OTHER SOLUTIONS

OTHER SOLUTIONS
Building Up Confidence

PLANS DE SÛRETE

GUIDE DE BONNES PRATIQUES

2019

AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT

OTHER SOLUTIONS Consulting

England and Wales Registration number 85 48 765 | VAT 169 5909 53

Avertissement

Les bonnes pratiques recensées dans ce guide ne sont fournies qu'à titre indicatif. Elles ne prétendent en aucun cas constituer des mesures suffisantes pour assurer la sécurité des biens et des personnes dans le cadre du contrat**. L'évaluation des risques et les mesures de sûreté à définir et mettre en place relèvent par conséquent de la responsabilité exclusive du partenaire de l'AFD qui les établira dans son plan de sûreté.** L'AFD et OTHER SOLUTIONS Consulting ne pourront être tenus responsables d'une évaluation des risques ou de mesures de sûreté qui s'avéreraient insuffisantes ou inadaptées aux risques et événements.

Définitions et Précisions

La sûreté vise à atténuer les risques induits par la violence ou tout acte intentionnel de malveillance, alors que la sécurité vise à atténuer les risques induits par des actes non intentionnels (liés par exemple à la santé ou aux catastrophes naturelles). L'attention des utilisateurs est attirée sur le fait que ce guide s'attache en priorité aux questions de sûreté. Les enjeux de sécurité associés aux catastrophes naturelles et à la santé ne sont pas abordés spécifiquement, à l'exception de quelques précisions sur les évacuations médicales. Les utilisateurs sont vivement encouragés à développer des mesures spécifiques pour atténuer l'impact de ces éléments en fonction de leur prévalence – annuelle ou saisonnière – dans les contextes d'intervention envisagés.

Contact

OTHER SOLUTIONS Consulting Ltd.

Bureau de Londres

contact@othersolutions.eu

+44 (0)2038456691

Entreprise enregistrée en Angleterre et Pays de Galles 85 48 765 | VAT 169 5909 53

https://othersolutions.eu

TABLE DES MATIÈRES

INTRODUCTION

À QUI S'ADRESSE CE GUIDE ?

Ce guide vise à éclairer la prise en compte des enjeux de sûreté et explicite les bonnes pratiques utiles à l'élaboration de plans de sûreté. Il s'adresse à toutes les entités souhaitant bénéficier ou bénéficiant d'un financement AFD pour intervenir dans une **zone orange ou rouge**[1] en particulier : aux prestataires recrutés directement par l'AFD ; aux organisations de la société civile (OSC) bénéficiant de subventions de l'AFD ; aux entreprises de travaux et consultants recrutés par une maîtrise d'ouvrage publique sur financement AFD. Il a **deux utilisations complémentaires** :

- Les OSC trouveront ici une explicitation de ce qui est attendue d'elles lorsqu'elles soumettent une réponse à un appel à projets (i.e. une analyse des risques).
- Toute organisation souhaitant intervenir en zone rouge ou orange y trouvera en sus des éléments touchant à la conception et à la mise en œuvre des mesures d'atténuation, dans la partie qui suit immédiatement la présentation de la matrice des risques.

CE QUE N'EST PAS CE GUIDE

Ce guide n'est pas destiné à se substituer aux pratiques des partenaires de l'AFD en matière de sûreté. Ceux-ci ont l'entière responsabilité de leurs pratiques en la matière.

Ce guide n'a pas une vocation prescriptive, notamment en termes de stratégies de sûreté, qui peuvent et doivent varier en fonction des organisations et des contextes. Son utilisation est à différencier en fonction du type de projet / prestation envisagé et du contexte dans lequel il / elle s'insère. En ce sens, il ne fournit pas une grille d'évaluation à l'aune de laquelle les soumissions seront examinées.

Enfin, s'il peut soutenir la réflexion des partenaires dans la définition de leurs budgets, par exemple en les alertant sur les coûts associés à la gestion de la sûreté, ce guide ne fournit pas de références spécifiques en la matière.

Il est rappelé que :

- L'AFD n'est jamais amenée à se prononcer sur les dispositifs de sûreté proposés par ses prestataires ou bénéficiaires, qui demeurent de leur entière responsabilité.
- Elle accepte de financer les mesures de sûretés, définies exclusivement par ses prestataires et bénéficiaires, des prestations et projets qu'elle finance y compris en cas de dégradation de la sécurité en cours de vie du projet.
- Dans des contextes sécuritaires dégradés, l'AFD peut
  - (i) Intégrer des conditions de recevabilité liés à la sûreté dans sa propre documentation de passation de marchés ;
  - (ii) Exiger de ses contreparties qu'elles utilisent une documentation de passation de marchés incluant des conditions de recevabilité liés à la sûreté ; et

[1] Le Ministère de l'Europe et des Affaires Etrangères (MEAE) français définit quatre types de zones à plus ou moins haute intensité de risques, allant de vert (très faible intensité) à rouge (très haute intensité). Elle est régulièrement actualisée et les mises à jour peuvent être consultées sur le site suivant :

https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/conseils-par-pays-destination/

(iii) Mettre à disposition de ses bénéficiaires un appui externe pour la revue de leur plan de sûreté (cas des ONG) ou ceux des entreprises recrutées (cas des maîtrises d'ouvrage publiques).

PRINCIPES GENERAUX

Le présent guide capitalise sur les bonnes pratiques en matière de sûreté et vise à les rendre accessibles de manière simple et claire. Bien que ce document ait une visée avant tout opérationnelle, il convient de revenir sur quelques principes généraux. Tout plan de sûreté s'insère dans un dispositif plus large, qui inclut :

i) **Les politiques internes de sûreté de l'organisation**. Celles-ci décrivent les devoirs et responsabilités de l'organisation et de ses employés en matière de sûreté. En fonction des cas, elles peuvent entre autres inclure l'appétit au risque de l'organisation, son organisation générale en matière de gestion de la sûreté (lignes d'autorité et responsabilités), sa politique de formation en ce domaine et ses procédures générales, sans que cette recension soit exhaustive.

ii) **Une stratégie de sûreté**, reposant sur l'acceptation, la protection ou la dissuasion. En termes généraux, la première stratégie vise à établir une relation de confiance avec les acteurs présents dans la zone de mise en œuvre des projets ; la deuxième vise à renforcer la sûreté en mettant en place des mesures de protection passive (murs, barbelés, filtrage des visiteurs, par exemple) ; la troisième repose sur des mesures de protection active (escorte armée ou toute autre mesure de contre-menace, par exemple).

iii) **Un plan de sûreté valable pour le pays d'intervention, et décliné dans chaque zone où se dérouleront la mise en œuvre des projets**. Ce plan inclut plusieurs éléments, décrits ci-après, qui peuvent être combinés dans une matrice d'analyse des risques. Ils se déclinent opérationnellement en **Procédures Opérationnelles Standard (POS) et en Plans de Contingence (PC) :**
   - **Les POS** correspondent aux mesures d'atténuation de probabilité et incluent typiquement des procédures facilitant et standardisant les communications, les déplacements, l'hébergement (par exemple la sécurisation des bureaux ou des lieux de vie destinés à accueillir du personnel de l'organisation), les procédures de transfert d'argent, etc.
   - **Les PC** correspondent aux mesures d'atténuation de probabilité et doivent définir des procédures guidant les processus d'hibernation, de relocalisation et d'évacuation, ainsi que la gestion de crise, y compris relations familiales, communication avec les autorités concernées et les média.

Autonomie des Organisations, Cohérence du Dispositif de Sûreté

Chaque organisation est libre de définir ses pratiques en fonction de ses moyens, de sa structure et de ses objectifs. Il est tout à fait possible qu'une ONG et des entreprises privées adoptent des stratégies et des procédures différentes dans un même contexte. En revanche, **il est impératif que l'articulation des différents documents cadres soit cohérente, et les mesures d'atténuation doivent refléter la stratégie de l'organisation. A titre d'exemple, des POS reposant avant tout sur la protection armée s'inscriraient malaisément dans une stratégie de sûreté centrée sur l'acceptation des équipes par les populations.**

Parce qu'elles englobent des activités qui vont au-delà des seuls projets financés par l'AFD, le présent guide n'aborde pas en détail les aspects touchant aux politiques internes ou aux stratégies de sûreté.

ORGANISATION DU GUIDE

Ce guide est organisé autour de quatre parties :

- **L'organisation générale de la sûreté**, qui aborde brièvement l'importance de clarté en matière de responsabilités et de lignes de communication.
- **L'analyse de risque**, comprenant l'analyse de contexte, l'analyse des menaces et des vulnérabilités.
- **La matrice de risques**. Reprenant les points principaux de l'analyse, elle permet de hiérarchiser les risques et d'identifier les principales mesures d'atténuation. Bien que faisant organiquement partie de l'analyse de risques, elle est présentée ici séparément.
- **Les mesures d'atténuation de la probabilité (Procédures Opérationnelles Standard - POS) et d'impact (Plans de Contingence - PC).** Des éléments de précision sur certains POS et PC spécifiques sont présentés, y compris ceux touchant à la gestion de crise, ainsi que des éléments de réflexion sur les mesures de sûreté préalables au déploiement d'équipes.

Les trois premières composantes sont au cœur de tout plan de sûreté. Si celui-ci peut inclure d'autres éléments au gré des organisations et des contextes d'intervention, les sujets présentés sont habituellement intégrés dans un plan de sûreté.

Les outils et méthodes présentés ci-après le sont de manière synthétique et introductive. Ils visent à sensibiliser le public de ce guide aux bonnes pratiques en la matière et ne doivent pas limiter les parties intéressées au seul contenu proposé ici. **Des références** pour approfondir la méthodologie ou les perspectives sont proposées en fin de document.

Les définitions de stratégie de sûreté sont laissées à l'appréciation des lecteurs. Les choix en la matière informent naturellement la conception et la mise en œuvre des POS et des PC. Ce guide a été rédigé en gardant à l'esprit la flexibilité nécessaire pour fournir un socle commun à une grande diversité d'acteurs.

Les interventions en zone orange ou rouge sont par nature soumises à un plus grand nombre d'**aléas** que dans des environnements plus stables. Pour en tenir compte, les lecteurs sont invités à **mener des revues régulières** de leurs analyses, POS et PC, sur des cycles annuels au plus. Enfin, l'attention de tous est attirée sur l'importance de quantifier correctement les budgets associés à la mise en œuvre effective d'un plan de sûreté.

ATTENTION

Les **différences de genre** se traduisent par des différences notables en termes d'exposition aux menaces, de profils de vulnérabilités et de mesures d'atténuation des risques. Il est **vivement recommandé** de concevoir, rédiger et mettre en œuvre les plans de sûreté avec **des équipes mixtes**, afin que la diversité des enjeux de sûreté soit analysée et anticipée le plus correctement possible.

1. ORGANISATION GENERALE DE LA SURETE

L'organisation générale de la sûreté peut varier grandement d'une organisation à l'autre. En fonction de la taille, des postes spécifiques peuvent être créés ou, à l'inverse, des missions peuvent s'insérer dans un périmètre de responsabilités plus large.

Dans tous les cas, des responsabilités claires existent au niveau international (siège), national (agence ou mission) et local (lieu de l'exécution du projet). Les lignes de communication entre les différents niveaux de responsabilité sont claires, formalisées et l'ensemble du personnel connait la personne à qui se référer en cas de besoin.

Niveau	Tâches principales
International (Siège)[2]	Une politique de sûreté est en place. Un plan de gestion des crises est en place, disséminé aux personnes pertinentes, qui sont formées à son utilisation et qui composent la Cellule de Gestion de Crises (CGC). Une personne est en charge des aspects administratifs de la sûreté (assurances, notamment pour risques médicaux). Un ou plusieurs référents sont clairement identifiés pour fournir un appui aux équipes à l'échelon national en matière de sûreté.
National (Agence, Bureau ou Mission)	Un plan de sûreté est en place. Les responsabilités en matière de sûreté sont claires et connues de tous : chacun sait qui a autorité pour valider les mouvements, pour décider d'une relocalisation ou d'une suspension temporaire des activités. Un plan de gestion des incidents est en place, disséminé aux personnes pertinentes, qui sont formées à son utilisation et qui composent la Cellule de Gestion d'Incidents (CGI). Une personne est en charge d'entretenir un réseau de veille auprès des interlocuteurs pertinents pour assurer une mise à jour continue des menaces spécifiques. Elle entretient les appuis pertinents pour soutenir les équipes le cas échéant (par exemple auprès des autorités, d'une ambassade ou autres en cas d'hibernation ou d'évacuation). Une personne veille à ce que l'équipement (matériel roulant, matériel de communications, kits médicaux, etc.) nécessaire à une gestion de la sûreté soit disponible, et à ce qu'il soit correctement entretenu.
Local (Projet)	Un plan de sûreté local est en place. Une personne est en charge d'entretenir un réseau de veille auprès des interlocuteurs pertinents pour assurer une mise à jour continue des menaces spécifiques. Elle entretient les appuis pertinents pour soutenir les équipes le cas échéant (par exemple auprès des autorités municipales et traditionnelles, les autres organisations présentes, etc.)

