **A security envelope**, to be kept with oneself, to be used in the event of petty crime, the aim of this envelope is to defuse any aggression quickly. The envelope can also be used in other circumstances (e. g. emergency movement).
- A small plastic document (size of a credit card that fits easily into a pocket), traditionally called a "**constant companion**" and summarizing the main contacts in case of an emergency (in the country and at headquarter, useful numbers including medical services) as well as the insurance policy number to call for medical evacuations if applicable.
- An **adequate telephone system** with the emergency contacts already saved.

4.2. STANDARD OPERATIONAL PROCEDURES

Necessary SOPs

There can be many depending on the context. The most important SOPs **- which must be included in the security plan** - are summarized in the following table:

SOP	Comments
Movements	Movement validation procedures, determination of the captain, equipment essential for the safety and security of the movement, compliance with speed limits, etc.;
Communication	Frequency of contacts, identification of focal points, nature of the contact (notification of location, etc.), contact modalities (e-mails, cellular network, etc.).
Personal security measures and behavior	Preparation of a « grab bag », personal security envelope, personal alertness, etc. Awareness of socio-cultural norms, etc.
Security and safety of the buildings	Offices and living areas.

WARNING

All SOPs should systematically indicate the purpose of the SOP (who is it for? when should it be used?) and who is responsible for the proper implementation of the SOP.

4.3. SPECIFIC SOPS AND SPECIFIC ELEMENTS

Movements

There are several types of SOPs for movements, and each organization is free to detail their procedures based on risk analysis. Nevertheless, the following points should be mentioned.

Point	Comment
Vehicle maintenance	- Designation of responsibilities - Specification of the logbook (maintenance manual) - Management of consumables
Recruiting, training and managing drivers	- Recruitment protocols (tests, validation) - Additional training (first aid, mechanics, etc.) - Definition of rules of conduct in addition to the traffic regulations - Document on responsibilities (authority of the driver with regard to on-board security rules)
Equipment in vehicles	- Mechanical equipment in case of a breakdown - Communication equipment (redundancy of means) - Water, food, first aid kit - Fire extinguishers - Safety belts and others
Approving trips	- Procedures for verifying the security of the route - Determination of a need for escort if necessary - Protocols for obtaining the escort - Determination of specific procedures (simultaneous movements or “kiss”, night driving, etc.)
Responsibilities	- Designation of a captain for passengers upon departure
Localizing a moving vehicle	- Communication protocols (at regular intervals or when passing through pre-identified sites) - Implementation of additional means if necessary (radio operator on base in case of HF communications, for instance).
Car accident	- Procedures to implement in the event of an accident - Procedures implement if the organization’s vehicle causes an accident (possible risks in the event of an arrest, of turning oneself in, etc.)
Checkpoints	- Location of known checkpoints - Equipment to take with you (official documentation) - Behavior to adopt when approaching and passing the checkpoint) -
Travelling in convoy	Detail of procedures (including distance, communication and contingency)

Communications

As with Movements, there are several types of SOPs for communications, and each organization is free to detail their procedures based on risk analysis and the complexity of their environment. Two major principles in this regard concern:

- The importance of having redundant means of communication (and not relying solely on mobile phones, whose reliability can be faulty in orange-red zone due to lack of a network).
- The importance of having reliable communication protocols

.

Point	Comment
Equipment	- Nature (mobile phone, satellite phone, radio, others). - Location of the equipment - Energy supply (charging rules) - Equipment maintenance by type - Designation of responsibilities for maintenance and charging - Possible methods of handing over the equipment to the teams (where, when, giving sim cards and/or prepaid cards for the smooth running of the communication.
Tool selection	- Mobile network coverage map and identification of non-covered areas. - Specification of the storage location of the tool (for satellite devices).
Communication protocols	- Protocols for routine communication, supplemented by an internal and external communication tree. - Communication protocols during movements and movements (intervals, frequency...) - If necessary, assign identifiers for the use of radios.
Security of Information	- How to protect the confidentiality of information in voice. - How to protect the confidentiality of electronic communications. - Procedures for the protection and safeguarding of information
Visibility	- Basic rules of the organization's signage (on people, vehicles and offices/places of residence).
Media	- What to do if solicited by national or international media.

