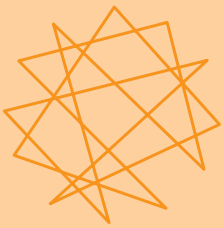
eisf



MANUEL EISF À L'ATTENTION DES ORGANISATIONS NON GOUVERNEMENTALES

La sécurité en pratique :

boîte à outils de gestion des risques à l'attention des agences humanitaires

EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF)

L'EISF est un réseau indépendant de points focaux de sécurité qui représentent actuellement 95 ONG humanitaires européennes œuvrant à l'échelle internationale. L'EISF s'engage à améliorer la sécurité des opérations de secours ainsi que celle des personnels impliqués. Son objectif est de faire bénéficier les agences humanitaires d'un accès sécurisé aux populations touchées par des situations d'urgence. Ses activités s'appuient sur le développement de recherches et d'outils propices à la sensibilisation, à la préparation aux différentes situations et aux meilleures pratiques.

L'EISF a été créé dans le but de conférer un rôle accru à la gestion des risques de sécurité dans le cadre des opérations humanitaires internationales. Il facilite les échanges entre les organisations membres et d'autres entités telles que les Nations Unies, les bailleurs de fonds institutionnels, les établissements universitaires et de recherche, le secteur privé et un large éventail d'ONG internationales. La vision de l'EISF consiste à devenir un point de référence mondial en matière de pratique appliquée et de connaissance collective, et le développement de recherches pratiques destinées à la gestion des risques de sécurité dans le secteur humanitaire représente un aspect clé de ses activités.

L'EISF est une entité indépendante financée par le Bureau américain de l'Aide d'urgence à l'étranger (OFDA), l'Agence suisse du développement et de la coopération (SDC) et les contributions de ses membres.

www.eisf.eu

Remerciements

Ce manuel a été élaboré conjointement par James Davis (Act Alliance) et Lisa Reilly, directrice exécutive du European Interagency Security Forum (EISF). Raquel Vazquez Llorente, chercheuse à l'EISF, était responsable du projet.

Le module 12 – Gestion des personnes a été développé par Christine Williamson. La responsable de projet était Adelicia Fairbanks, conseillère en recherche à l'EISF.

L'European Interagency Security Forum (EISF) et James Davis tiennent à remercier le groupe de travail d'avoir bien voulu les faire profiter de ses connaissances : Marko Szilveszter Macskovich (Bureau pour la coordination de l'aide humanitaire des Nations Unies), Michelle Betz (Betz Media Consulting), Veronica Kenny-Macpherson (Cosantóir Group), Jean Michel Emeryk, Peter Wood, Shaun Bickley, William Carter, Rebekka Meissner, Christine Newton, Emmanuelle Strub, Andrew Eckert, et Hélène Cardona.

Citation suggérée

Davis, J. et al. (2018) *La sécurité en pratique : boîte à outils de gestion des risques à l'attention des agences humanitaires.* European Interagency Security Forum (EISF).

Conception et illustrations : www.wave.coop

Clause de non-responsabilité

L'EISF est une association de membres et n'a pas de statut juridique en vertu des législations en vigueur en Angleterre et au pays de Galles, ou de toute autre juridiction. Les références à l'« EISF » dans le présent document englobent les organisations membres, les agences d'observation et le secrétariat de l'EISF.

Le contenu de ce document n'est pas destiné à correspondre à des conseils sur lesquels les lecteurs peuvent compter. Les lecteurs doivent obtenir des conseils professionnels ou spécialisés avant d'agir, ou de ne pas agir, en fonction du contenu de ce document.

Bien que l'EISF se soit efforcé de veiller à l'exactitude des informations figurant dans le présent document, il n'en garantit ni la précision, ni l'exhaustivité. Les informations présentées sont fournies « telles quelles », sans aucune condition, garantie ou autre modalité quelle qu'elle soit, et l'utilisation de tout renseignement ou autre information contenus dans le présent document est entièrement aux risques des lecteurs. Dès lors, dans toute la mesure permise par la législation en vigueur, l'EISF décline toute responsabilité quant aux représentations, garanties, conditions et autres conditions qui, sans cet avis légal, pourraient être applicables par rapport aux informations contenues dans le présent document. L'EISF ne saurait être tenu responsable de toute perte ou de tout dommage, de quelque sorte que ce soit, causés au lecteur ou à une tierce partie résultant de l'utilisation des informations contenues dans ce document.

Table des matières

Introduction

À propos du « La sécurité en pratique »

« La sécurité en pratique » a été conçu comme un manuel facile d'emploi à l'attention des experts non spécialistes de la sécurité afin de leur permettre d'instaurer rapidement des systèmes élémentaires de sûreté, de sécurité et de gestion du risque dans des contextes nouveaux ou dans des situations d'urgence à évolution rapide. Il s'adresse tant aux organisations internationales qu'aux agences nationales qui s'établissent dans de nouvelles régions et/ou mettent en place de nouveaux programmes ; il vise plus particulièrement les environnements dont le niveau de risque évolue en raison de facteurs humains ou naturels.

Ce manuel ne propose pas une analyse exhaustive de tous les systèmes de gestion de la sûreté, de la sécurité et du risque pouvant être développés ou mis en œuvre par les organisations nationales et internationales qui opèrent dans des contextes difficiles. L'objectif du « La sécurité en pratique » est plutôt de fournir des orientations sur les principaux besoins auxquels il leur faudra répondre lors de l'ouverture d'un nouveau bureau, programme ou mission. Ce manuel fait appel à des listes de contrôle et à des outils étape par étape pour permettre d'identifier et gérer les obligations importantes en matière de devoir de protection.

Le contenu de ce guide est le fruit d'une collaboration entre différents types d'organisations, individus et agences de conseil qui travaillent sur les questions de sûreté et de sécurité des organisations humanitaires internationales. Les thématiques sélectionnées dans ce guide concernent de nombreuses questions primordiales ; nous espérons que des modules viendront s'y ajouter, ou que cette version sera mise à jour, au fur et à mesure de l'évolution des organisations et lorsque celles-ci auront partagé les enseignements qu'elles ont pu retirer de différents contextes.

Mode d'emploi du « La sécurité en pratique »

Ce guide peut être utilisé de diverses manières. Au niveau le plus élémentaire, il peut être enregistré sur une clé USB. Il peut également être imprimé et emporté par le personnel déployé dans un nouveau contexte – il servira alors de modèle à suivre pour mettre en place des systèmes et des politiques dès les étapes initiales, et pour assurer la sécurité du personnel lors de la mise en place d'un programme. Dans l'idéal, ce document devrait être considéré par l'équipe responsable d'un projet comme faisant partie intégrante des processus de planification de déploiement du personnel, de conception de programmes, ou pris en compte lorsque l'organisation étend ses activités face à une situation d'urgence ou à un changement significatif dans le contexte.

Vous trouverez dans ce guide :

- Des activités et conseils essentiels, signalés par le symbole
- Des témoignages d'experts, signalés par le symbole
- Des renvois vers d'autres parties du manuel, signalés par le symbole
- Les principaux concepts et définitions se trouvent dans le glossaire.