[2] Toutes les références au niveau international ne sont bien évidemment applicables qu'aux entités internationales

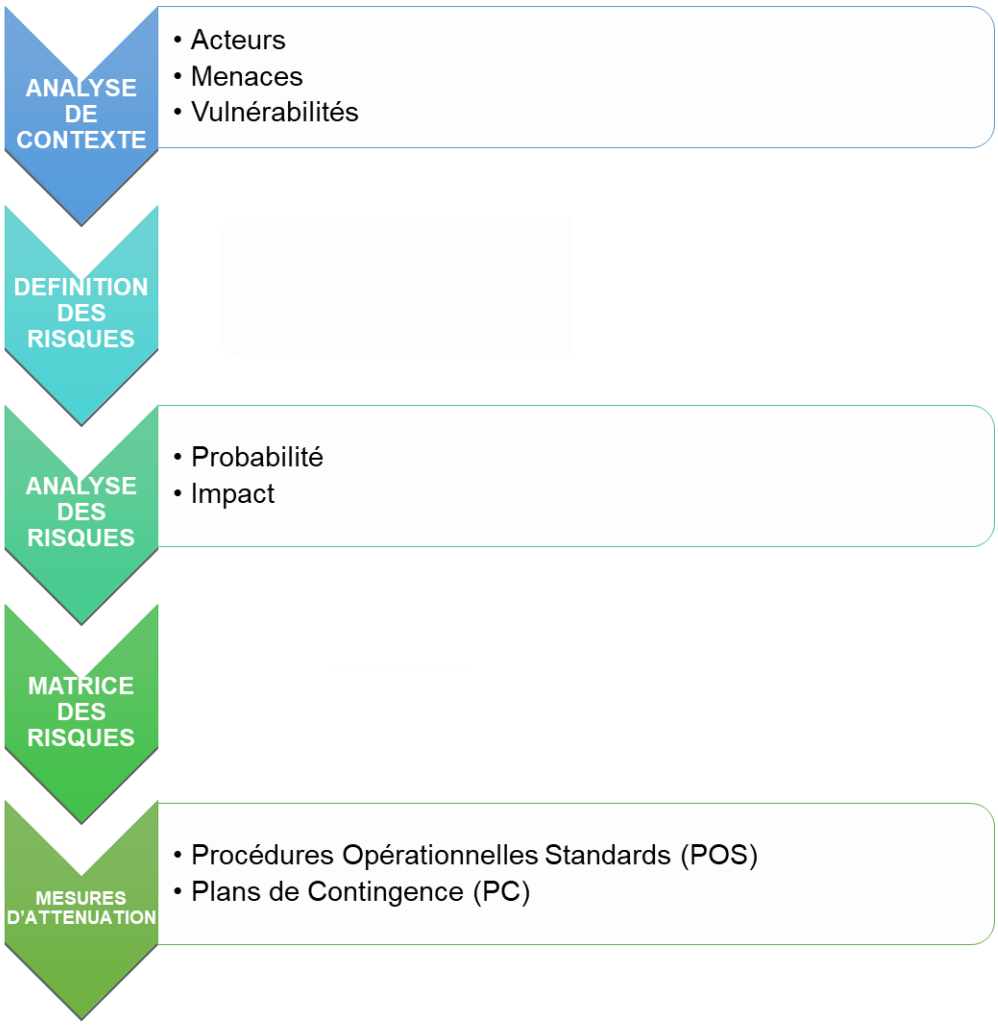
2. ANALYSE SURETE ET MENACES

La définition de mesures adaptées aux risques encourus demande de définir ceux-ci avec précision et de les hiérarchiser. A cette fin, il faut engager une analyse de contexte, dont le but est de mieux cerner les menaces autour de l'environnement du projet, et les menaces auxquelles celui-ci expose l'organisation. Le graphique ci-dessous récapitule les principales étapes de la définition d'un plan de sûreté, qui consistent en :

- Une analyse du contexte ;
- Une analyse des risques ;
- Des mesures d'atténuation de l'impact et de la probabilité de chaque risque associé.

Tous ces éléments doivent idéalement figurer dans le plan de sûreté.[3]

[3] Le graphique ci-dessus est issu de : 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. Communément appelé GPR8 v 2010, il est disponible en français à l'adresse suivante : https://odihpn.org/wp-content/uploads/2011/03/GPR8_revised_edition_French.pdf



2.1. L'ANALYSE DE CONTEXTE

Comprendre le contexte

L'analyse de contexte est le préalable à toute analyse des risques. Elle permet de situer les acteurs, les menaces et les vulnérabilités qui façonnent les risques auxquels l'organisation est susceptible d'être exposée.

Tout plan de sûreté doit présenter le contexte de manière plus ou moins détaillée, chaque organisation étant libre d'agencer cette section en fonction de ses objectifs, mais il est toujours nécessaire de décrire les principaux points suivants :

Sujet	Caractéristiques
Aspects humains	Démographie, ethnicité, peuplement (urbain/rural, migrations économiques, déplacement), mode de vie (agriculteurs et pastoralistes), langues véhiculaires et locales, etc.
Géographie	Le terrain et les ressources, en particulier eau et énergie
Histoire	Principales étapes de la formation de l'ensemble politique et social du pays considéré et, idéalement de la zone considérée

Politique	Développements politiques ayant une incidence sur la situation : Echéances électorales Enjeux politiques (réforme agraire, code de la nationalité, réforme de la constitution)
Politique étrangère	Insertion dans les ensembles régionaux Commerce extérieur Partenariats stratégiques et systèmes d'alliance Enjeux stratégiques
Situation économique et sociale	Structure de l'économie (primaire, secondaire et tertiaire) PIB/habitant, salaire moyen, emploi, taux d'alphabétisation, etc. Système de santé
Conflictualité	Description du ou des principaux conflits (le cas échéant) : Acteurs Enjeux Aspects idéologiques Aspects économiques du conflit

L'analyse de contexte demande à être régulièrement revue, idéalement tous les ans, parfois plus en fonction de développements soudains.

Etapes clefs de l'analyse de contexte

1. **Revue documentaire** : Cette phase consiste à recueillir, analyser et synthétiser le plus d'informations disponibles sur le pays et la zone d'intervention. Média (en particulier presse et radio), sources électroniques, sites spécialisés et revues universitaires peuvent fournir un matériel considérable susceptible d'étayer la construction d'un questionnaire le plus fin possible pour les étapes suivantes.

2. **Enquête hors du pays d'intervention** : Idéalement structurée par une recherche documentaire solide, il est possible d'entrer en contact avec plusieurs types d'organisations ayant une connaissance de la zone de projet. Ce peuvent être les représentations diplomatiques, les centres de recherches universitaires, les think tanks, les organisations internationales ou non-gouvernementales.

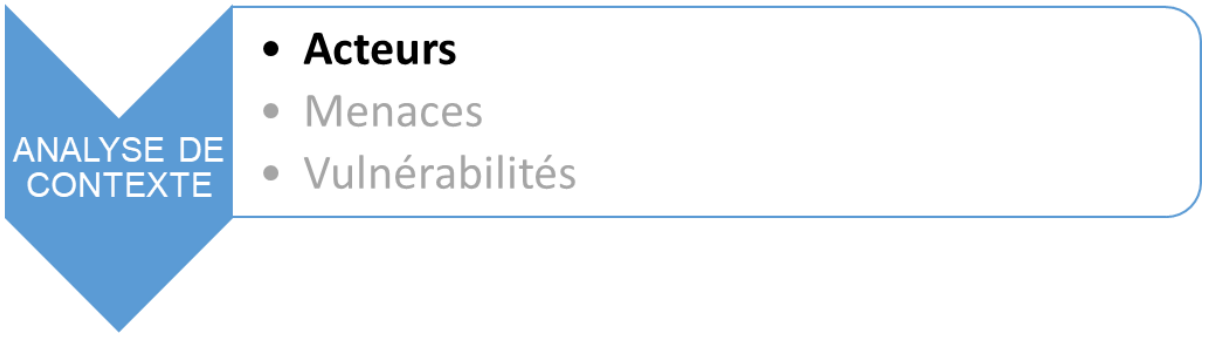
3. **Enquête de terrain en capitale** : S'appuyant sur les travaux précédents, l'enquête de terrain permet de recueillir l'analyse de plusieurs types d'intervenants : autorités gouvernementales, organismes (national et international) actifs dans/ou autour la zone de projet, et permettant d'aussi d'aiguiller des entretiens vers le monde de l'entreprise (prestataires logistiques, notamment). La recherche universitaire nationale ainsi que les acteurs de la société civile sont des ressources clefs et souvent oubliées de cette étape.

4. **Enquête de terrain sur le site du projet** quand cela est possible. En conclusion du processus, ce travail permet d'entrer en contact avec les acteurs locaux actifs sur la zone de projet, comme par exemple les autorités locales (Préfecture, Municipalité, etc.) ou traditionnelles (Sultanat, Lamidats, Chefferies, etc.), et les représentants locaux de la société civile (ONG, Centres de Recherche et Universités, etc.). Le secteur privé est également source d'informations non négligeables. Il est enfin, dans certains cas, nécessaire d'entrer directement en contact avec des acteurs armés.

ATTENTION

Il peut se révéler impossible de se rendre sur le terrain avant la soumission. Il est toutefois indispensable d'avoir conclu les deux premières étapes pour renseigner les éléments clefs du plan de sûreté à ce moment.

L'analyse des acteurs



La première étape de l'analyse de contexte consiste à identifier les acteurs de votre environnement. Ceux-ci peuvent être de plusieurs types, dont le tableau suivant donne une liste non exhaustive :

	Type	Exemples
Acteurs armés	Forces armées régulières du pays d'intervention	L'armée nationale, les forces de police ou autres forces officielles.
	Milices	Les Mayi Mayi en République Démocratique du Congo ou les Kamajohs en Sierra Leone.
	Compagnie de Sécurité Privée (CSP)	Les groupes chargés de la sûreté des sites sensibles dans le delta du Niger. Les compagnies chargées de la sûreté des lieux de vie à Nairobi.
	Groupes d'Opposition Armés (GOA)	Groupes organisés politiquement et militairement, contestant par les armes l'autorité du gouvernement au niveau local ou national.
	Autres	Katibas familiales en Syrie. Organisations criminelles et terroristes. Petite criminalité non organisée (par exemple en milieu urbain).
Acteurs non-armés	Autorités gouvernementales	Ministères, administrations centrales et déconcentrées / décentralisées
	Autorités traditionnelles	Sultanat dans le Kanem au Tchad
	Autorités locales	Les chefs de camp dans des camp de personnes déplacées internes
	Populations résidentes	Différents groupes ethniques co-existant dans un même milieu (rural ou urbain).
	Populations déplacées	Groupes déplacés en Irak depuis la province de Ninive vers le Kurdistan Irakien.

Chacun de ces acteurs a un mode opératoire et une organisation distincts (et parfois pas d'organisation clairement identifiables, comme c'est souvent le cas pour la petite criminalité, par exemple). Identifier ces deux aspects permet de clarifier les autorisations ou réassurances éventuelles qu'il convient d'obtenir, et de spécifier les menaces que représentent spécifiquement certains de ces groupes dans votre environnement. Jauger d'un mode opératoire, des intentions et des capacités d'un acteur permet d'évaluer si une menace liée à cet acteur est crédible, et donc probable, ou non.