Personal se, behaviors and actions

Point	Comments
Training	- What are the recommended prerequisites? - What training, if any, should be provided during the stay?
Equipment	- The person is equipped with a "grab bag" during travel - See below what should be included in the "grab bag".
Knowledge of the premises	- Familiarize yourself with the work and living spaces, and relevant procedures (location of first aid kits, fire extinguishers, evacuation plans) - If necessary, know how to locate the safe in the building in case of armed robbery (in order to be able to direct thieves and get them out as quickly as possible).
First aid	- Hold a first aid certificate (PSC 1 level) - Provide the telephone number for medical emergencies
Constant Companion	- This pocket format plastic document summarizes the list of emergency contacts in the area of the mission (police and medical emergency numbers, embassy, internal managers). - It must be updated regularly and distributed to each expat.
Knowledge and respect traditions	- If your organization has a code of conduct, it must have been shared - Each expatriate must be made aware of the customs and habits of the country and region.
Reporting and procedures	- The treatment of breaches of ethics must be clarified, in particular as regards reporting procedures and any disciplinary procedures to be considered.

A grab bag is intended to facilitate an emergency departure (in the event of an emergency evacuation of a site or, more rarely, in the event of a fire alarm). It must at least contain identity and immigration documents (original or copy), a security envelope, water, chlorine tablets, protein bars, clothing adapted to the context, poncho, string, multi-purpose pocket knife, compass, map of the area (non-exhaustive list).

Safety and security of premises

If staff are housed in premises owned by the organization, the procedures should specify the following points, which also apply to workplaces

Points	Main elements
Site structure and organization	- Outer wall of the building (specifying height, thickness, distance of the wall from the building) - Fence characteristics (simple or with airlock) - Emergency exits - Guard's booth - Location of a safe room, description of the room's equipment (minimum safety box and first aid kit) - Gender components (location and separation of toilets, dedicated equipment) - Alternative energy equipment (generator at least) - Evacuation flow and location of fire extinguishers in the event of a fire alarm - Location of first aid kits if necessary
Security management of living and work places	- Procedures for selecting, training and supervising guards if they are recruited by the organization - Points of attention in the selection of a security service provider if necessary - Awareness-raising and training procedures for workplace and resident staff (firefighting and first aid)
Access monitoring	- The procedures for managing visitor flows are specified.

If staff are hosted in accommodation facilities (hotels or other), it is recommended to systematically assess the security of the premises (including the location) and to set up an ad hoc procedure for bookings, daily trips, and additional measures (e.g. communication in case of evacuation, etc.).

4.4. CONTINGENCY PLAN

Necessary CPs

The most important CPs to be completed / adjusted in the light of the situation envisaged that must be included in the security plan are summed up in the following table:

CP	Comments
Death	Identification of checks to be undertaken to confirm identity, contacts with the family (identification and training of designated interlocutors), etc.
Sexual assault	Basic conduct towards the survivor and potential witnesses, possible medical support measures (prophylaxis), possible legal support measures (in consultation with the survivor), specific reporting procedures (in consultation with the survivor, except in specific cases), etc.
Abduction and hostage takings	Provides the IMU with the framework for initial reactions in the event of abduction or confirmed hostage-taking. Such incidents automatically involve the activation of the CMC at headquarters.
Hibernation	Defines the measures to be anticipated in the event of confinement (during a demonstration or the looting of a city). It includes the location of a secure room, the contents of a hibernation trunk (food, drink, energy equipment, hygiene, etc.).
Relocation and Evacuation	Identifies decision protocols (chain of responsibly), route and primary and secondary means of transportation, contacts to have in case of extraction or external support, visas to be obtained in advance in case of evacuation to a third country, etc.
Medical Evacuation	First aid procedures (including specific communication), contact with pre-identified medical support (including ambulance and paramedical), link with medical insurance (communication of insurance policy numbers and emergency contacts), companion of the victim, etc.