Pour faciliter la compréhension, ce guide est organisé en trois catégories de modules : **Planification et préparation**, **Réponse** et **Services de soutien**.

Les modules de planification, de préparation et de réponse de ce guide correspondent au **processus de planification de la gestion des risques de sécurité** (voir page 7). Vous trouverez au début de chaque chapitre un diagramme de navigation indiquant en vert l'étape du processus dont il sera question.

Les modules relevant des services de support couvrent des domaines et des processus qui affectent, complètent et s'intègrent dans la gestion des risques de sécurité d'une organisation et devraient être pris en compte tout au long du processus de planification de la gestion des risques de sécurité.

La structure des modules a été conçue pour aider les personnels à élaborer des contre-mesures ou des stratégies de réduction du risque afin de faire face aux menaces identifiées lors de l'évaluation des risques par l'organisation. Les listes de contrôle, les plans et les modèles devront être modifiés pour tenir compte des spécificités de chaque organisation et de chaque contexte.

1 Processus de planification de la gestion des risques de sécurité

Comme pour toutes les mesures destinées à la sûreté et la sécurité, la première étape critique consiste à effectuer une évaluation des risques. Les catastrophes naturelles, les famines, les épidémies voire les élections nationales sont des événements tout aussi susceptibles de présenter des risques que les conflits, le terrorisme ou d'autres types de violence. Ce guide propose un modèle d'évaluation des risques sous un format simple à utiliser qui permettra aux personnels d'identifier et de mesurer les différents risques.

Une bonne gestion de la sécurité n'est pas synonyme d'aversion aux risques mais de capacité à reconnaître les risques et à élaborer des mesures de gestion des risques adaptées pour permettre l'exécution des programmes en toute sécurité. Si les mesures de sécurité empêchent la mise en œuvre d'un programme, les organisations devront s'interroger sur leur capacité à travailler dans cet environnement.

▶ *Voir le Module 3 – Outil d'évaluation des risques*

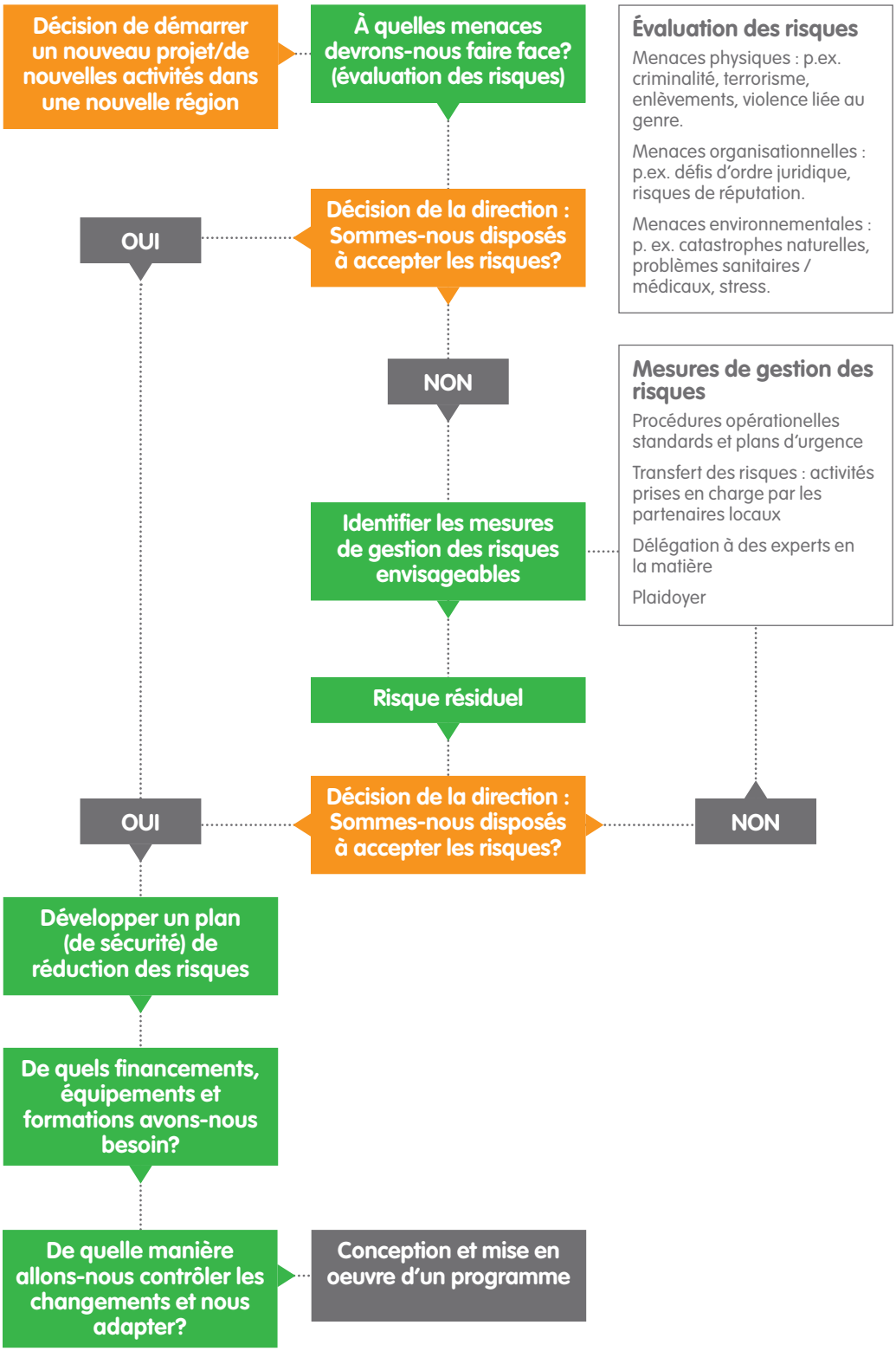
▶ *Voir le Glossaire*

Menace

Toute forme de défi, que ce soit en termes de sûreté, de sécurité ou autre, auquel sont confrontés vos personnels, vos actifs, votre organisation, votre réputation ou vos programmes dans votre contexte opérationnel.

Risque

Différentes manières dont une menace pourrait affecter vos personnels, vos actifs, votre organisation, votre réputation ou ses programmes.


Décision de démarrer un nouveau projet/de nouvelles activités dans une nouvelle région
À quelles menaces devrons-nous faire face? (évaluation des risques)
Évaluation des risques
Menaces physiques : p.ex. criminalité, terrorisme, enlèvements, violence liée au genre.
Menaces organisationnelles : p.ex. défis d'ordre juridique, risques de réputation.
Menaces environnementales : p. ex. catastrophes naturelles, problèmes sanitaires / médicaux, stress.
Décision de la direction : Sommes-nous disposés à accepter les risques?
OUI
NON
Mesures de gestion des risques
Procédures opérationelles standards et plans d'urgence
Transfert des risques : activités prises en charge par les partenaires locaux
Délégation à des experts en la matière
Plaidoyer
Identifier les mesures de gestion des risques envisageables
Risque résiduel
Décision de la direction : Sommes-nous disposés à accepter les risques?
OUI
NON
Développer un plan (de sécurité) de réduction des risques
De quels financements, équipements et formations avons-nous besoin?
De quelle manière allons-nous contrôler les changements et nous adapter?
Conception et mise en oeuvre d'un programme

Face à une nouvelle urgence, ou lors du lancement d'opérations dans une nouvelle région, il est essentiel qu'une évaluation des risques de sécurité fasse partie de l'évaluation des besoins. Ainsi, tous les frais de gestion des risques de sécurité pourront dès le début être inclus dans la conception du programme, au lieu d'être ajoutés à la fin.