Tous ces groupes ont des intentions plus ou moins claires, et disposent de moyens plus ou moins importants. Les intentions concernent leurs objectifs. Ceux-ci peuvent être élémentaires (survie pour le cas des populations déplacées), difficiles à cerner (dans le cas de groupes hétérogènes, où les objectifs sont contestés en interne) ou très clairs (par exemple, l'ambition affichée par certains groupes de kidnapper les ressortissants de certaines nationalités).

De même, les moyens dont disposent ces différents groupes sont très variables. Certains groupes armés (GOA) peuvent-être tout à fait sous-équipés ou, au contraire, disposer des ressources humaines qualifiées pour exploiter un arsenal important, que celui-ci soit militaire, administratif ou autre.

La mise en regard des intentions et des moyens des différents acteurs permet d'évaluer le degré de menace que chacun peut représenter. Un groupuscule peu armé et sans hostilité affichée pour des opérateurs représente une faible menace pour ceux-ci. A contrario, un GOA aux ambitions résolument hostiles et à la capacité démontrée de mener des opérations léthales et complexes constitue une très forte menace.

Intentions et moyens peuvent évoluer très rapidement au gré de recadrages idéologiques, des combats ou d'autres facteurs. C'est pourquoi il convient d'évaluer ces deux aspects de manière dynamique autant que faire se peut. Il est possible de mobiliser pour ce faire :

- Ressources diplomatiques (conseils aux voyageurs des différentes ambassades) ;
- La presse nationale si celle-ci est accessible, la presse internationale spécialisée ;
- Les sites spécialisés (recherche universitaire, think tanks)
- Les contacts avec des organisations présentes sur place.

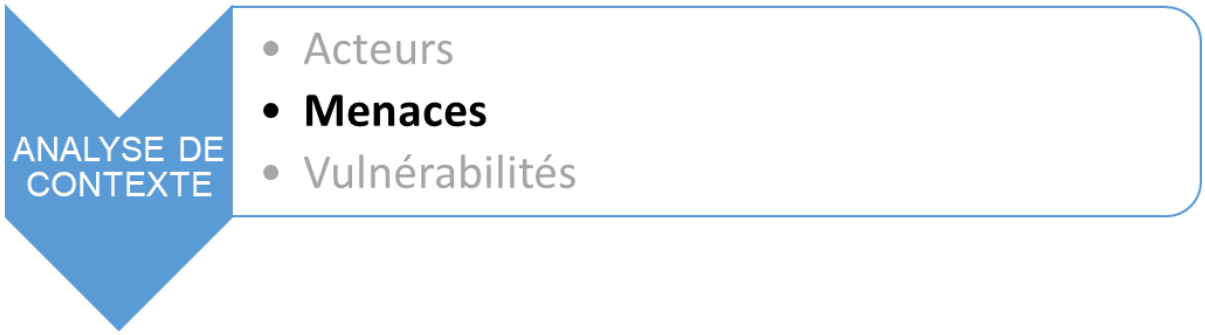
Une fois consolidés, et en vue de préparer la matrice des risques, ces éléments peuvent se synthétiser par grandes catégories, dont le tableau page suivante fournit un exemple. Les catégories mentionnées sont génériques et le lecteur est libre de les adapter en fonction de ses besoins. Pour chaque catégorie, un indicateur est défini sur une base de 1 à 5, allant d'un environnement paisible (niveau 1) à une haute intensité de menaces (niveau 5).

	Conflit	Troubles	Militantisme	Criminalité
Description du niveau de sûreté	1- Pas de conflit armé depuis plus de 10 ans et/ou problèmes liés au conflit résolus	1- Pas de tension socio-politique	1- Pas de dissidence armée dans le pays	1- Les crimes violents sont très rares
	2- Pas de conflit armé depuis plus de 5 and et/ou questions sur les accords de paix	2- Troubles localisés avec violence occasionnelle	2- Présence de dissidents armés dans le pays mais pas dans les zones d'intervention	2- Les crimes violents sont limités à des zones précises
	3- Conflit de basse intensité en cours et/ou tensions dans les relations régionales	3- Troubles réguliers avec violence occasionnelle	3- Des groupes armés lancent des attaques contre des intérêts locaux ou étrangers	3- Les crimes violents ne ciblent que les nationaux
	4- Conflit de haute intensité sans sortie de crise en vue	4- Troubles soutenus avec violences systématiques et impact sur la stabilité locale	4- Des groupes armés ciblent indirectement les civils et/ou le système d'aide humanitaire. Les négociations d'accès restent possibles.	4- Les crimes violents ciblent les nationaux et parfois les étrangers
	5- Conflit armé de haute intensité	5- Guerre civile ou coup d'Etat	5- Des groupes armés ciblent directement les civils et/ou le système d'aide. Les négociations d'accès sont impossibles.	5- Criminalité violente généralisée.

	Environnement	Administratif	Genre	Infrastructure
Description du niveau de sûreté	1- Très peu de risques environnementaux et/ou très bonnes infrastructures d'urgence	1- Bonne coopération entre organisations et gouvernement, sans restriction d'accès par d'autres acteurs	1- Le contexte permet une liberté de vie quel que soit le genre ou l'orientation sexuelle.	1 - L'électricité, le transport, les communications et les services de santé sont de qualité et rarement interrompus.
	2- Risques environnementaux localisés et/ou infrastructures d'urgence acceptables	2- Les organisations peuvent opérer librement avec des restrictions limitées.	2- Le contexte permet une liberté de vie relative.	2 - L'électricité, le transport, les communications et les services de santé sont de qualité acceptable et sont interrompus de temps en temps.
	3- Risques environnementaux périodiques ou saisonniers et/ou infrastructures d'urgence faible	3- Les organisations sont limitées à certaines zones ou font face à des résistances de la part des communautés. Le gouvernement peut mettre en place des restrictions.	3- Le contexte est défini par des rôles prescriptifs pour les genres, avec une tolérance implicite pour la diversité.	3 - L'électricité, le transport, les communications et les services de santé sont fréquemment interrompus et ont un niveau de sûreté faible.
	4- Risques environnementaux réguliers et/ou infrastructures d'urgence limitées	4- Les opérations font face à une hostilité claire. Certaines organisations sont ciblées par des groupes militants. Le gouvernement peut menacer d'expulsion.	4- Le contexte est conservateur et défini par des rôles prescriptifs pour les genres, avec une tolérance très limitée pour la diversité.	4- L'électricité, le transport, les communications et les services de santé sont de faible qualité. Les coupures ou disruptions sont fréquentes.
	5- Risques environnementaux majeurs et/ou pas d'infrastructures d'urgence	5- Les organisations ne peuvent pas intervenir de façon sûre et les opérations ne sont pas durables. Le gouvernement est hostile et des organisations peuvent être ciblées directement.	5- Le contexte est très conservateur et la diversité n'est pas acceptée.	5- L'électricité, le transport, les communications et les services de santé sont sévèrement dégradés ou inexistants

L'analyse des menaces

Le plan de sûreté doit inclure un bref narratif pour les principales menaces identifiées, en indiquant pour chacune les indications pertinentes (zones à risque, personnes à risque, mode opératoire).



Dans le cadre de la revue documentaire, un travail préalable consiste à identifier les menaces les plus prévalentes sur la zone d'intervention, en s'appuyant notamment sur les ressources mentionnées précédemment.

En lien avec la table des niveaux (voir. p.17-18), et aussi en vue de préparer la matrice des risques, le tableau page suivante propose une liste non exhaustive de menaces associées à chaque catégorie, auxquelles il est possible d'être confronté dans les environnements à sécurité dégradée.

	Conflit	Troubles	Militantisme	Criminalité	Environnement	Administratif	Genre	Infrastructure
Exemples de Menaces	Frappes aériennes	Manifestations	Attaques suicides	Cambriolages	Tremblements de terre	Restrictions sur les visas	Viol	Réseau de communication insuffisant
	Tirs d'artillerie / mortier	Mouvements de foule	Explosifs improvisés ciblés	Vol	Morsures ou attaques d'animaux	Interférence	Harcèlement ou agression verbale	Structures médicales insuffisantes
	Tirs-Croisés	Emeutes	Tirs d'artillerie / mortier	Vol à main armée	Problèmes électriques	Diversion de l'aide	Harcèlement ou agression physique	Etat des routes dégradé
	Mines et UXOs	Pillages	Embuscades	Banditisme	Incendie (accidentel)	Fraude / Corruption	Discrimination	
	Embuscades	Coup d'Etat	Arrestation / Détention / Interrogation	Car-jacking	Incendie (naturel)	Ciblage direct	Intimidation	
	Pièges improvisés		Kidnapping	Incendie volontaire	Epidémies	Menaces ou intimidation	Chantage	
	Points de contrôle		Explosifs improvisés indirects	Kidnapping	Climat extrême	Harcèlement / agression	Harcèlement (en ligne ou non)	
	Tirs directs et ciblés		Raids armés	Meurtre	Maladies	Restrictions d'accès ou de voyage	Harcèlement non-verbal	
	Arrestation / détention /		Violences sexuelles	Enlèvement	Accident de circulation	Chantage	Lynchage	
	Raids armés		Menace directe	Fraude / corruption	Crash aérien	Surveillance (online ou non)	Restrictions	
			Enlèvement		Inondation	Arrestation / Détention /	Enlèvement	
							Arrestation / Détention /	

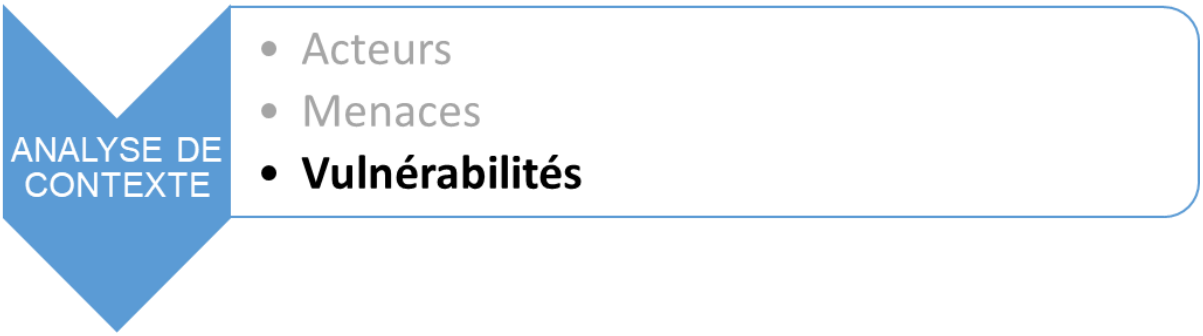
ATTENTION

Il faut distinguer menaces internes et menaces externes. Ces dernières sont localisées dans l'environnement et sont indépendantes de l'activité liée à un projet. La petite criminalité est par exemple endémique dans certains lieux. Les menaces internes sont en revanche liées aux organisations chargées de la mise en œuvre d'un projet, dont la présence peut engendrer une insécurité inconnue auparavant dans votre lieu d'intervention. L'arrivée de véhicules à quatre roues motrices dans un contexte où ils représentent une nouveauté peut par exemple faire apparaître du brigandage sur les axes routiers. Plus finement, il convient de veiller aux menaces induites par toute présence nouvelle. A titre d'illustration, dans certains endroits, la politique de recrutement local doit veiller à respecter les équilibres entre différents groupes locaux. La surreprésentation de l'un de ces groupes pourrait attiser les tensions communautaires et attirer une attention malvenue sur l'organisation.

Une fois les 8 à 10 menaces les plus probables identifiées, il importe de les appréhender plus finement en précisant pour chaque menace comment elle se réalise. Le tableau suivant présente les principales questions à se poser pour chaque menace, avec des exemples en illustration.