CPs related to death, sexual assault and kidnapping generally trigger the activation of a crisis cell and are discussed below as part of a more general crisis management plan (CMP). The CMP is separate from the organization's security plan, but it is strongly recommended to have one for any entity working in a red or orange zone.

Some specific CPs must be described in detail and are specified in the following section.

WARNING

The more SOPs and CPs there are, the greater the probability that they will be poorly controlled or little used by teams. It should be ensured that their implementation and updating remain practical and realistic.

Crisis management

In the event of a serious to critical incident, the IMU in the country of operation must contact a pre-identified referent at headquarters. This referent may be the security manager or another manager in charge on call. The contact at headquarters then alerts the relevant stakeholders by following the procedures described in the organization's crisis management plan, and the Crisis Management Cell (CMC) is activated.

The existence of the crisis management plan must be certified in the security plan, but not detailed. Such a plan must include at least the following elements, to be completed / adjusted in the light of the situation envisaged:

Chapter	Main elements
1. Organization 1.1. Composition of the CMC 1.2. Decision mechanisms 1.3. Activation procedure of the CMC 1.4. Agenda of the first meeting of the CMC 1.5. Lines of communication 1.6. Post-crisis management	This first section clarifies all the main mechanisms of the CMC and effectively supports its members in the early hours of crisis management, when the sidereal effect can be significant and the heterogeneity of information can make decision-making processes difficult. Note: the composition of the CMC must include the name of the senior manager and an alternate for all identified functions. Everyone's emergency telephone numbers must be clearly identified.
2. Main roles 2.1. CMC Manager 2.2. Security Manager 2.3. Human resources Manager 2.4. Communication Manager	The roles of the main managers detail their objectives, the prerequisites for taking up a position in the CMC (training and simulations, in particular) and their main tasks during and after the crisis.
3. Main scenarios 3.1. Death of an employee following a critical incident 3.2. Kidnapping 3.3. Sexual violence	Although each crisis is distinct, the critical incident at the origin of the crisis imposes specific and recognizable sequences. The scenarios provide a standard framework for management that CMC members can rely on.
4. Liaison protocol for families	Liaison with families, usually carried out by the Human Resources Department, requires a specific and particular protocol to deal with difficult situations.

It is recommended that the crisis management plan be subject to regular simulations in order to raise awareness among CMC members of the specificities of crisis management.

Medical evacuation

Subscription to an insurance policy allowing the medical evacuation of the staff (International SOS is a reference organization in this field). The medical evacuation plan must include the following points, to be completed / adjusted according to the situation envisaged:

1. Prior to any medical procedure, the security referent of the country concerned must have identified the main hospitals and medical centers in the region, including emergency numbers. In addition, the main means of transport to health facilities must have been identified, with the means to contact them (public or private ambulances, means made available by the United Nations or other stakeholders).
2. The security adviser is responsible, directly or by delegation to human resources, for compiling emergency medical information for all personnel likely to be medically evacuated. This information must include, in addition to the surname, first name and means of identification (hair color, eyes, etc.):
    - Recent illnesses
    - Ongoing medical treatment if any
    - Known allergies
    - Vaccinations
    - Blood type
    - Emergency number of a family member.
3. Procedure for alerting and triggering the country's Incident Management Unit (IMU), which in due course notifies the security focal point at headquarters for coordination purposes.
4. Medical information on the patient's condition to be collected for transmission to the company in charge of the evacuation.
5. Procedures for putting the company in charge of medical evacuation in contact with the patient's doctors if the patient has been referred to a medical facility.
6. Appointment of an attendant during the evacuation.
7. Designation of a focal point in charge of alerting relatives.

Hibernation

Hibernation is a voluntary containment procedure in the event of violent demonstrations or other similar events that may jeopardize the security of the teams. Hibernation is normally a contingency that can be easily anticipated, particularly with regards to specific deadlines (elections, sporting events, etc.).