Duty of care (l'expression anglaise, souvent aussi utilisée en français, est employée dans ce manuel et correspond aux expressions « devoir de diligence », « devoir de protection » ou « responsabilité de l'employeur ») est un concept de plus en plus important pour les organisations qui déploient des personnels dans des environnements difficiles. En bref, duty of care est l'obligation légale et morale qui incombe à une organisation de prendre toutes les mesures possibles pour réduire le risque de préjudice causé aux personnes qui travaillent pour elle ou opèrent pour son compte. Ces personnes comprennent les personnels, les bénévoles, les stagiaires, les sous-traitants (gardiens, chauffeurs) et les organisations partenaires chargées de la mise en œuvre du programme (bien que le niveau de *duty of care* requis puisse être différent). Dans de nombreux pays, les ONG, y compris leurs cadres supérieurs et leurs directeurs, pourront faire l'objet de poursuites judiciaires si elles négligent leur *duty of care*.

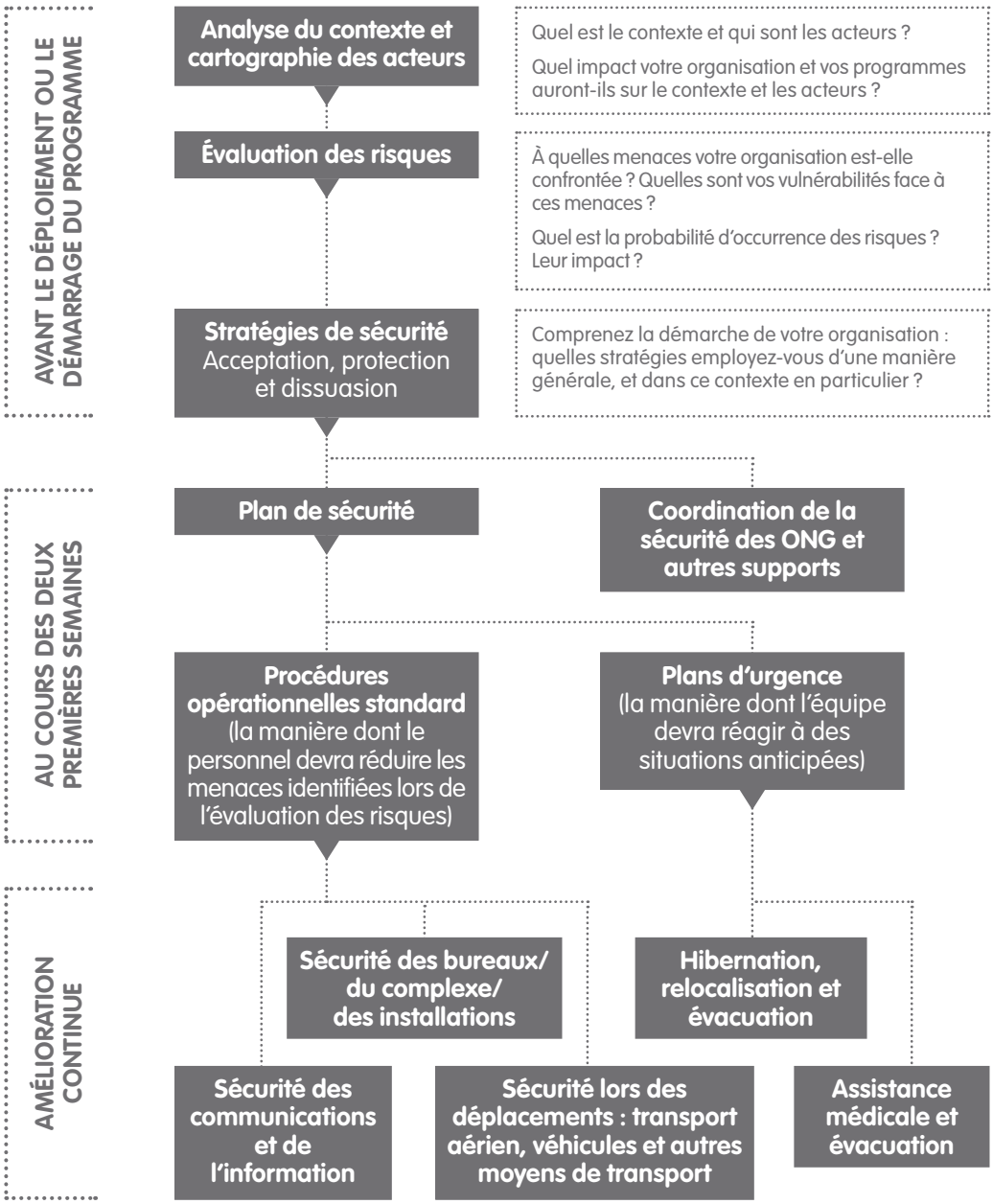
▶ *Voir le Glossaire*

Une gestion des risques de sécurité de qualité n'est pas forcément synonyme de coûts élevés. Dans de nombreux cas, il s'agira plutôt de former le personnel, d'instaurer des politiques cohérentes et d'assurer un suivi constant du contexte de menace. La tenue d'un registre des incidents, la mise en place d'une politique exigeant des individus qu'ils confirment leur présence, l'application de limitations de vitesse pour les véhicules, la constitution de stocks d'urgence ou la participation aux forums d'ONG sont autant de mesures qui peuvent avoir un coût minime mais des répercussions majeures sur la sûreté de l'organisation et la sécurité de son personnel et de ses actifs. Le principal défi consiste à identifier le ou les membre(s) du personnel responsable(s) et à accorder le temps nécessaire à la réalisation de ces activités.

Il est de plus en plus fréquent que les bailleurs de fonds aient conscience des coûts associés à la gestion de la sûreté et de la sécurité. Si l'évaluation des risques justifie les dépenses, les coûts directs peuvent être inclus dans le budget de mise en œuvre du programme. Les coûts de la sécurité, notamment pour l'équipement (radios, téléphones satellite, trousses de premiers secours, matériel/fournitures d'urgence, fonds d'urgence, amélioration des installations, assurance, etc.), ou du temps à y consacrer (mise en œuvre d'une stratégie d'acceptation proactive, négociations relatives à un accès durable), peuvent être inclus dans les propositions de financement. Si l'évaluation des risques le justifie, les bailleurs de fonds sont souvent disposés à financer ces lignes budgétaires pour la sécurité.