Question	Exemple
- Y a-t-il un historique ou une chronologie disponible pour chaque menace permettant de cerner certains aspects (par exemple des quartiers connus pour abriter la petite criminalité, des axes routiers à forte incidence d'accidents, etc.)	Les favelas au Brésil ou les bidonvilles à Nairobi sont connus pour leur précarité et la prévalence du petit banditisme (braquage à main armée). Dans certaines villes, la proximité des gares ferroviaires ou routières est aussi un lieu de petit banditisme (vol à la tire, pickpockets).
- Quelles-sont les cibles visées pour chaque menace ? S'agit-il de groupes, de personnes isolées avec un profil spécifique (genre, nationalité, orientation sexuelle, richesse apparente), etc.	Dans certains contextes, les menaces connues et répétées contre du personnel de certaines nationalités (pays d'Amérique du Nord et Europe de l'Ouest) ont conduit des organisations y affecter leur personnel de type non caucasien. Dans certains pays d'Afrique Centrale et de l'Est, la communauté LGBTQ fait l'objet d'une défiance inhabituelle les exposant à des menaces élevées de violence physique. Toute richesse ostentatoire est en général susceptible d'attirer une attention malveillante.
- Quel est le mode opératoire connu des acteurs de la menace ?	Dans certains pays, des malfaiteurs se jettent volontairement contre les véhicules dans lesquels circulent du personnel d'ONG. Compte tenu des stratégies de sûreté de celles-ci, identifiées et comprises par les malfaiteurs, l'objectif est de forcer les ONG à fournir une indemnisation rapide, dans ce qui s'apparente à une forme d'extorsion. Dans d'autres pays, la présence d'un homme ciblé pour différentes raisons (richesse, appartenance au personnel diplomatique ou décisionnaire d'une

	grande entreprise) peut exposer celui-ci à être drogué pour ensuite lui dérober ses biens.



Que des menaces existent ne veut pas dire qu'on y est exposé. A titre d'illustration, le risque pour une voiture d'être attaquée par des « coupeurs de routes » sur un axe routier (la menace) est fonction de la fréquence avec laquelle la voiture circule (la vulnérabilité). L'absence de tout déplacement correspond à une vulnérabilité nulle, une haute fréquence de déplacements à une vulnérabilité élevée.

L'analyse des menaces permet de comprendre les facteurs de vulnérabilité, en distinguant ceux sur lesquels il est possible d'avoir un élément de contrôle de ceux sur lesquels cela est impossible. En regard des menaces identifiées, le plan de sûreté doit indiquer les facteurs internes et externes de vulnérabilité.

Certains facteurs de vulnérabilité sont propres au contexte considéré et sont hors de contrôle. La présence de groupes armés en est une illustration. D'autres en revanche sont susceptibles d'aménagement. Dans les contextes ou certaines nationalités ou certains types physiques sont plus particulièrement ciblés (ressortissants français ou américains dans certaines régions du Moyen-Orient ou du Sahel, type caucasien au Yémen), il importe d'identifier la vulnérabilité, qui peut être neutralisée par des mesures de recrutement spécifiques à la zone concernée.

Un examen de l'historique des incidents, localisation, cibles, peut permettre de mettre à jour et de différencier ces types de vulnérabilités, dont le plan de sûreté doit faire mention en préalable à la définition ultérieure des mesures d'atténuation.

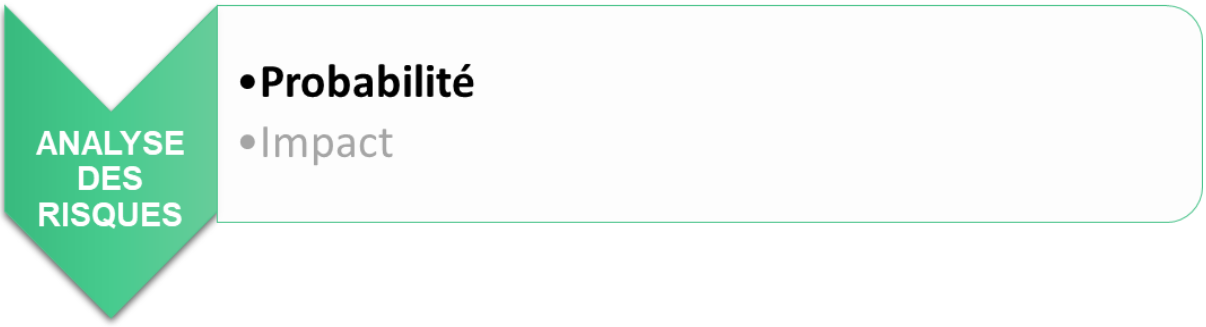
2.2. L'analyse des risques

ATTENTION

C'est cette analyse des risques qui devra être intégrée dans la proposition élaborée en réponse à un APCC.

La combinaison des menaces et des vulnérabilités se traduit en risques. La présence de mines (menace) sur des axes routiers empruntés par une organisation avec des moyens inadaptés (vulnérabilité) peut mener à l'explosion du véhicule, avec pour conséquences des dommages importants aux personnel et aux biens de l'organisation, voire à sa réputation (risques). L'analyse des risques consiste à identifier les risques età les hiérarchiser. Cette analyse permettra ensuite, dans la phase suivante et au sein d'une matrice des risques (point 3.), de dégager des mesures d'atténuation adaptées. La matrice des risques n'a pas à être intégrée à l'APCC.

Probabilité



La probabilité se mesure sur l'échelle de 1 à 5, allant du moins probable au plus probable. Elle s'évalue sur un horizon temporel défini, en général d'un an, parfois moins en fonction de la volatilité du contexte. A titre d'illustration, quand le pouvoir est contesté, la probabilité de manifestations violentes est plus élevée autour d'échéances électorales (campagne, organisation du scrutin, dépouillement et proclamation des résultats). Cette probabilité est moins forte en dehors de ces échéances.

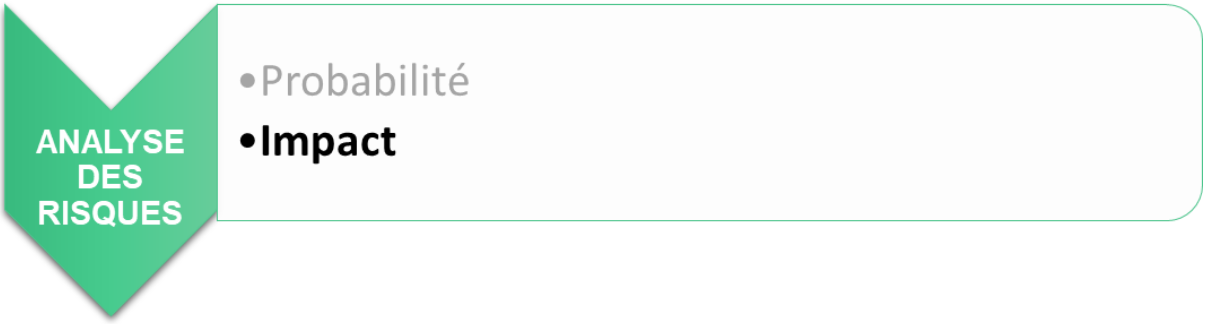
De manière importante, si certains risques sont à probabilité constante sur une période relativement importante, comme le paludisme dans certaines régions, d'autres peuvent évoluer au gré des développements politiques, sociaux, économiques ou militaires. Il convient ainsi de préciser quand le risque est saisonnier, comme la petite criminalité en période de soudure, c'est-à-dire dans la période quand s'épuisent les réserves alimentaires en attendant les prochaines récoltes, et qui correspond aux cycles agricoles. Plus généralement, il est important de mettre à jour l'analyse des risques de manière régulière – de 6 mois à un an dans des contextes à sécurité dégradée, pour tenir compte de l'apparition – voire de la disparition – de certains risques au fil du temps.

Le tableau suivant propose une méthodologie plus détaillée pour assigner la probabilité de survenance à un risque spécifique.

Probabilité	Définition	*Intention* *Capacité* *(Voir p. 15)*		Historique	Niveau
Très improbable	L'évènement est considéré comme n'ayant pas de probabilité réaliste de se produire.	Inconnue	Aucune	N'est jamais arrivé au cours des 12 derniers mois.	1
Improbable	L'évènement est considéré comme ayant une probabilité raisonnable de se produire.	Potentielle	Faible	S'est rarement produit au cours des 12 derniers mois.	2
Possible	L'évènement est considéré comme ayant une probabilité moyenne de se produire.	Possible	Modérée	S'est produit quelques fois au cours des 12 derniers mois.	3
Probable	L'évènement est considéré comme ayant une très forte probabilité de se produire.	Probable mais non explicite	Notable	S'est produit à de multiples occasions au cours des 12 derniers mois.	4
Très probable	Il est attendu que l'évènement se produise.	Volonté affirmée	Forte	S'est produit régulièrement au cours des 12 derniers mois.	5

En dehors des risques naturels, il convient de préciser les menaces associées à la présence de groupes armés, de la petite criminalité aux GAO. Les notions d'intention et de capacité reprises dans ce tableau font référence aux concepts présentés dans l'analyse des acteurs p.15.

Impact



L'impact se mesure également de 1 à 5, allant du moins au plus impactant. L'impact se mesure en prenant en compte les éléments suivants :

- Impact sur les personnes (maladies, agressions physiques, agressions laissant des traumas physiques ou psychologiques, décès) ;
- Impact sur les biens (vols d'argent, d'intrants, de véhicules, etc. ; destruction de biens, pillage, etc.) ;
- Impact sur les activités (allant de la suspension temporaire à l'arrêt indéfini) ;
- Impact sur la réputation (entraînant par exemple une perte de clientèle, une suspension de l'exécution, des poursuites judiciaires, etc.).

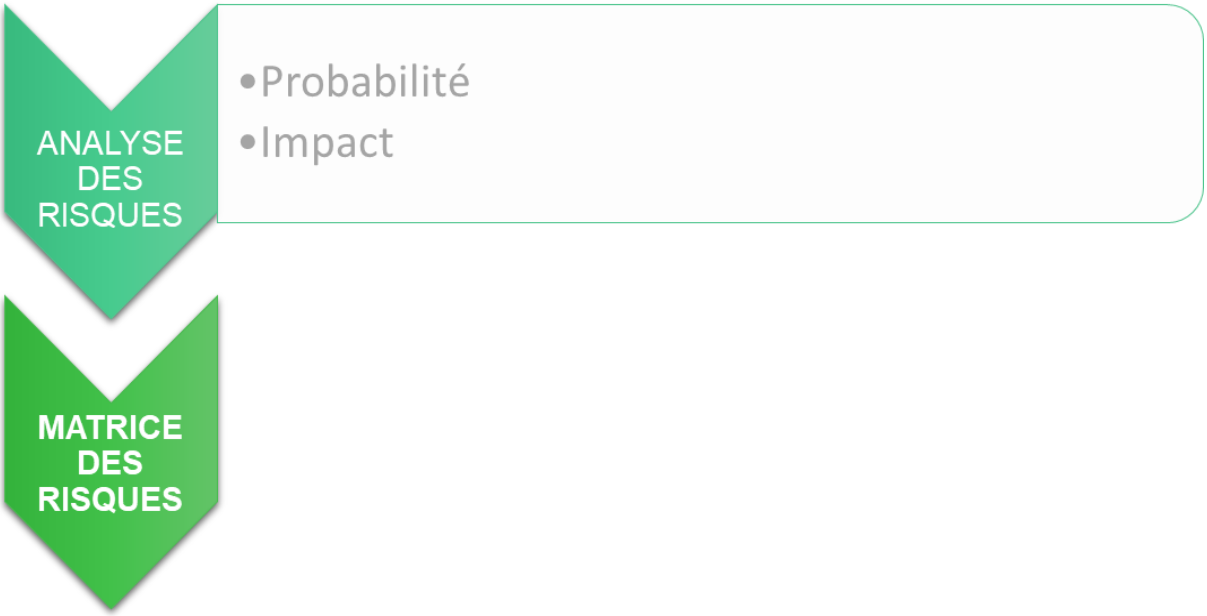
ATTENTION

En général, un impact élevé combine un ou plusieurs de ces éléments. Un cambriolage en bande organisée peut par exemple avoir un impact sur les personnes (blessures) et sur les biens (argent et matériel dérobé). Une exception est le kidnapping : indépendamment de toute combinaison, sa survenance qualifie directement l'impact à son niveau plus élevé et implique la mise en place d'une cellule de crise.

Le tableau suivant propose une méthodologie plus détaillée de l'assignation de l'impact à un risque spécifique.