A successful hibernation is based on the development of a safe and discreet site in the premises, and its equipment, grouped together in what is known as a hibernation trunk.

The following points must be addressed, to be completed / adjusted in the light of specific situations:

Points	Main components
Localization	- Identification of the appropriate site in living and working areas. - Definition of procedures to be followed in the event of hibernation at the premises of a partner organization.
Numbers	- Assessment of the number of people likely to remain in hibernation. - Evaluation of the number of days during which hibernation is likely to last.
Equipment	- Specification of life equipment (water and food, possibly floor mats and blankets). - Specification of hygiene equipment (bucket, evacuation, bin, feminine hygiene products). - Specification of the energy equipment (battery, batteries, candles, etc.). - Specification of communication equipment (equipment, available credits, chargers).
Site and trunk check	- Definition of equipment supervision responsibilities, - Renewal of perishables
Ad hoc protocols	- Action to be taken in the event of interaction with one or more intruders (assignment of responsibilities, talking points, etc.) - Monitor the situation and how it develops. - Communication protocols with internal or external focal point (likely to support possible extraction, in particular). - Rules for living in a confined space

WARNING

The reader is again reminded of the importance of mobilizing a mixed male/female team to oversee the design and implementation of security plans. This point must be strongly emphasized with regard to Hibernation CPs, which touch on situations that put everyone's privacy to the test, thereby inducing risks outside the situation that led to hibernation in the first place.

Evacuation for security reasons

Evacuation for security reasons

Evacuation can take two forms:

- Relocation refers to the transfer of staff from a base to a safe place in the country for security reasons;

- Evacuation per se involves the transfer of all staff from one country to another for security reasons.

The two procedures contain enough common elements to be dealt with in a common document, although it is recommended to deal with them separately.

The plan must specify the following elements, to be completed / adjusted in the light of the envisaged situation:

1. Evacuation decision mechanisms, including the decision-maker and information on the rule formally forbidding staff from challenging such a decision.

2. Communication lines during the evacuation.

3. Secure assembly points to facilitate groupings, if possible

4. The different evacuation routes precisely by specifying at least two routes (a preferential one and an alternative one)

5. Preferred means of evacuation based on pre-identified scenarios (depending on the local availability of evacuation support, including air transportation)

6. Pre-identified evacuation sites. If they are in third countries, the plan must identify the visa requirements, and the security referent will have made the necessary arrangements to ensure that evacuated staff have either the visas or the foreign currency required to obtain a visa upon their arrival.

7. The staff to be evacuated must be identified.

8. The list of authorized equipment to be carried (from "grab bag" to luggage) must be specified.

9. Ad hoc contacts in the event of evacuation by the military or similar means (United Nations) must be specified.

10. Ad hoc procedures in the event of recourse to consular means must be included (islet system, communication tree).

11. The tasks to be carried out to inform national staff of the decision and take appropriate measures (salary processing, preservation or destruction of potentially sensitive documentation, contracts, preservation of equipment if possible, etc.).

CONCLUSION

The tools presented in this guide are aligned with best practices in the drafting of a security plan. However, these best practices only cover a range of procedures and are not all adapted to the specificities of each organization and the context in which they wish to operate. The appendix will allow us to learn more about security plans and explore different documents in order to build the most appropriate management tools.

It is worth recalling here that any implementation must be accompanied by a reflection on the means and resources to be made available to the company.

REFERENCES

Most documents available are in English. Besides, given the nature of the areas of operation, the majority are intended for international NGOs. However, these resources and documents are valuable for anyone willing to work in orange or red areas. It is worth noting that in English, “sûreté” translates to “security”, and “sécurité” translates to “safety”.

Embassies’ websites

It is strongly advised that the competent bodies of any organization ensure that they consult the country websites of the French embassies, as well as those of the United States and Great Britain, which regularly provide updated information on the country of destination.