▶ *Voir le rapport de l'EISF intitulé « The cost of security risk management for NGOs »*

Processus de planification de la gestion des risques



Aucune situation n'est immuable. Elles peuvent s'améliorer comme se détériorer. Les politiques et les procédures de sécurité doivent régulièrement être actualisées ou adaptées à l'évolution des menaces présentes dans l'environnement opérationnel. Il est important de définir les points suivants :

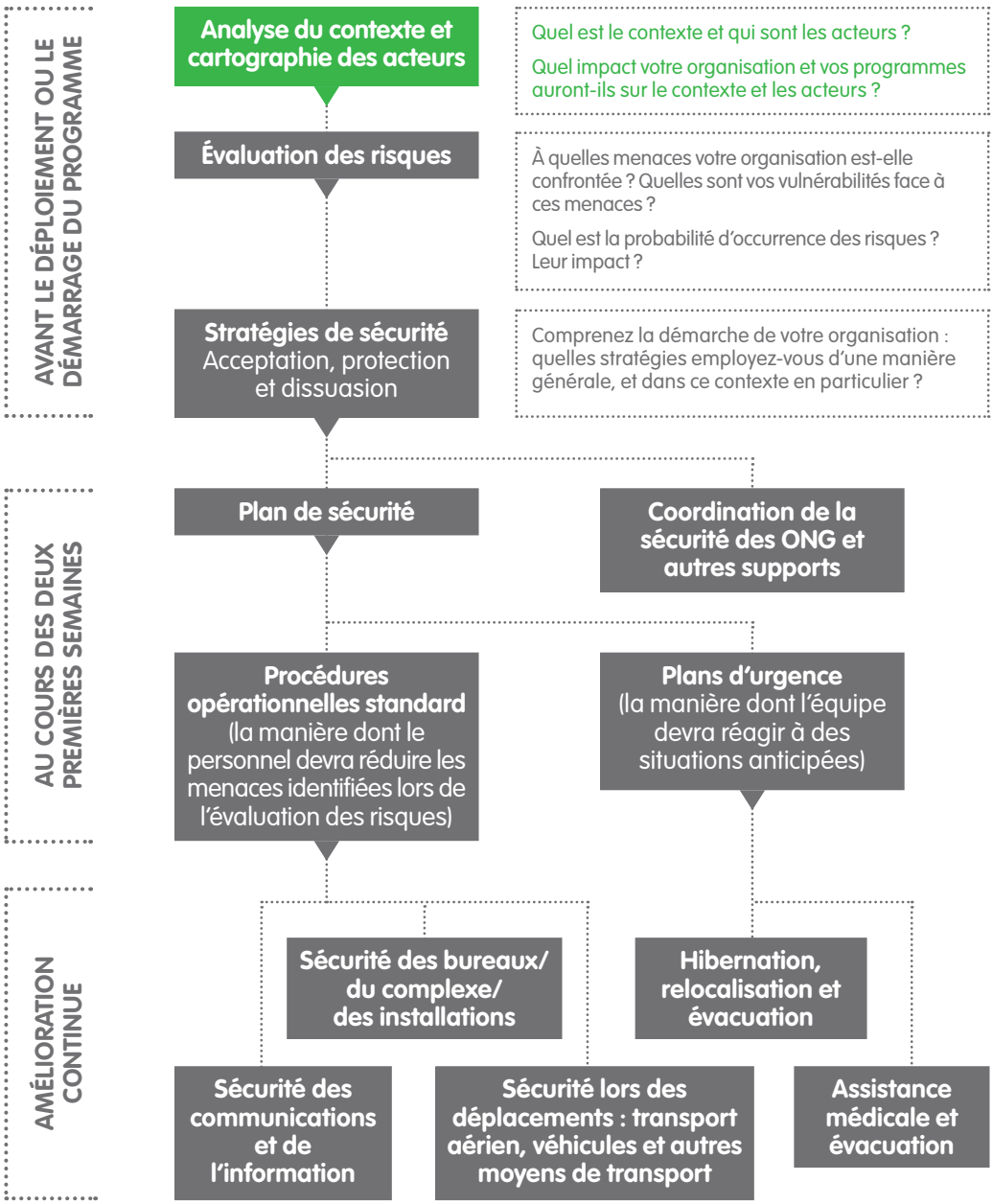
- Qui est chargé de passer en revue et d'actualiser l'évaluation des risques et les plans de sécurité ?
- À quelle fréquence cet exercice doit-il être effectué (une fois par an, par trimestre, par mois) ?
- Comment le personnel sera-t-il informé des changements apportés aux politiques ou procédures et formé en conséquence ?

Pour suivre l'évolution des menaces dans l'environnement opérationnel, il faut identifier les indicateurs du changement, autrement dit savoir quels développements contextuels peuvent et doivent faire l'objet d'un suivi si l'on veut connaître précocement les changements susceptibles d'avoir un impact sur les risques organisationnels.

L'une des méthodes les meilleures et les plus simples pour surveiller le changement consiste à élaborer une cartographie des incidents, en incluant les accidents évités de justesse, ainsi que les incidents qui se sont produits dans votre environnement opérationnel mais sans pour autant affecter spécifiquement votre organisation.

Le fait de consigner régulièrement le moment et le lieu où les incidents se produisent, y compris l'heure, les personnes concernées et les conséquences, vous aidera à voir à quels moments la situation s'améliore ou se détériore. Par exemple, prenez une carte et plantez-y des épingles de différentes couleurs représentant chaque type d'incident et/ou l'entité impliquée (votre organisation, une autre ONG, l'ONU, une organisation partenaire, une ONG locale).

2 Cartographie des acteurs et analyse du contexte



La cartographie des différents acteurs de l'environnement opérationnel et l'analyse du contexte sont deux activités clés pour les organisations qui partent travailler dans un nouveau pays ou une nouvelle région, ou qui lancent un nouveau programme ou projet. Elles sont également essentielles dans un contexte opérationnel familier en cas de perturbation majeure du statu quo.

Ces dernières années, des ONG ont été ordonnées de quitter certains pays, ou bien leur personnel a été condamné ou emprisonné, et ce, malgré l'urgence des besoins humanitaires de l'État en question, au motif que quelqu'un avait commis un impair, offensé un gouvernement hôte ou lancé des travaux sans avoir obtenu au préalable une reconnaissance de la part des structures de leadership formelles et informelles. Il est fortement conseillé de démarrer une cartographie des acteurs et une analyse du contexte le plus tôt possible et de poursuivre ces exercices tout au long du programme.

Quels sont les principaux individus, groupes, organisations, institutions étatiques et autres parties prenantes qui sont susceptibles d'affecter votre sécurité et vos opérations ? Que savez-vous de leur position politique et/ou sociale, de leur pouvoir, de leur historique et de leurs rapports avec votre organisation ou de l'intérêt qu'ils lui prêtent ?