Impact	Personnes	Biens	Programmes	Réputation	Niveau
Négligeable	Pas de blessés	Pas de dégâts	Perturbations mineures	Négligeable	1
Mineur	Blessures légères/stress possible	Possibles dégâts ou pertes	Retards limités	Localisé et limité	2
Modéré	Blessures non mortelles/stress élevé	Quelques pertes	Retards	Localisé et étendu	3
Majeur	Blessures graves/traumatisme	Perte importante	Perturbations graves	À travers tout le pays et limité	4
Critique	Blessures handicapantes/décès	Perte majeure ou complète	Suspension des activités	À travers tout le pays et étendu	5

3. LA MATRICE DES RISQUES



La matrice des risques est un document de synthèse qui :

- Reprend l'analyse de contexte et l'analyse des risques,
- Assigne des valeurs quantitatives aux risques (probabilité et impact)
- Dégage les lignes principales des mesures d'atténuation (de probabilité et d'impact)
- Evalue le risque résiduel une fois ces mesures mises en œuvre.

Les tableaux pages suivantes donnent un format possible de matrice des risques, avec quelques précisions en complément des points abordés précédemment.

Étape	*1*	*2*	*3*	*4*
#	**CONTEXTE**			
	Catégorie	**Indicateur**	**Description**	**Menace**
1	***Conflit***	***3- Conflit de basse intensité en cours et/ou tensions dans les relations régionales***	*Depuis le 15 mars 2013 plusieurs GOA sont présents dans la Région de YYY, où est déployée la Mission des Nations Unies. Les attaques sont particulièrement violentes à l'Ouest et au Sud, du fait de la forte concentration des Groupes Armés*	***1.1. Tirs Croisés***
				1.2.
				1.3
				1.4
				1.5
2	**Trouble**			
3	**Militantisme**			
4	**Criminalité**		-	
5	**Environnement**			
6	**Administratif**			
7	**Genre**			
8	**Infrastructure**			

Etape 1 : Les catégories données ici sont génériques et le lecteur est libre de les reprendre à son compte ou de les adapter. Les éléments en italique sont donnés à titre illustratif et sont fictifs.
Etape 2 : Mentionner l'indicateur de niveau correspondant à la catégorie.
Pour les deux premières étapes, les tableaux p.16-17 fournissent une référence.
Etape 3 : La description correspond à l'indicateur. L'exemple fictif donné ici synthétise les informations clefs issues de l'analyse de contexte.
Etape 4 : Les menaces ne doivent pas être présentées de manière détaillée. Des intitulés génériques sont fournis p. 19.

Étape	*5*	*6*	*7*	*8*		*9*
Menace (cf. *Etape 4*)	**QUALIFICATION DU RISQUE**			**EVALUATION DU RISQUE BRUT**		
	Description (auteur, causes, motivation, lieu, temps…)	**Vulnérabilité Spécifique**	**Risque**	**Probabilité de 1 à 5**	**Impact de 1 à 5**	**Niveau de Risque de 1 à 25**
1.1. Tirs Croisés	*Dans les zones d'intervention d'XXX à YYY des tirs entre les GOA et l'armée régulière sont toujours possibles. Des tensions inter communautaires fortes existent entre les communautés pastorales et agricultrices.*	*Les zones d'XXX et d'YYY sont prioritaires pour la bonne marche du projet. L'exécution de l'opération y impose des mouvements fréquents.*	*Se trouver au moment des affrontements entre les GOA et l'armée régulière, ou au cours d'affrontements intercommunautaires.* *Des balles perdues peuvent atteindre des cibles non visées.*	***3***	***3***	***9***
1.2.						
1.3.						
2						
3						
4		-				
5						
6						
7						
8						

Etapes 5 à 7 : Un court narratif permet de contextualiser la menace et la vulnérabilité, conduisant à l'identification du risque.
Etape 8 : Il faut indiquer ici les indicateurs chiffrés issus des analyses de probabilité et d'impact et synthétisés p. 23 et 24, respectivement.
Etape 9 : L'indicateur de risque brut, c'est-à-dire avant mesures d'atténuation, multiplie simplement l'indicateur de probabilité par l'indicateur d'impact.

Étape	*10*	*11*	*12*		*13*
Menace (*Etape 4*)	**MESURES D'ATTENUATION**		**EVALUATION DU RISQUE RESIDUEL**		
	de la Probabilité	**de l'Impact**	**Probabilité Résiduelle**	**Impact Résiduel**	**Niveau de Risque Résiduel**
1.1. Tirs Croisés	*La fréquence des mouvements est réduite. Tous les mouvements sont validés après consultation des parties prenantes (GOA, Armée, Communautés). Les véhicules sont équipés de moyens de communication redondants (GSM et Satellitaire/ou Radio) et des points réguliers sont faits pendant le mouvement pour réévaluer la situation.*	*Le personnel est équipé de gilets pare-balles. Les véhicules sont équipés avec un « trauma kit » (pansements compressifs, garrots, notamment). Les équipes sont formées à leur usage.*	***2***	***2***	***4***
1.2.					
1.3.					
2					
3					
4	-				
5					
6					
7					
8					

Etape 10 : Des mesures permettant d'atténuer la probabilité de survenance du risque sont mentionnées, et devraient faire l'objet d'un POS détaillé.

Etape 11 : Des mesures permettant d'atténuer l'impact du risque sont mentionnées, et devront faire l'objet d'un PC détaillé.

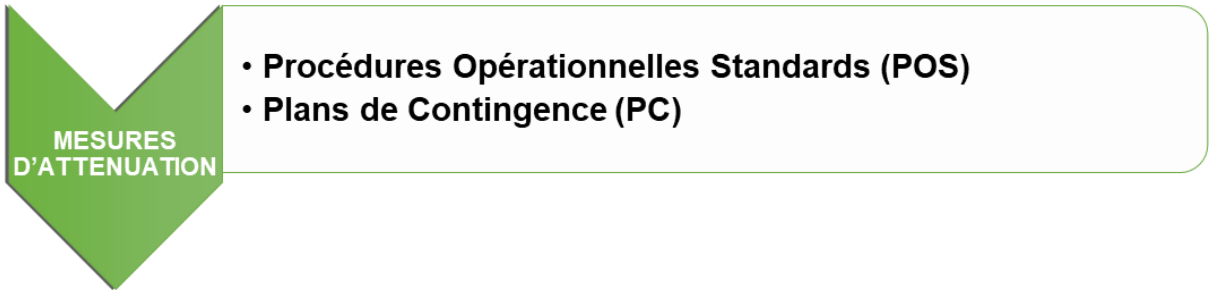
Etapes 12 à 14 : Même procédure que pour les étapes 8 et 9, le résultat final donne le niveau de risque résiduel et permet d'apprécier l'acceptabilité du risque.

ATTENTION

Les étapes 10 et 11 doivent également permettre d'identifier les éléments qu'il faudra inclure dans un éventuel budget dédié à la sûreté.

4. MESURES DE SURETE GENERALES

Une fois les risques spécifiés et hiérarchisés, il devient possible d'identifier les leviers qui vont permettre d'en réduire la probabilité d'occurrence ou l'impact. Les premiers constituent les Procédures d'Opérations Standard (ou POS). Les seconds constituent les Plans de Contingence (PC).



Principes généraux de définition et mise en œuvre

POS et PC obéissent à certains principes généraux

Les mesures d'atténuation sont définies nationalement (capitale et aspects généraux pays) **et localement** (base et aspects spécifiques contexte local).
Dans tous les cas, u**n travail collégial présidant à leur rédaction inclut des équipes mixtes hommes/femmes et National/International**, notamment pour prendre en compte les aspects de genre et les expositions différentes aux risques (par exemple mise en place d'heures de bureau permettant au personnel national de rentrer à domicile en toute sécurité avant la tombée de la nuit).

La diffusion des documents est un point d'attention particulier. Bien qu'en principe ils ne récapitulent que des éléments généraux, ils peuvent être mal interprétés (par exemple menant à des suspicions d'espionnage). La liste de diffusion de chaque plan ou procédure doit être spécifique et viser les personnes clefs concernées. A titre d'illustration, les chauffeurs doivent absolument connaître les POS Mouvements et Communication, mais sont moins concernés par les POS concernant les lieux de vie des expatriés.

Certaines mesures envisagées doivent faire l'objet d'une **formation**, comme par exemple les POS communications si ceux-ci incluent l'utilisation d'équipement spécifique (HF, VHF ou téléphone satellitaire).

Il est recommandé que ces mesures fassent l'objet **d'exercices** réguliers, comme par exemple les POS Sûreté des locaux, dont l'appropriation peut être renforcée significativement par des évacuations des locaux (alerte type sirène ou autres, regroupement au lieu de rassemblement, exercices de lutte anti-feu pour les extincteurs à destination du personnel formé, qui doit être identifié).

De manière très importante, les POS et les PC doivent être **budgétés**, en prenant notamment en compte les éléments suivants (non exhaustif) :

- Achat éventuel d'équipement (radios, extincteurs, etc.)
- La formation du personnel (notamment si celle-ci est externalisée, comme pour les premiers secours ou la lutte anti-feu).

Enfin, les mesures d'atténuation doivent être **mises à jour**, afin de prendre en compte les évolutions du contexte, au même titre que l'analyse des risques. La cyclicité des mises à jour peut varier, mais **il est recommandé de ne pas dépasser plus d'un an entre deux revues, et de l'adapter systématiquement en cas de développements nouveaux** (changements politiques, évolution sensible de l'environnement sécuritaire, etc.).

ATTENTION

Il est possible de recourir à des sociétés spécialisées dans la gestion des risques pour développer tout ou partie des éléments du plan de sûreté présentés ci-dessus. Toutefois, il est fortement recommandé de maintenir un contact régulier avec les prestataires ; et de spécifier dans la soumission si la rédaction du plan a été externalisée, et à quelle organisation.

4.1. MESURES DE SURETE PREALABLES

La construction et la mise en œuvre du plan de sûreté dans le pays et la zone d'intervention permettent d'alimenter les procédures de préparation au départ pour le personnel expatrié. Les éléments suivants constituent des recommandations standard et ne sont pas destinés à être inclus dans le plan de sûreté en tant que tels, bien qu'ils puissent y être mentionnés.

Avant le départ, il convient d'arbitrer sur l'ouverture du poste à un statut familial ou non, et le personnel concerné doit en être avisé au cours de la proposition de poste.

Il est indispensable de veiller à ce que tout le personnel expatrié ait **consulté un médecin** avant le départ, ait son **carnet de vaccination à jour**, et soit informé des principales règles en matière d'hygiène et de santé dans le pays de destination.

Avant le départ, le référent sûreté au siège doit donner un **briefing sûreté individualisé** à la personne concernée, visant à l'informer a minima :

- De la politique de sûreté de l'organisation ainsi que des rôles et responsabilités.
- De la situation sûreté générale dans le pays et particulière à la zone d'intervention, en présentant les risques analysés et les mesures d'atténuation mises en œuvre ;
- Des règles de comportement en vigueur ;
- De l'importance de s'enregistrer localement auprès de son ambassade ou consulat de rattachement (procédure ARIANE pour la France et équivalents) ;
- Du plan de sûreté, dont une version complète ou spécifique au poste doit lui être remise ;
- Des procédures d'accueil à l'arrivée.

Il est de plus recommandé de proposer **une formation en sûreté personnelle ainsi qu'une formation de premier secours** à tout le personnel étant appelé à se déplacer en zone orange ou rouge.

Immédiatement **à l'arrivée, le référent sûreté dans le pays d'intervention doit donner un briefing détaillé à la personne concernée**, qui approfondit les points évoqués ci-dessus. Une visite guidée de la ville, des bureaux et des lieux de vie est également recommandée. De plus, il convient de lui remettre :

- **Une enveloppe de sûreté**, à garder par devers soi, destinée à être employée face à la petite criminalité, et dont l'usage vise à désamorcer toute agression rapidement. L'enveloppe peut également être utilisée en d'autres circonstances (recours à un mouvement d'urgence, par exemple).
- Un document plastifié de petit format (taille d'une carte de crédit s'insérant aisément dans une poche), traditionnellement appelé **« compagnon constant »** et récapitulant les principaux contacts en cas d'urgence (dans l'organisation pays et siège, numéros utiles y compris services médicaux) ainsi que le numéro de la police d'assurance en vigueur pour les évacuations médicales le cas échéant.
- Un **équipement téléphonique adapté** comprenant les contacts d'urgence pré enregistrés.