Travel advice (MFA) :
https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/

The map showing the red and orange zones is regularly updated and can be consulted at the following link:
https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/conseils-par-pays-destination/

State Department (USA, in English) :
https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html

Government of the United Kingdom (in English):
https://www.gov.uk/foreign-travel-advice

These last two sites are the equivalent of the MFA site indicated above.

General websites

The **Humanitarian Outcomes** think tank specializes in security issues and often publishes relevant analyses, including its annual report on the security of international and national staff in conflict zones. Although limited to humanitarian operations, each report covers all countries in the orange and red zones, and may therefore be useful for all readers of this guide.
https://www.humanitarianoutcomes.org/

The British think tank **Overseas Development Institute** (ODI) has a branch dedicated to humanitarian activities, the Humanitarian Practice Group (HPG). It occasionally publishes security studies. Their page dedicated to security can be found here:
https://odihpn.org/topics-countries/?topic=security

United Nations Department for Safety and Security (UNDSS)

As part of the United Nations General Secretariat, **UNDSS is responsible for providing security support to specialized United Nations organizations** and, sometimes, to other organizations working in conflict areas. Most of the sub-sites to which the parent site redirects are reserved for organizations or individuals listed in the UNDSS register and it is recommended to contact the UNDSS representative in your destination country for further details. https://www.undss.org/

Specialized Documents

The **reference guide** in terms of operational security is entitled:
Operational security management in violent environments, 2010 revised version 2010, mentioned before.
Available on the two following websites
In French:
https://odihpn.org/wp-content/uploads/2011/03/GPR8_revised_edition_French.pdf
In English
https://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

It provides valuable additional information to all the elements discussed in this guide. Although originally intended for international NGOs working in conflict areas, it is now used by many CSOs as well as in the private sector.

The **Centre de Recherches et d'Analyse des Savoirs Humanitaires** (CRASH), Médecins sans Frontières France (MSF – F)'s internal think-tank has published a book in 2016 on crisis management entitled:
Michaël Neuman, Fabrice Weissman, *Secourir sans périr: la sécurité humanitaire à l'ère de la gestion des risques*, 29 mars 2016,
URL : https://www.msf-crash.org/fr/publications/guerre-et-humanitaire/secourir-sans-perir-la-securite-humanitaire-lere-de-la-gestion
The book provides case studies and another perspective on security management. Focusing on MSF France's practices, it focuses primarily on humanitarian action but more broadly on action in the red and orange zones.

LIST OF ACRONYMS

AFD :	French Development Agency
AOG :	Armed Opposition Groups
CMC :	Crisis Management Cell
CP :	Contingency Plan
CSO :	Civil Society Organization
HF :	High Frequency
IMU :	Incident Management Unit
NGO :	Non-Governmental Organization
PO :	Project Ownership
PSC :	Private Security Company
PTSD :	Post-traumatic stress disorder
RCCP :	Request for Crises and Conflict Proposal
SOP :	Standard Operational Procedure
TD :	Tender Document
UNDSS :	United Nations Department of Safety and Security
UXO :	Unexploded Ordnance : ammunitions that have not exploded
VHF :	Very High Frequency

GLOSSARY[4]

Abduction: the act of taking a person against his or her will. This is distinct from "kidnapping", which involves the kidnapper asking for something in return (e. g. a ransom) to release the victim.

Acceptable risk threshold: point beyond which you consider that the risk is too high to continue the operation (compared to the impact of your action) and that you must leave the danger zone; influenced by the probability that an incident will occur and the severity of the impact if it does.

Acceptance approach: a component of a security strategy that attempts to reduce exposure to a threat by building relationships with local communities and relevant stakeholders in the area of operation, so as to obtain their acceptance of your organization's presence and consent to its work.

Ambush: A sudden attack launched from a hidden position, usually consisting of a stop element and a destruction element. A term often used in the context of attacks on a road/vehicle/convoy.

Carjacking: stealing a car while the driver is driving.