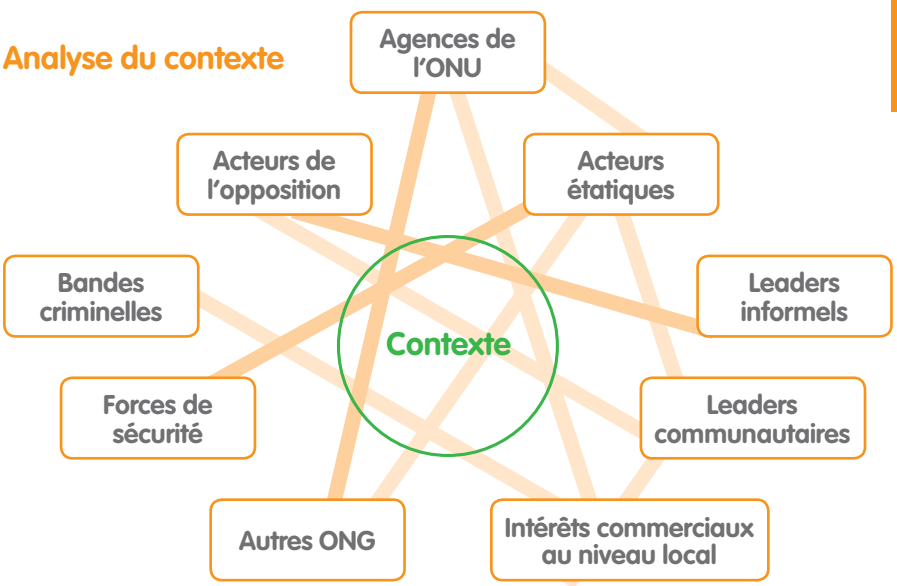
Cartographie des acteurs

La cartographie des acteurs permet d'identifier les principaux individus, parties prenantes ou autres organisations qui auront une incidence sur l'environnement opérationnel. Citons notamment :

- Les ministres du gouvernement hôte, les responsables de département ou postes similaires
- Les personnalités, groupes ou principaux sympathisants de l'opposition
- Les forces de sécurité du gouvernement hôte (armée, police, autres)
- Les bailleurs de fonds
- Les agences de l'ONU et leurs points de contact
- Les chefs communautaires
- Les leaders formels et informels de la région d'opération
- Les autres ONG, nationales et internationales
- Les principales entreprises et leurs dirigeants qui sont susceptibles de contrôler l'approvisionnement et la logistique au niveau local
- Les médias locaux
- Les groupes bénéficiaires
- Les communautés d'accueil
- Autres

Les intérêts déclarés d'un individu ou d'un groupe peuvent être différents de leurs intérêts véritables.

Une fois les principaux acteurs identifiés, il est important de comprendre les liens qui existent entre eux, et de savoir dans quelles circonstances une interaction avec un acteur pourrait avoir une incidence sur un autre acteur. Interrogez-vous sur les relations qu'ils entretiennent – quels acteurs sont alliés et lesquels sont en conflit, par exemple – ainsi que sur la manière dont ces relations pourraient être affectées par la présence de votre organisation et de vos futurs programmes.



L'analyse du contexte repose sur la cartographie des acteurs. Elle permet d'étudier un maximum de facteurs contextuels. Par exemple :

- L'histoire, récente et plus ancienne
- Les traditions culturelles et religieuses, qui peuvent être différentes en zone urbaine et en zone rurale
- Les alliances raciales, tribales ou politiques
- Les facteurs socioéconomiques
- L'état de l'infrastructure
- Le niveau de sécurité ou d'insécurité et les facteurs qui y contribuent
- L'attitude à l'égard des étrangers (Occidentaux, diaspora ou régionaux)
- L'attitude à l'égard des agences d'aide humanitaire
- Les questions de gouvernance
- La corruption
- L'impact de l'arrivée des ONG, et de leurs programmes, sur les relations sociales, économiques et de pouvoir au niveau local
- Autres facteurs

Lors de votre analyse de contexte, tenez compte des facteurs suivants en utilisant le modèle PESTEL

Politiques

Économiques

Sociaux

Technologiques

Environnementaux

Légaux

La cartographie des acteurs et l'analyse du contexte peuvent être difficiles lorsqu'il faut réagir rapidement à un nouvel environnement. L'identification de tous les acteurs et parties prenantes peut à elle seule être délicate, sans même parler d'essayer d'établir les relations de pouvoir ou les motivations officieuses. Il est important d'inclure un maximum de perspectives. Les moteurs et les relations qui caractérisent le contexte peuvent être perçus différemment selon l'âge, l'ethnicité et le genre de la personne.

Dans un premier temps, il est important de trouver de bonnes sources de savoir local, tout en ayant conscience que celles-ci peuvent manquer d'objectivité, mais il faut également effectuer des recherches sur les autres organisations ou individus qui ont récemment travaillé dans ce contexte et les interroger.