4.2. PROCEDURES OPERATIONNELLES STANDARD

POS indispensables

Il peut y en avoir beaucoup selon les contextes. Les POS les plus importants – **et qui doivent absolument figurer dans le plan de sûreté**, sont récapitulés dans le tableau suivant :

POS	Commentaires
Mouvements	Procédures de validation des mouvements, détermination du chef de bord, équipement indispensable à la sûreté et à la sécurité du mouvement, respect des limitations de vitesses, etc.;
Communication	Fréquence des contacts, identification des interlocuteurs, nature du contact (point de situation, etc.), modalités des contacts (e-mails, réseau cellulaire, etc.).
Mesures de sécurité personnelle, comportement et attitude	Préparation d'un « grab bag », enveloppe de sûreté personnelle, vigilance personnelle, etc Sensibilisation aux normes socio-culturelles, etc.
Sécurité et sûreté des locaux	Bureau et lieux de vie.

ATTENTION

Tous les POS devraient systématiquement indiquer l'objectif du POS (à qui sert-il ? quand doit-il être utilisé ?) ainsi que la personne responsable de la bonne mise en œuvre du POS.

4.3. POS SPECIFIQUES ET POINTS PARTICULIERS

Mouvements

Il existe plusieurs types de POS concernant les mouvements, et chaque organisation est libre de détailler leurs procédures en fonction de l'analyse des risques. Néanmoins, les points suivants devraient être explicités.

Point	Commentaire
Entretien et maintenance des véhicules	- Désignation des responsabilités - Spécification du carnet de bord (manuel d'entretien) - Gestion des consommables
Recrutement, formation et encadrement des chauffeurs	- Protocoles de recrutement (tests, validation) - Formation additionnelle (premiers secours, mécanique, etc.) - Définition de règles de conduite en complément du code de la route - Soutien à la responsabilité (autorité du chauffeur sur les règles de sûreté à bord)
Equipement des véhicules	- Equipement mécanique en cas de panne - Equipement de communication (redondance de moyens) - Eau, nourriture, kit de premier secours - Extincteurs - Ceintures de sécurité et autres
Validation des mouvements	- Procédures de vérification de la sûreté de l'itinéraire - Détermination d'un besoin d'escorte le cas échéant - Protocoles d'obtention de l'escorte - Détermination de procédures spécifiques (mouvements simultanés ou « kiss », conduite de nuit, etc.)
Lignes de responsabilité	- Désignation d'un chef de bord au départ vis-à-vis des passagers
Localisation du véhicule en cours de mouvement	- Protocoles de communications (à intervalles réguliers ou au passage de sites pré-identifiés) - Mise en place de moyens additionnels le cas échéant (radio opérateur sur base en cas de communications HF, par exemple).
Accident de la route	- Procédures à adopter en cas d'accident - Procédures à adopter si le mouvement provoque un accident (risques éventuels en cas d'arrêt, auto-référencement aux autorités, etc.
Checkpoints	- Localisation des checkpoints connus - Equipement à emporter (documentation officielle) - Comportement à observer à l'approche et au passage du checkpoint)
Mouvements en convoi	Détail des procédures (notamment espacement, communication et contingence)

Communications

De même que pour les Mouvements, il existe plusieurs types de POS concernant les communications, et chaque organisation est libre de détailler leurs procédures en fonction de l'analyse des risques et de la complexité de leur environnement. Deux principes majeurs en la matière concernent :

- L'importance de disposer de moyens de communication redondants (et ne pas se fier aux seuls mobiles, dont la fiabilité peut être éprouvée en zone rouge orange faute de réseau).
- L'importance de disposer de protocoles de communication fiables.

Point	Commentaire
Equipement	- Nature (téléphone mobile, satellitaire, radio, connectique autres). - Localisation de l'équipement - Alimentation en énergie (règles de chargement) - Entretien de l'équipement par type - Désignation des responsabilités pour l'entretien et le chargement - Modalités éventuelles de remise de l'équipement aux équipes (à quel lieu, moment, mise à disposition de cartes sim et/ou de crédit pour la bonne marche de la communication.
Sélection de l'outil	- Carte de couverture des réseaux mobiles et identification des zones non couvertes. - Spécification du lieu d'entreposage de l'outil (pour les dispositifs satellitaires).
Protocoles de communication	- Protocoles pour les communication routinières, complétées par un arbre de communication en interne et en externe. - Protocoles de communication pendant les mouvements et déplacements (intervalles, fréquence…) - Le cas échéant, assignation des identifiants pour l'usage des radios.
Sécurité de l'information	- Conduite à tenir pour préserver la confidentialité des informations en phonie. - Conduite à tenir pour préserver la confidentialité des communications électroniques. - Procédures de protection et de sauvegarde des
Visibilité	- Règles de base en matière de signalisation de l'organisation (sur les personnes, véhicules et bureaux/lieux de vie).
Media	- Conduite à tenir en cas de sollicitation par des média nationaux ou internationaux.

Sécurité personnelle, comportement et attitude

Point	Commentaire
Formation	- Quelles sont les formations préalables recommandées ? - Quelles sont les formations à mettre en place pendant la durée du séjour, le cas échéant ?
Equipement	- La personne est équipée d'un « grab bag » pendant les déplacements - Voir ci-dessous pour la composition du « grab bag »
Connaissance des locaux	- Prendre connaissance des lieux de travail et d'habitation, et des procédures pertinentes (localisation des kits de premiers secours, des extincteurs, des schémas d'évacuation) - Le cas échéant, savoir localiser le coffre-fort dans le lieu, en cas de vol à main armée (afin de pouvoir orienter les voleurs et les faire partir le plus vite possible).
Premiers secours	- Être titulaire d'un certificat de premier secours (niveau PSC 1) - Mettre à disposition le numéro de téléphone des urgences médicales
Constant Companion	- Ce document récapitule en format poche et plastifié la liste des contacts d'urgence sur le lieu d'assignation (numéros d'urgence police et médical, consulaire, hiérarchie interne). - Il doit être mis à jour régulièrement et distribué à chaque expatrié.
Connaissance et respect des us et coutumes	- Si votre organisation a un code de conduite, il doit avoir été partagé - Chaque expatrié doit être sensibilisé aux us et coutumes du pays et de la région.
Signalement et procédures	- Le traitement des manquements à la déontologie doit être explicité, notamment pour ce qui concerne les procédures de signalement et éventuelles procédures disciplinaires à envisager.

Un grab bag est destiné à faciliter un départ d'urgence (en cas d'évacuation d'urgence d'un site ou, plus rarement, en cas d'alerte incendie). Il doit au moins contenir les documents d'identité et d'immigration (originaux ou copie), une enveloppe de sécurité, de l'eau, des tablettes de chlore, des barres protéinées, des vêtements adaptés à l'environnement, un poncho, de la ficelle, un canif multi-usage, une boussole, une carte de l'environnement (liste non exhaustive).

Sécurité et sûreté des locaux

Si le personnel est hébergé dans des locaux appartenant à l'organisation, les procédures devraient spécifier les points suivants qui s'appliquent également aux lieux de travail

Points	Composantes Principales
Structure et aménagement du site	- Enceinte de locaux (spécifiant hauteur, épaisseur, éloignement de l'enceinte par rapport au bâtiment) - Caractérisation du portail (simple ou à sas) - Issues de secours - Poste de gardien - Localisation d'une pièce de sécurité, description de l'équipement de la pièce (a minima malle de sécurité et kit de premier secours) - Composantes de genre (localisation et séparation des toilettes, équipement dédié) - Equipement énergie alternatif (générateur au moins) - Flux d'évacuation et localisation des extincteurs en cas d'alerte incendie - Localisation des kits de premier secours le cas échéant
Gestion de la sécurité des lieux de vie et de travail	- Procédures de sélection, de formation et d'encadrement des gardiens si ceux-ci sont recrutés par l'organisation - Points d'attention dans la sélection d'un prestataire de gardiennage le cas échéant - Procédures de sensibilisation et de formation du personnel au travail et du personnel résident (lutte anti-feu et premiers secours)
Contrôle des accès	- Les procédures de gestion des flux visiteurs sont spécifiées.

Si le personnel est hébergé dans des structures d'accueil (hôtelières ou autres), il est recommandé d'évaluer systématiquement la sûreté des lieux (et notamment de l'emplacement) et de mettre en place une procédure ad hoc pour les réservations, les mouvements quotidiens, et les mesures complémentaires (par exemple communication en cas d'évacuation, etc.).

4.4. PLANS DE CONTINGENCE

PC indispensables

Les PC les plus importants, à compléter / ajuster le cas échéant, qui doivent impérativement figurer dans le plan de sûreté, sont récapitulés dans le tableau suivant :

PC	Commentaires
Décès	Identification des vérifications à entreprendre pour confirmer l'identité, contacts avec la famille (identification et formation des interlocuteurs désignés), etc.
Agressions Sexuelles	Comportement de base vis-à-vis du survivant et des témoins éventuels, mesures d'appui médical éventuelles (prophylaxie), mesures d'appui légal éventuelles (en concertation avec le survivant), procédures spécifiques de reporting (en concertation avec le survivant, sauf cas spécifiques), etc.
Enlèvement et prise d'otage	Fournit à la CGI le cadre des réactions initiales en cas d'enlèvement ou de prise d'otages confirmés. De tels incidents impliquent automatiquement l'activation de la CGC au siège.
Hibernation	Définit les mesures à anticiper en cas de confinement (pendant une manifestation ou le pillage d'une ville). Il inclut la localisation d'une pièce sécurisée, les contenus d'une malle d'hibernation (nourriture, boisson, équipement énergie, hygiène, etc.).
Relocalisation et Evacuation	Identifie les protocoles de décision (chaîne de responsabilité), l'itinéraire et le moyen principal et secondaire, les contacts à prendre en cas d'une extraction ou de support extérieur, les visas à obtenir en avance en cas d'évacuation vers un pays tiers, etc.
Evacuation Médicale	Procédures de premiers secours (y compris communication spécifique), contact avec appui médical (y compris ambulance et paramédical) pré identifiés, lien avec assurance médicale (communication des numéros de polices d'assurance et des contacts d'urgence), accompagnement de la victime, etc.

Les PC touchant aux décès, agressions sexuelles et kidnapping déclenchent généralement l'activation d'une cellule de crise et sont abordés ci-dessous dans le cadre plus général d'un plan de gestion de crise (PGC). Le PGC est distinct du plan de sûreté de l'organisation, mais il est fortement recommandé d'en avoir un pour toute entité travaillant en zone rouge ou orange.

Certains PC spécifiques doivent être décrits avec détail et sont précisés dans la section suivante.

ATTENTION

Plus il y a de POS et de PC, plus la probabilité qu'ils soient mal maîtrisés ou peu utilisés par les équipes est grande. Il convient de veiller à ce que leur mise en œuvre et leur mise à jour conserve un caractère pratique et réaliste.

Gestion de crise

En cas d'incident grave à critique, la CGI dans le pays d'intervention doit contacter un référent pré-identifié au siège. Ce référent peut-être le responsable sûreté ou un autre cadre responsable en astreinte. Le contact au siège donne alors l'alerte en suivant les procédures décrites dans le plan de gestion de crise de l'organisation, et la Cellule de Gestion de Crise (CGC) est activée.

L'existence du plan de gestion de crise doit être attestée dans le plan de sûreté, sans toutefois être détaillée. Un tel plan doit comporter les éléments suivants *a **minima***, à compléter / ajuster au regard de la situation envisagée :

Chapitre	Composantes principales
1. Organisation 1.1. Composition de la CGC 1.2. Mécanismes de décision 1.3. Procédure d'activation de la CGC 1.4. Ordre du jour de la première réunion de la CGC 1.5. Lignes de communication 1.6. Gestion post-crise	Cette première section permet de clarifier pour tous les mécanismes principaux de la CGC et d'appuyer efficacement ses membres dans les premières heures de la gestion de crise, quand l'effet de sidération peut être important et que l'hétérogénéité des informations peut rendre difficile les processus de décision. A noter : la composition du CGC doit inclure le nom du responsable principal et d'un suppléant pour toutes les fonctions identifiées. Les numéros de téléphone d'urgence de chacun doivent être clairement identifiés.
2. Fonctions principales 2.1. Responsable de la CGC 2.2. Responsable de la sûreté 2.3. Responsable des ressources humaines 2.4. Responsable communication	Les fonctions des principaux responsables détaillent leurs objectifs, les prérequis à la prise de poste en CGC (formation et simulations, notamment) leurs tâches principales pendant et après la crise.
3. Principaux scénarios 3.1. Mort d'un employé suite à un incident critique 3.2. Kidnapping 3.3. Violences sexuelles	Bien que chaque crise soit distincte, l'incident critique à l'origine de la crise impose des séquences spécifiques et reconnaissables. Les scénarios permettent d'établir des canevas types de gestion sur lesquels les membres de la CGC peuvent s'appuyer.
4. Protocole de liaison avec les familles	La liaison avec les familles, habituellement assumée par le département des ressources humaines, demande un protocole spécifique et particulier face à des situations de détresse.