Civil-military coordination: liaison between military stakeholders (including for peacekeeping operations) and civilian stakeholders deployed in the field, in particular those from the humanitarian and development community.

Clan: A social group of people united by kinship, that is, believing they have a common ancestor.

Communication network: A set of similar elements linked together to quickly communicate information, such as a security alert. Under this system, a person/organization informs a predetermined list of other people/organizations, which in turn informs others on their list, etc.

Convoy: a group of vehicles (or ships) moving together in an organized manner and under the command of a leader to support and protect each other.

Counter-surveillance: the act of watching if someone is watching you. Strategy to detect if your movements, systems and/or facilities are being investigated by people with malicious intent, e. g. kidnapping, bombing or armed robbery.

Critical incident: a security incident whose severity significantly disrupts an organization's ability to operate; generally endangers or causes death.

Critical Incident Management Team (CIMT): A group created to manage the organizational response to crisis situations. Team generally composed of specific staff members, identified and trained upstream, and with a good knowledge of the critical incident management procedures and protocols implemented by their organization.

Detection: an essential technique used to get out of suspected mined terrain, in which the ground is very carefully examined before stepping on it.

Detention: the act of holding a person in captivity under authority (e. g. police, border guards).

Determination the incident profile: visualization, usually on a map but also possible in a time frame, of the time, location and type of incidents that occurred in order to determine trends and identify possible trends such as high-risk areas and/or periods.

[4] The glossary is from : *Revue des bonnes pratiques, Gestion opérationnelle de la sécurité dans des contextes violents, version révisée Décembre 2010*, p. XV sq.

Deterrence strategy: a component of a security approach that attempts to prevent a threat by using a counter threat. This can, in its most extreme form, be armed protection.

Emergency planning: a management tool used to ensure adequate preparedness for various potential emergency situations specific to a context.

Evacuation: securing staff by removing them from a country.

Extortion: the use of coercion or intimidation to obtain money, objects or favors.

Focal point: Security liaison officer, usually responsible for a group of people in a defined geographical area; the focal point is an important "link" in the communication chain and will also ensure that all people under his responsibility follow the adopted security procedures.

Gang: an organized group of aggressive people with destructive, criminal, rogue or violent intentions.

Ghetto mentality: the tendency of members of an organization to discuss and analyze the external environment among themselves, within the protective limits of their "group", without much consultation or interaction with the various actors of the external environment.

Harassment: abusive behavior, whether verbal or physical, towards a person that causes distress or embarrassment.

Hazard habituation: the phenomenon of adaptation, generally unconscious, of its acceptable risk threshold, resulting from regular or constant exposure to the hazard; consequently, the objective assessment of the risk and its potential consequences is reduced, which can lead to increased risk taking through uncontrolled exposure.

Hibernation: the process of taking shelter on site until the threat and/or danger passes, assistance is provided or it is possible to move safely.

Hostage situation: situation in which a person or group of people is in a state of siege in a known place. As in the case of a kidnapping situation, the security and subsequent release of hostages is generally subject to certain conditions. These may include a political or financial request.

Gender-based violence: violence against a person based on gender, sex. Includes threats and/or acts that inflict physical, mental or sexual suffering, coercion or other deprivation of liberty. Although people of both sexes and all ages can be victims, women and girls are the main victims because of their subordinate status.

IED: Improvised explosive device. A bomb that can be placed almost anywhere, for example, on the side of a road, in a vehicle, bag, parcel, letter or clothing.

Incident analysis: A more in-depth and decisive study of the structural, operational and contextual factors that led to a security incident; questioning the effectiveness of the various dimensions and measures of security management and asking whether and to what extent the organization or one or more of its staff could be considered to have "been at the source of the incident".

Incident investigation: the collection of situational and circumstantial information about an incident that has occurred, in addition to the basic facts set out in the incident report.

Kidnapping: The kidnapping and detention of a person by force for the explicit purpose of obtaining compensation (money, equipment or certain actions) against the life and release of the person.

Knowledge of the field: being attentive and understand the physical and social environment in which you operate, know the source of potential hazards, assistance and shelter.