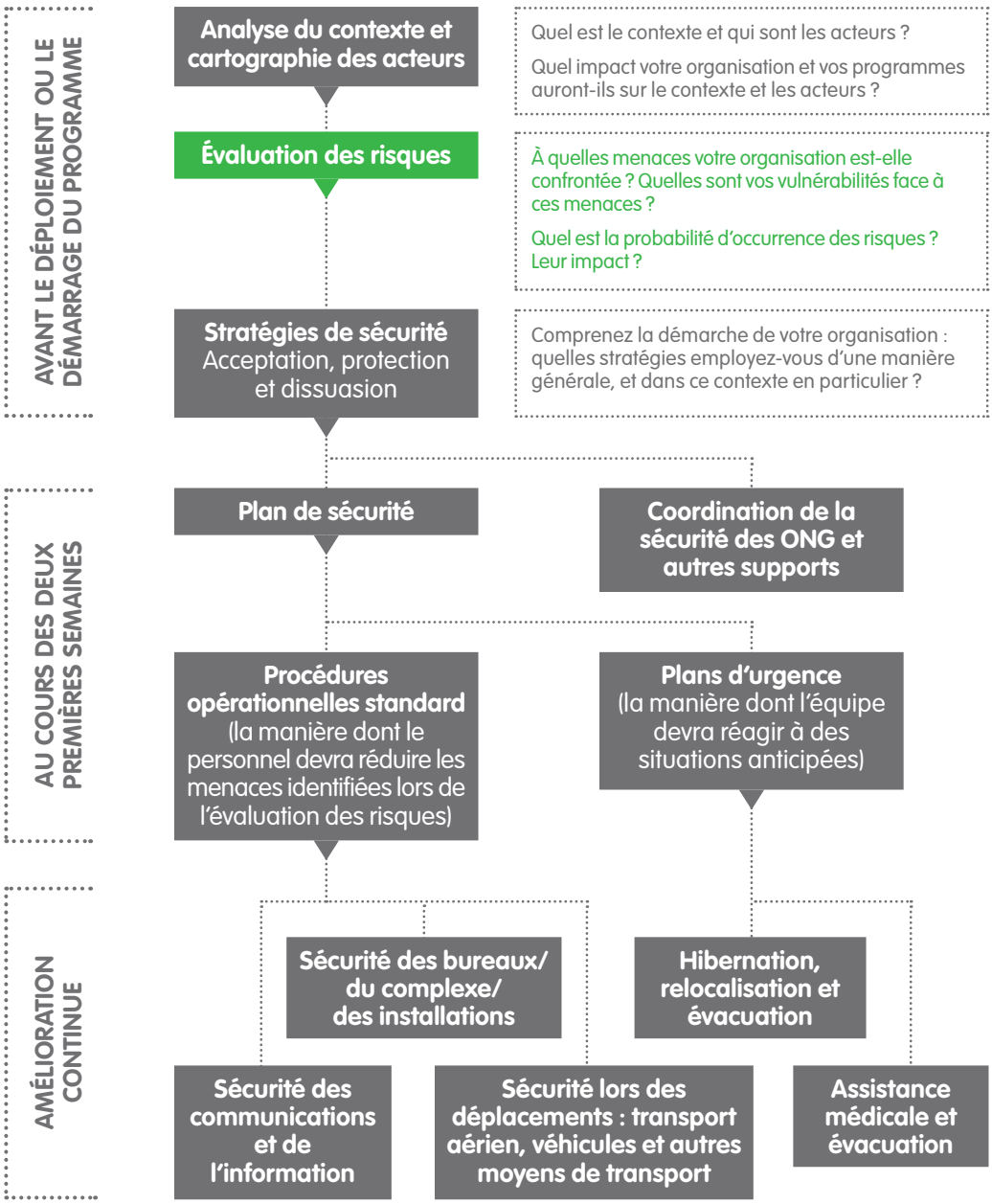
Votre organisation

Soutien possible	Soutien probable	Sources de menace
Forces de sécurité	Acteurs étatiques	Bandes criminelles
Intérêts commerciaux au niveau local	Agences de l'ONU	Terroristes
Leaders informels	Leaders communautaires	Groupes armés
Médias locaux	Autres ONG	
Acteurs de l'opposition		

Au tout début d'une nouvelle intervention, la cartographie des acteurs et l'analyse du contexte doivent être actualisées régulièrement dès que de nouvelles informations apparaissent. L'équipe responsable devra veiller à la confidentialité des résultats de cet exercice afin d'éviter de heurter les sensibilités au niveau local. En outre, il ne faudra pas donner l'impression de vouloir collecter des « renseignements » ; par conséquent, la gestion de l'information, son utilisation et les façons de la diffuser devront faire l'objet d'un contrôle étroit.

Voir le Module 8 – Sécurité des communications et de l'information

3 Outil d'évaluation des risques



Il est difficile d'instaurer des systèmes de gestion des risques de sûreté et de sécurité si les menaces ou risques ne sont pas parfaitement compris. La première étape critique de tout nouveau déploiement ou programme devra donc consister à comprendre les bases du contexte.

L'objectif de l'évaluation des risques de sécurité est de faciliter le développement de mesures de réduction du risque propices à la mise en œuvre de programmes sûrs et durables.

L'évaluation des risques fera partie de la conception du programme et du projet. L'exposition au risque et les mesures de réduction du risque sont liées aux objectifs et à la mise en œuvre du programme.

L'environnement des risques de sûreté et de sécurité peut englober un large éventail de menaces – violence, conflits, catastrophes naturelles, terrorisme, problèmes sanitaires, ingérence politique, criminalité, corruption, etc. Cet outil a été conçu pour permettre aux organisations et aux individus qui n'ont pas une expérience particulière des questions de sécurité d'effectuer une évaluation de base des risques de sécurité dans le cadre d'un processus d'évaluation plus large.

Cet outil d'évaluation se compose de trois étapes :

Identification des menaces → **Évaluation des menaces ainsi que du niveau de risque pour l'organisation (vulnérabilité)** → **Élaboration de stratégies pour réduire le risque et la vulnérabilité**

Voir le Glossaire

Il est important que toutes les agences comprennent leur « seuil » de risque acceptable, en tant qu'organisation mais aussi pour leur personnel. Certaines organisations ont déjà une expérience des environnements présentant un risque modéré à élevé, et justifient de capacités à travailler dans ce type de contextes, tandis que d'autres ne sont capables d'opérer que dans des zones présentant un risque faible ou modéré. Pour déterminer le seuil acceptable en vue de répondre à une urgence humanitaire, il est donc important de connaître la capacité de l'organisation à gérer le risque. Le seuil de risque acceptable dépend également des types de programmes mis en œuvre, par exemple s'ils doivent sauver des vies, s'il s'agit d'un plaidoyer contre des structures de pouvoir existantes ou s'ils visent le développement à long terme.

1ère étape : Identification des menaces

Plusieurs méthodologies permettent d'identifier les menaces, dont la cartographie des acteurs et l'analyse du contexte. Cependant, un grand nombre d'entre elles nécessitent une grande quantité de recherches et un séjour prolongé dans la région, et peuvent donc ne pas être pratiques si une évaluation doit être réalisée dans l'urgence.

Néanmoins, les organisations devraient au moins effectuer une analyse préliminaire dans le cadre des évaluations initiales requises pour la conception et la mise en œuvre du projet. Cette analyse devra être complétée au fur et à mesure de l'apparition de nouvelles informations.

▶ *Voir le Module 2 – Cartographie des acteurs et analyse du contexte*

Certaines organisations internationales et nationales qui démarrent des opérations dans un nouveau contexte sont confrontées à un large éventail de menaces et de risques. Voici les plus communs :

Menaces violentes

- Attaque armée ciblée
- Conflit armé non ciblé
- Enlèvement
- Terrorisme
- Violence avec explosifs (mines antipersonnel, EEI, bombardement)
- Piraterie routière
- Violence sexuelle
- Agitation civile
- Violence religieuse
- Criminalité
- Autre ?

Menaces organisationnelles

- Risque de réputation
- Risque financier (système bancaire, échange de devises, vol, détournement de fonds)
- Corruption
- Risques d'ordre juridique (permis de travail, respect de la législation nationale, résistance au plaidoyer)
- Risque politique
- Violence ou discrimination sur le lieu de travail
- Défis d'ordre culturel
- Autre ?

Menaces environnementales

- Risques naturels (météo, tremblements de terre, inondations, etc.)
- Risques médicaux (possibilité pour le personnel d'avoir accès à des soins médicaux adaptés)
- Questions sanitaires (nourriture, eau, maladies, stress)
- Accidents de la route
- Autres types d'accidents
- Incendies
- Autre ?

Si l'organisation décide de lancer un programme de réponse d'urgence, une évaluation des risques plus détaillée devra être réalisée dans les 10-15 premiers jours du déploiement et les résultats seront inclus dans la stratégie globale.

2ème étape : Évaluation des menaces et du risque

Lorsque l'organisation a identifié les types de menaces auxquelles il lui faudra faire face, elle doit évaluer chacune d'entre elles, ainsi que le niveau de risque pour le personnel, l'organisation dans son ensemble et ses opérations.

Une fois toutes les menaces répertoriées et tous les risques identifiés, il est important de classer tous les risques. Cela permettra de connaître plus facilement la gravité du risque et le degré de priorité à lui accorder.