Il est recommandé que le plan de gestion de crise fasse l'objet de simulations régulières afin de sensibiliser les membres de la CGC aux particularités de la gestion de crise.

Evacuation médicale

Souscription à une police d'assurance permettant l'évacuation médicale de leur personnel (International SOS est une organisation de référence dans ce domaine). Le plan d'évacuation médicale doit comprendre les points suivants, à compléter / ajuster au regard de la situation envisagée :

1. En préalable à toute procédure médicale, le référent sécurité du pays concerné doit avoir identifié les hôpitaux et centres médicaux de référence dans la région, y compris les numéros d'urgence. En complément, les principaux moyens de transport vers les structures de santé doivent avoir été identifiés, avec les moyens de les contacter (ambulances publiques ou privées, moyens mis à disposition par les Nations Unies ou d'autres acteurs).
2. Le référent sécurité est responsable, directement ou par délégation aux ressources humaines, de la compilation des informations médicales d'urgence pour tout le personnel susceptible d'être évacué médicalement. Ces informations doivent inclure, outre le nom, prénom et moyens d'identification (couleur des cheveux, yeux, etc.) :
    - Pathologies récentes
    - Traitement en cours le cas échéant
    - Allergies connues
    - Statut des vaccinations
    - Groupe sanguin
    - Numéro d'urgence à contacter dans la famille.
3. Procédure d'alerte et de déclenchement de la Cellule de Gestion d'Incident (CGI) du pays qui, en temps utile en avise le référent sûreté au siège à fins de coordination.
4. Informations médicales sur l'état de patient à collecter pour transmission à la compagnie en charge de l'évacuation.
5. Procédures de mise en relation de la compagnie en charge de l'évacuation médicale avec les médecins du patient si celui-ci a été référé en milieu médicalisé.
6. Désignation d'un accompagnant pendant l'évacuation.
7. Désignation d'un point focal en charge d'alerter les proches.

Hibernation

L'hibernation est une procédure de confinement volontaire en cas de manifestations violentes ou autres événements de même nature susceptibles de mettre en jeu la sûreté des équipes. Une hibernation est normalement une contingence qui s'anticipe aisément, notamment en regard d'échéances spécifiques (élections, événements sportifs, etc.).

Une hibernation réussie repose sur l'aménagement d'un site sûr et discret dans les locaux, et sur son équipement, regroupé dans ce qu'il est convenu d'appeler une malle d'hibernation.

Les points suivants doivent être abordés, à compléter / ajuster au regard de la situation envisagée :

Points	Composantes Principales
Localisation	- Identification du site adapté dans les lieux de vie et les lieux de travail. - Définition des procédures à suivre en cas d'hibernation dans les locaux d'une organisation partenaire.
Dimensionnement	- Evaluation du nombre de personnes susceptibles de rester en hibernation. - Evaluation du nombre de jours pendant lesquels l'hibernation est susceptible de durer.
Equipement	- Spécification de l'équipement vie (eau et nourriture, éventuellement tapis de sol et couvertures). - Spécification de l'équipement hygiène (seau, évacuation, poubelle, produits d'hygiène féminine). - Spécification de l'équipement énergie (batterie, piles, bougies, etc.). - Spécification de l'équipement communication (matériel, crédits disponibles, chargeurs).
Vérification du site et de la malle	- Définition des responsabilités de supervision du matériel, - Renouvellement des périssables.
Protocoles ad hoc	- Conduite à tenir en cas d'interaction avec un ou plusieurs intrus (assignation des responsabilités, éléments de langage, etc.) - Veille sur l'évolution de la situation. - Protocoles de communication avec les interlocuteurs internes ou externes (susceptibles de soutenir une extraction éventuelle, notamment). - Règles de vie en espace confiné

ATTENTION

L'attention du lecteur est à nouveau rappelée sur l'importance de mobiliser une équipe mixte homme/femme pour superviser la conception et la mise en œuvre des plans de sûreté. Ce point doit être souligné avec vigueur pour ce qui concerne les PC d'Hibernation, qui touchent à des situations mettant l'intimité de tous à l'épreuve, induisant de fait des risques extérieurs à la situation qui a conduit à l'hibernation en premier lieu.

Evacuation pour raisons de sûreté

L'évacuation peut prendre deux formes :

- La relocalisation concerne le transfert de personnel d'une base vers un lieu sûr dans le pays pour raisons de sûreté ;
- L'évacuation proprement dite concerne le transfert de l'ensemble du personnel du pays vers un autre pour raisons de sûreté.

Les deux procédures contiennent suffisamment de points communs pour pouvoir être traitées dans un document commun, bien qu'il soit recommandé de les traiter séparément.

Le plan doit préciser les éléments suivants, à compléter / ajuster au regard de la situation envisagée :

1. Les mécanismes de décision d'évacuation, notamment la personne décisionnaire et les informations sur la règle interdisant formellement aux équipes de contester une telle décision.
2. Les lignes de communication pendant l'évacuation.
3. Les points de rassemblement sûrs pour faciliter les regroupements, si cela est possible
4. Les différents itinéraires d'évacuation de manière précise en spécifiant impérativement deux itinéraires au moins (un préférentiel et une alternative)
5. Les moyens d'évacuation préférentiels en fonction de scénarios pré-identifiés (en fonction de la disponibilité locale d'un appui à l'évacuation, notamment aérien)
6. Les lieux d'évacuation pré-identifiés. Si ceux-ci sont dans des pays tiers, le plan doit identifier les prérequis en matière de visas, et le référent sûreté aura pris les dispositions nécessaires pour que le personnel évacué dispose soit des visas soit des devises requises pour l'obtention d'un visa à l'arrivée.
7. Le personnel à évacuer doit être recensé.
8. La liste de l'équipement autorisé à l'emport (allant du « grab bag » aux bagages) doit être spécifiée.
9. Les contacts ad hoc en cas d'évacuation par moyens militaires ou assimilés (Nations Unies) doivent être spécifiés.
10. Les procédures ad hoc en cas de recours à des moyens consulaires doivent être incluses (système d'ilots, arbre de communication).
11. Les tâches à mener pour informer le personnel national de la décision et prendre les mesures adéquates (traitement des salaires, préservation ou destruction de la documentation potentiellement sensible, contrats, préservation du matériel si cela est possible, etc.).

CONCLUSION

Les outils présentés dans ce guide sont alignés sur les bonnes pratiques de matière d'élaboration d'un plan de sûreté. Toutefois, ces bonnes pratiques ne couvrent qu'un éventail de procédures et ne sont pas toutes adaptées aux spécificités de chaque organisation et au contexte dans lequel celle-ci souhaite intervenir. Les éléments en annexe permettront d'aller plus loin et d'explorer différents documents afin de construire les outils de gestion les plus adaptés.

Il n'est pas inutile de rappeler ici que toute mise en œuvre doit s'accompagner d'une réflexion sur les moyens et les ressources à mettre à la disposition de l'entreprise.

REFERENCES

La grande majorité des documents disponibles sont en anglais. De plus, compte tenu de la nature des zones d'intervention, l'essentiel des publications existantes vise avant tout les ONG internationales. Ces ressources et documents sont tout toutefois d'un grand intérêt pour quiconque souhaitant travailler en zone orange ou rouge. A noter qu'en anglais, « sûreté » se traduit « security », et « sécurité » se traduit « safety ».

Les sites consulaires

Il est fortement recommandé aux organes compétents de toute organisation de veiller à consulter les sites pays des ambassades de France, ainsi que des Etats-Unis et de Grande Bretagne, qui diffusent régulièrement des mises à jour d'informations concernant le pays de destination.

Conseil aux Voyageurs (MAE) :
https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/

La carte indiquant les zones rouge et orange est régulièrement actualisée et peut être consultée sur le lien suivant :
https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/conseils-par-pays-destination/

Département d'Etat (Etats-Unis, en anglais) :
https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html

Gouvernement du Royaume-Uni (en anglais) :
https://www.gov.uk/foreign-travel-advice

Ces deux derniers sites sont le pendant du site du MAE indiqué ci-dessus.

Sites généralistes

Le think tank **Humanitarian Outcomes** est spécialisé dans les questions de sûreté et publie régulièrement des analyses pertinentes, dont son rapport annuel sur la sûreté du personnel international et national en zones de conflit. Bien que limité aux opérations humanitaires, chaque rapport touche à l'ensemble des pays en zone orange et rouge, et donc peut se révéler utile pour l'ensemble des lecteurs du présent guide.
https://www.humanitarianoutcomes.org/

Le think tank anglais **Overseas Development Institute** (ODI) a une branche dédiée aux activités humanitaires, le Humanitarian Practice Group (HPG). Celui-ci publie occasionnellement des études sur la sécurité. Leur page dédiée à la sûreté se trouve ici :
https://odihpn.org/topics-countries/?topic=security

United Nations Department for Safety and Security (UNDSS)

Rattaché au secrétariat général des Nations Unies, **UNDSS est chargé de fournir un appui en sûreté aux organisations spécialisées des Nations Unies** ainsi que, parfois, à d'autres organisations travaillant en zones de conflit. La plupart des sous-sites vers lesquels le site mère redirige sont réservés à des organisations ou individus inscrits au registre d'UNDSS et il est recommandé de solliciter le représentant d'UNDSS sur votre pays de destination pour obtenir plus de précisions.
https://www.undss.org/

Documents spécialisés

Le **guide de référence** en matière de sûreté opérationnelle s'intitule :
Operational security management in violent environments, version révisée 2010, déjà mentionné.
Il est disponible aux liens URL suivants :
En français :
https://odihpn.org/wp-content/uploads/2011/03/GPR8_revised_edition_French.pdf
En anglais
https://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

Il fournira un complément précieux à tous les éléments abordés dans ce guide. Bien qu'originellement destiné aux ONG internationales travaillant en zones de conflit, il est maintenant utilisé par de nombreuses OSC ainsi que dans le secteur privé.

Le **Centre de Recherches et d'Analyse des Savoirs Humanitaires** (CRASH), think-tank interne de Médecins sans Frontières France (MSF – F) a publié en 2016 un ouvrage de réflexion sur la gestion des risques, intitulé :
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
L'ouvrage propose des études de cas et offre un autre regard sur la gestion de la sûreté. Centré sur la pratique de MSF F, il s'intéresse avant tout à l'action humanitaire mais concerne plus largement l'action dans les zones rouge et orange.

LISTE DES ACRONYMES

AFD :	Agence Française de Développement
APCC :	Appel à Projets Crises et Conflits
CGC :	Cellule de Gestion de Crise
CGI :	Cellule de Gestion d'Incident
CSP :	Compagnies de Sécurité Privée
DAO :	Dossier d'Appel d'Offres
GOA :	Groupe d'Opposition Armé
HF :	High Frequency
MOA :	Maîtrise d'Ouvrage
ONG :	Organisation Non Gouvernementale
OSC :	Organisation de la Société Civile
PC :	Plan de Contingence
POS :	Procédure Opérationnelle Standard
TSPT :	Trouble de Stress Post-Traumatique
UNDSS :	United Nations Department of Safety and Security
UXO :	Unexploded Ordnance, acronyme anglais pour désigner les munitions non explosées
VHF :	Very High Frequency

GLOSSAIRE[4]

Accoutumance au danger : phénomène d'adaptation, généralement inconscient, de son seuil de risque acceptable, résultant d'une exposition régulière ou constante au danger ; en conséquence, l'évaluation objective du risque et de ses conséquences potentielles est réduite, ce qui peut entraîner une prise de risque accrue par une exposition non contrôlée.