Medevac: Medical evacuation - transfer of a patient by road, sea or air to obtain medical treatment in another location.

Neighborhood Watch: a more or less formalized community program between neighbors aimed at monitoring suspicious people and fighting crime in their area of influence or residential area.

Private security provider/company/private security provider: a private entity providing security services to individuals or organizations for a fee. These services can range from "soft" security (e.g., consultations, training and logistical support) to "hard" security (guard services, armed protection) and risk and crisis management, armed forces training and even operational command and combat.

Protection: used here separately for "safety" and "security" and refers to the "securing" of civilians and non-combatants who are not members of the humanitarian aid organization's staff.

Protection approach: a component of a security strategy that emphasizes the use of protection procedures and devices to reduce vulnerability to existing threats; this approach has no effect on the level of the threat.

Post-traumatic stress disorder (PTSD): A psychological disorder that can affect people who have suffered severe emotional trauma and can cause sleep disturbances, flashbacks, anxiety, fatigue and depression

Relocation: The relocation of staff from a place of operation to a safer place, usually within the country.

Risk: the probability and potential impact of facing a defined threat.

Risk assessment/analysis: an attempt to consider risk more systematically in terms of the threats in your environment, your particular vulnerabilities and your security measures to reduce the threat and/or reduce your exposure.

Risk mitigation: the objective of your security management is to reduce the threat and/or your vulnerability.

Rules of Engagement: guidelines for any combatant or armed guard specifying the conditions and limits under which they may use force when using their firearms.

Safety: to be protected from risk or damage resulting from unintentional acts (accidents, natural phenomena/disasters or disease).

Scenario creation: predict how the situation could unfold in the short to medium term and how threats in your environment could evolve; review the hypotheses in your plans and consider what you would do if they did not occur.

Security: to be safe from risk or harm resulting from violence or other intentional acts.

Security audit: Assessment of the strengths and weaknesses of an organization's security management and infrastructure in order to assess its effectiveness and identify areas for improvement.

Security (alert) phases: summary of the classification of different possible levels of risk and insecurity in your environment, each requiring a specific set of mandatory security procedures.

Security strategy: the philosophy, combination of approaches and use of resources that together define the security management of an organization.

Sexual assault: act or threat of rape, sexual assault and intimidation, sexual harassment or unwanted touching.

Small arms: weapons used for self-protection and close or short-range combat.

Social reference: a personal recommendation or "guarantee" concerning the possible recruitment of a person, without necessarily having worked with him/her but with knowledge of his/her position and reputation in a community.

Standard Operating Procedures: formally established procedures for conducting certain actions or acting in certain situations, in particular to prevent an incident from occurring (preventive aspect) or to survive an incident, or procedures to be followed when managing an incident/crisis in an organization (reactive aspect).

Stress: a state of physical and/or emotional tension, deep or prolonged worry. "A person's state or feeling when he or she feels that the demands exceed the personal and social resources he or she is able to mobilize. (Richard S Lazarus)

Survival on the battlefield: measures to reduce the risk of death or injury when a person is under enemy fire, or in a shooting zone, regardless of the type of weapon used.

Terrorism: acts intended to inflict spectacular or fatal injuries on civilians and to create an atmosphere of fear, usually to pursue a political or ideological objective.

Threat: danger in your operating environment.

Threat assessment/analysis: an attempt to examine more systematically the nature, origin, frequency and geographical concentration of threats.

Threat mapping: visualize and illustrate threats on a map.

Trap: an improvised or specially designed explosive system, usually attached to ordinary objects or hidden under objects (teddy bear, doll, military object, etc.), used to deter, injure or kill people approaching the trapped area.

Triangulation: cross-checking information or details by comparing the opinion or version of different sources.

Unexploded Ordnance (UXO): any type of ammunition (bullet, hand grenade, mortar shells, etc.) that has been primed (prepared for firing) but not used, or that has been fired but has not exploded and is unstable and dangerous.