	Menace	Lieu	Personne ou équipement concerné par ce risque	Impact du risque
	Répertorier les menaces identifiées lors de la première étape et noter chacune d'entre elles ici.	La menace se limite-t-elle à une ou quelques zones, ou la région entière est-elle affectée ? Soyez précis.	Personnel international Personnel national Membres de la communauté Véhicules non banalisés Matériel humanitaire	Mort Perte d'actifs Réputation ternie au sein de la communauté/auprès du gouvernement Baisse de la capacité à travailler
p. ex.	Piraterie routière	Route menant à l'aéroport – Autoroute 1	Tout le personnel Véhicules non banalisés VUS	Perte d'actifs Baisse de la mobilité des équipes Baisse de la capacité à travailler Blessures physiques du personnel Mort

L'évaluation du risque résulte de l'association de deux facteurs : la probabilité qu'un incident se produise, et le niveau d'impact qu'il provoquera.

Les Nations Unies et la plupart des ONG utilisent un système de classement du risque de cet ordre :

1. Très faible

2. Faible

3. Moyen

4. Élevé

5. Très élevé

Le niveau de menace peut varier selon l'endroit où l'on se trouve. Il pourra s'avérer nécessaire d'évaluer le risque au cas par cas, et non pas au niveau national ou régional. Par exemple, une zone frontalière peut présenter une

forte probabilité de conflit armé, tandis que cette situation sera improbable dans les provinces proches de la capitale. Selon la gravité de la situation d'urgence, vous pourrez ainsi vous retrouver avec un seul niveau de risque global pour la région, ou plusieurs pour la zone affectée et pour chaque type de risque.

Les menaces peuvent également être en fonction du niveau de vulnérabilité du personnel. Par exemple, il peut arriver que, dans une région spécifique, le personnel national coure un risque moins élevé que le personnel international. L'ethnicité, le genre et l'expérience peuvent aussi affecter la vulnérabilité du personnel.

Vous trouverez ci-après un tableau qui vous aidera à déterminer le niveau de risque de chaque menace identifiée. Si possible, essayez d'utiliser des incidents déjà signalés pour différents types de menaces afin de justifier le niveau de risque que vous lui attribuez. Cependant, pour les situations nouvelles n'ayant pas suscité de réponse humanitaire récemment, il vous faudra éventuellement utiliser des données tirées d'interventions similaires ainsi que des informations récentes recueillies auprès de sources locales. Les définitions de chaque niveau devront être convenues à travers l'organisation afin de permettre une comparaison des différents contextes.

Impact	Négligeable	Mineur	Modéré	Grave	Critique
	• Pas de blessures graves • Un minimum de pertes d'actifs ou de dommages • Pas de retards au niveau des programmes	• Blessures mineures • Certaines pertes ou dégâts • Certains retards au niveau des programmes	• Blessures non mortelles • Stress élevé • Pertes ou dégâts au niveau des actifs • Retards et perturbations au niveau des programmes	• Blessures graves • Destruction majeure d'actifs • Perturbation grave au niveau des programmes	• Morts ou blessures graves • Destruction ou perte totale des actifs • Perte de programmes et de projets
Probabilité					
Très improbable Tous les 4 ans et plus	Très faible	Très faible	Très faible	Faible	Faible
Improbable Tous les 2-3 ans	Très faible	Faible	Faible	Moyen	Moyen
Moyennement probable Tous les ans	Très faible	Faible	Moyen	Élevé	Élevé
Probable Une fois par semaine	Faible	Moyen	Élevé	Élevé	Très élevé
Très probable Tous les jours	Faible	Moyen	Élevé	Très élevé	Très élevé

Certaines organisations utilisent un système d'évaluation du niveau de sécurité axé sur le niveau global de risque pour l'organisation, les programmes et le personnel et qui tient compte de l'ensemble des menaces. L'élaboration d'un système d'évaluation du niveau de sécurité n'est pas couverte par cet outil.

3ème étape : Élaboration de stratégies pour réduire le risque et la vulnérabilité

Une fois que les menaces susceptibles d'affecter une réponse humanitaire ont été identifiées et évaluées, et que les risques ont été classés, il est important de recommander des mesures de réduction du risque pour faire face à ces vulnérabilités. Chaque situation est unique, mais certaines mesures peuvent généralement être prises pour réduire l'exposition au risque.

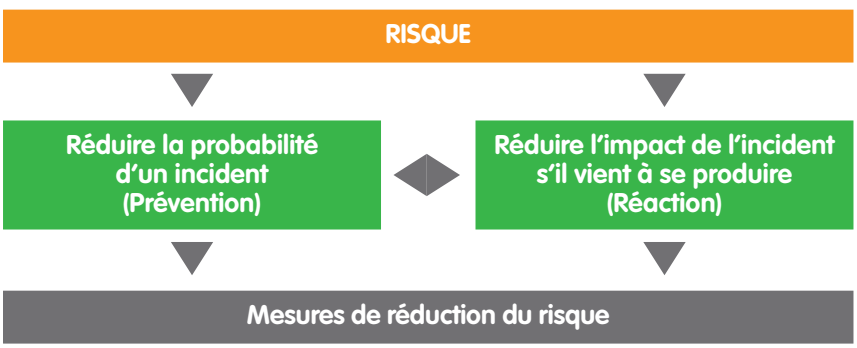
L'élaboration de stratégies de sécurité est essentielle pour s'assurer que l'agence a pris toutes les mesures raisonnables afin de minimiser le risque, et ce, avant d'affecter du personnel et des actifs et d'engager la réputation de l'organisation.

Il s'agit là d'un élément clé du *duty of care*. Les stratégies de réduction du risque devraient correspondre aux stratégies de gestion du risque choisies par l'organisation, que ce soit l'acceptation, la protection ou la dissuasion.

▶ *Voir le Glossaire*

▶ *Voir le Module 4 – Stratégies de sécurité : acceptation, protection et dissuasion*

D'une manière générale, la réduction de l'exposition au risque revêt deux formes :



Les mesures de réduction du risque doivent cibler à la fois la prévention (réduire la probabilité) et la réaction (réduire l'impact). Cela vous permettra de réduire le niveau de risque résiduel provenant du niveau attribué initialement à chaque menace identifiée et, ainsi, d'améliorer votre capacité à exécuter des programmes de réponse d'urgence. N'oubliez pas que l'objectif de la gestion des risques de sécurité n'est pas d'entraver l'exécution des programmes mais de permettre aux organisations de rester engagées et capables de mettre en œuvre des projets malgré le niveau de risque.

Par exemple, les mesures suivantes permettent de réduire l'exposition au risque d'accidents de la route :

Réduction de la probabilité

- Veiller au bon entretien des véhicules
- Faire respecter les limitations de vitesse
- Former les chauffeurs
- Éviter les déplacements de nuit en dehors des villes
- Éviter les axes très fréquentés à haut risque
- Éviter les déplacements en cas de conditions météorologiques extrêmes

Réduction de l'impact

- Veiller au port systématique des ceintures de sécurité
- Disposer de trousses de premiers secours et former le personnel
- Prévoir un extincteur
- Disposer des numéros à appeler en cas d'urgence
- Placer un triangle de pré-signalisation à bord des véhicules
- Disposer d'une assurance et de conseils

Certaines menaces comme les incendies dans les bureaux, les vols ou les accidents de la route peuvent être réduits grâce à de bonnes stratégies de prévention. Cependant, il est pratiquement impossible d'empêcher les menaces telles que les catastrophes naturelles, les défaillances au niveau de l'infrastructure ou le risque politique ; la priorité devra donc être accordée à la réaction afin de réduire l'impact sur le personnel et les programmes.