Agression sexuelle : acte ou menace de viol, d'attaque et intimidation sexuelles, harcèlement sexuel ou attouchements non désirés.

Analyse d'incident : étude plus approfondie et plus décisive sur les facteurs structurels, opérationnels et contextuels qui ont donné lieu à un incident de sécurité ; consiste à questionner l'efficacité des diverses dimensions et mesures de la gestion de la sécurité et à demander si et dans quelle mesure l'organisation ou l'un ou plusieurs des membres de son personnel pourraient être jugés avoir « été à la source de l'incident ».

Approche d'acceptation : composante d'une stratégie de sécurité qui tente de diminuer l'exposition à une menace en créant des relations avec les communautés locales et les parties prenantes concernées dans la région d'intervention, de manière à obtenir leur acceptation de la présence de votre organisation et leur consentement à son travail.

Approche de protection : composante d'une stratégie de sécurité qui met l'accent sur l'utilisation de procédures et de dispositifs de protection pour diminuer la vulnérabilité aux menaces existantes ; cette approche n'a aucun effet sur le niveau de la menace.

Armes légères : armes utilisées pour l'autoprotection et le combat rapproché ou à courte distance.

Atténuation du risque : objectif de votre gestion de la sécurité, vise à réduire la menace et/ou votre vulnérabilité.

Audit de sécurité : évaluation des forces et des faiblesses de la gestion et de l'infrastructure d'une organisation en matière de sécurité afin d'en apprécier son efficacité et d'identifier les domaines à améliorer.

Bande : groupe organisé de personnes agressives ayant des intentions destructrices, criminelles, crapuleuses ou violentes.

Clan : groupement social de personnes unies par des liens de parenté, c'est-à-dire pensant avoir un ancêtre commun.

Connaissance du terrain : être attentif et comprendre l'environnement physique et social dans lequel on évolue, connaître la source de dangers potentiels, d'aide et d'abri.

Contre-surveillance : action de surveiller si quelqu'un vous épie. Stratégie pour détecter si vos déplacements, systèmes et/ou installations sont étudiés par des personnes ayant des intentions malveillantes, p. ex. un rapt, un bombardement ou un vol à main armée.

Convoi : groupe de véhicules (ou de navires) se déplaçant ensemble de manière organisée et sous la commande d'un chef afin de se soutenir et se protéger mutuellement.

[4] Le glossaire est extrait de : *Revue des bonnes pratiques, Gestion opérationnelle de la sécurité dans des contextes violents, version révisée Décembre 2010*, p. XV sq.

Coordination civil-militaire : liaison entre acteurs militaires (y compris pour les opérations de maintien de la paix) et acteurs civils déployés sur un même terrain, en particulier ceux qui sont issus de la communauté humanitaire et du développement.

Création de scénarios : prévoir comment la situation pourrait se développer à court et moyen termes et comment les menaces qui existent dans votre environnement pourraient évoluer ; examiner les hypothèses de vos plans et envisager ce que vous feriez si elles ne se réalisaient pas.

Détection : technique essentielle utilisée pour sortir d'un terrain soupçonné d'être miné, selon laquelle le sol est très soigneusement examiné avant d'y poser un pied.

Détention : action de retenir une personne en captivité sous l'autorité (p. ex. police, gardes-frontières).

Déterminer le profil des incidents : visualisation, généralement sur une carte mais également possible dans un cadre temporel, du moment, du lieu et du type des incidents survenus afin de déterminer les tendances et d'identifier de possibles tendances telles que les zones et/ou périodes à haut risque.

Détournement de voiture : vol d'une voiture, lorsque le chauffeur est au volant.

EEI : Engin Explosif Improvisé. Bombe pouvant être placée pratiquement n'importe où, par exemple sur le bord d'une route, dans un véhicule, un sac, un colis, une lettre ou des vêtements.

Embuscade : attaque soudaine lancée depuis une position dissimulée, généralement constituée d'un élément d'arrêt et d'un élément de destruction. Terme souvent employé dans le contexte d'attaques sur une route/de véhicules/de convoi.

Engins non explosés (UXO) : tout type de munitions (balle, grenade à main, obus de mortier, etc.) qui ont été amorcées (préparées au tir) mais pas utilisées, ou qui ont été tirées mais qui n'ont pas explosé et qui sont instables et dangereuses.

Enlèvement : action d'emmener une personne contre son gré. À distinguer du « rapt », qui implique que le ravisseur demande une contrepartie (p. ex. une rançon) pour libérer la victime.

Enquête sur incident : collecte d'informations situationnelles et circonstancielles au sujet d'un incident qui a eu lieu, en complément des faits de base énoncés dans le rapport d'incident.

Équipe de gestion des incidents critiques (EGIC) : Groupe créé dans le but de gérer la réponse organisationnelle aux situations de crise. Équipe généralement composée de membres spécifiques du personnel, identifiés et formés au préalable, et ayant une bonne connaissance des procédures et protocoles de gestion des incidents critiques mis en place par leur organisation.

Établir la cartographie des menaces : visualiser et illustrer les menaces sur une carte géographique.

Évacuation : mise en sécurité du personnel en le faisant sortir d'un pays.

Évaluation/analyse des menaces : tentative d'examiner plus systématiquement la nature, l'origine, la fréquence et la concentration géographique des menaces.

Évaluation/analyse du risque : tentative de considérer le risque de manière plus systématique en termes de menaces dans votre environnement, vos vulnérabilités particulières et vos mesures de sécurité pour réduire la menace et/ou réduire votre exposition.

Evasan : Évacuation sanitaire – transfert d'un patient par voie routière, maritime ou aérienne afin d'obtenir un traitement médical dans un autre lieu.

Extorsion : utilisation de la contrainte ou de l'intimidation pour obtenir de l'argent, un bien ou un acte de favoritisme.

Fournisseur/ société / prestataire privé de sécurité : entité privée fournissant des services de sécurité à des personnes ou des organisations contre rémunération. Ces services peuvent aller d'une sécurité « douce » (p. ex. consultations, formation et soutien logistique) à une sécurité « dure » (services de garde, protection armée) et à la gestion des risques et des crises, la formation des forces armées et même au commandement opérationnel et au combat.

Harcèlement : attitude abusive, que ce soit verbalement ou physiquement, à l'encontre d'une personne et qui provoque détresse ou embarras.

Hibernation : processus de s'abriter sur place jusqu'à ce que la menace et/ou le danger passe, qu'une assistance soit fournie ou qu'il soit possible de se déplacer en sécurité.

Incident critique : incident de sécurité dont la sévérité perturbe considérablement la capacité d'une organisation à exercer son activité ; met généralement en danger de mort ou provoque la mort.

Menace : danger dans votre environnement d'intervention.

Mentalité ghetto : tendance des membres d'une organisation à évoquer et à analyser l'environnement externe entre eux, dans les limites protectrices de leur « enclos », sans grande consultation ni interaction avec les divers acteurs de l'environnement externe.

Phases de sécurité (d'alerte) : résumé de la classification de différents niveaux possibles de risque et d'insécurité dans votre environnement, chacun nécessitant un ensemble spécifique de procédures de sécurité obligatoires.

Piège : système explosif improvisé ou spécialement conçu, généralement attaché à des objets ordinaires ou dissimulés sous des objets (peluche, poupée, objet militaire…), servant à dissuader, blesser ou tuer les personnes qui s'approchent de la zone piégée.

Planification d'urgence : outil de gestion employé pour une préparation adéquate à diverses situations d'urgence potentielles spécifiques à un contexte.

Point focal : agent de liaison en matière de sécurité, ayant généralement la responsabilité d'un groupe de personnes dans une zone géographique définie ; le point focal est un « noeud » important de l'arbre de communication et s'assurera aussi que toutes les personnes placées sous sa responsabilité suivent les procédures de sécurité adoptées.

Procédures opérationnelles standard : procédures officiellement établies pour mener certaines interventions ou pour agir dans certaines situations, ici plus particulièrement pour éviter qu'un incident ne se produise (aspect préventif) ou pour survivre à un incident, ou procédures à observer dans le cadre de la gestion d'un incident/d'une crise d'une organisation (aspect réactif).

Protection : employé ici de façon distincte de « sûreté » et de « sécurité » et fait référence à la « sécurisation » des civils et des non-combattants qui ne font pas partie du personnel de l'organisation d'aide humanitaire.

Rapt : enlèvement et détention d'une personne par la force dans le but explicite d'obtenir une contrepartie (argent, équipement ou certains actes) pour la vie et la remise en liberté de la personne.

Référence sociale : recommandation ou « garantie » personnelle concernant le recrutement possible d'une personne, sans avoir nécessairement travaillé avec elle mais en ayant connaissance de sa position et de sa réputation dans une communauté.

Règles d'engagement : directives destinées à tout combattant ou garde armé précisant dans quelles conditions et dans quelles limites ils peuvent employer la force en faisant usage de leurs armes à feu.

Relocalisation : retrait du personnel d'un lieu d'opérations vers un lieu plus sûr, généralement à l'intérieur du pays.

Réseau de communications : Ensemble d'éléments de même nature reliés les uns aux autres pour communiquer rapidement des informations, telles qu'une alerte à la sécurité. Selon ce système, une personne/organisation informe une liste prédéterminée d'autres personnes/organisations qui, à leur tour, en informent d'autres sur leur liste, etc.

Risque : probabilité et impact potentiel de faire face à une menace définie.

Sécurité : être à l'abri du risque ou des atteintes provenant d'actes non intentionnels (accidents, phénomènes/catastrophes naturels ou maladie).

Seuil de risque acceptable : point au-delà duquel vous considérez que le risque est trop élevé pour poursuivre l'intervention (proportionnellement a l'impact de votre action) et que vous devez quitter la zone de danger ; influencé par la probabilité qu'un incident se produise et par la gravité de l'impact s'il se produisait.

Situation d'otages : situation dans laquelle une personne ou un groupe de personnes est dans un état de siège dans un lieu connu. Comme dans le cas d'une situation de rapt, la sécurité et la remise en liberté ultérieure des personnes sont généralement soumises à certaines conditions. Celles-ci peuvent inclure une demande politique ou financière.

Stratégie de dissuasion : composante d'une approche de la sécurité qui tente de prévenir une menace en utilisant une contre menace. Celle-ci peut, sous sa forme la plus extrême, être une protection armée.

Stratégie de sécurité : philosophie, combinaison des approches et utilisation des ressources qui globalement définissent la gestion de la sécurité d'une organisation.

Stress : état de tension physique et/ou émotionnelle, inquiétude profonde ou prolongée. « État ou sentiment d'une personne lorsqu'elle sent que les demandes excèdent les ressources personnelles et sociales qu'elle est en mesure de mobiliser ». (Richard S Lazarus)

Sûreté : être à l'abri du risque ou des atteintes provenant de la violence ou d'autres actes intentionnels.

Surveillance de quartier : programme communautaire plus ou moins officialisé entre voisins ayant pour objectif de surveiller les personnes suspectes et de lutter contre la criminalité dans leur zone d'influence ou résidentielle.

Survivre sur les champs de bataille : mesures visant à atténuer le risque de mort ou de blessure lorsqu'une personne est sous le feu de l'ennemi, ou dans une zone de tir, quel que soit le type d'arme utilisé.

Terrorisme : actes destinés à infliger des blessures spectaculaires ou mortelles à des personnes civiles et à créer une atmosphère de peur, généralement pour poursuivre un objectif politique ou idéologique.

Triangulation : recoupement des informations ou détails en comparant l'opinion ou la version de différentes sources.

Trouble de stress post-traumatique (TSPT) : trouble psychologique dont peuvent souffrir les personnes ayant subi un traumatisme émotionnel sévère et qui peut occasionner perturbations du sommeil, retours en arrière, angoisse, fatigue et dépression.

Violence basée sur le genre : violence à l'encontre d'une personne basée sur le genre, le sexe. Inclut les menaces et/ou les actes qui infligent des souffrances physiques, mentales ou sexuelles, la contrainte ou autres privations de liberté. Bien que des personnes des deux sexes et de tous âges puissent en être victimes, les femmes et jeunes filles en sont les principales victimes en raison de leur statut de subordination.