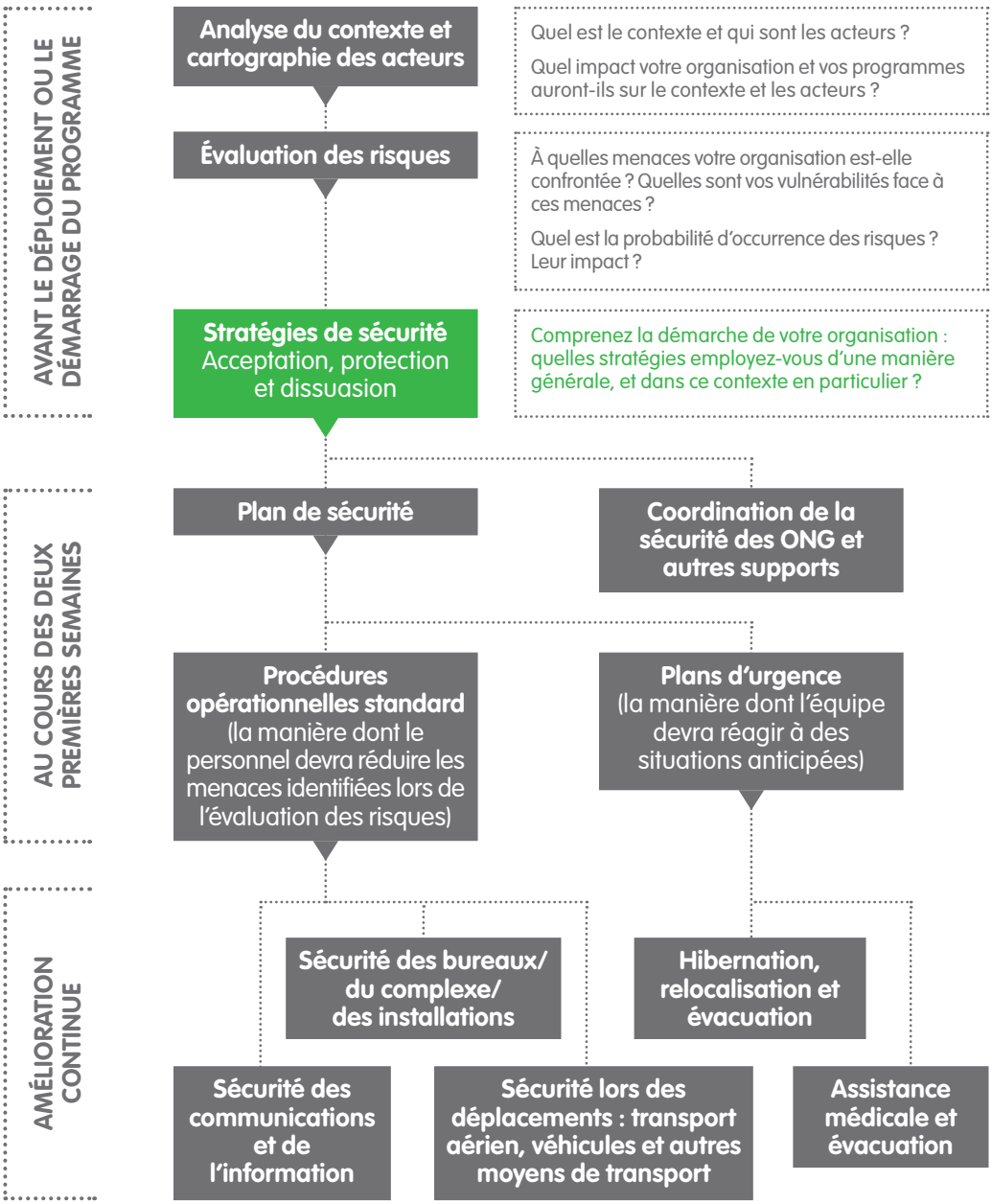
Si possible, identifiez des systèmes d'alerte précoce fiables qui sont susceptibles d'aider votre organisation à réduire le risque. Certaines mesures réactives peuvent être mises en place dans le cadre de la préparation de l'organisation, notamment la fourniture de trousses de premiers secours, la formation aux premiers secours, la constitution de stocks d'urgence ou la formation à la sécurité personnelle.

Les mesures de réduction du risque devraient correspondre à l'évaluation des risques. Par exemple, si une menace particulière est identifiée comme étant très improbable mais pouvant avoir un impact critique, le fait de ne mettre en œuvre que des mesures destinées à en réduire la probabilité n'aura qu'une incidence limitée sur la réduction du risque.

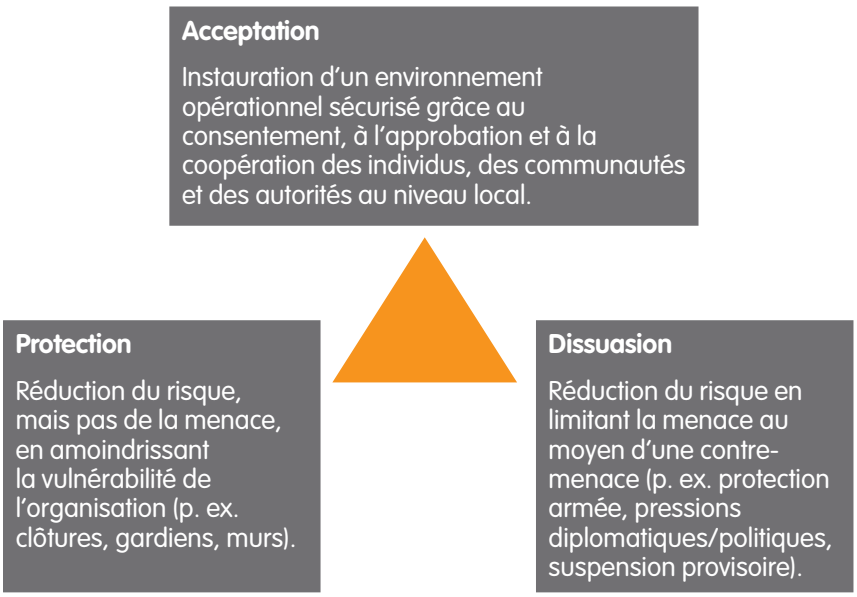
De plus en plus d'organisations choisissent de passer par des partenaires locaux pour réduire leur exposition au risque, surtout dans des contextes difficiles. Cependant, le risque est alors transféré vers les partenaires locaux. Même si la menace globale pour l'ONG locale reste la même, il est important de comprendre que les risques qui en découlent peuvent être très différents ; par ailleurs, le simple fait que l'organisation partenaire soit locale ne signifie pas qu'elle ne s'exposera pas à ce risque.

▶ *Voir le document de l'EISF « International agencies working with local partners »*

4 Stratégies de sécurité : acceptation, protection et dissuasion



Les organisations spécialisées dans l'aide humanitaire emploient généralement trois stratégies de sécurité dans différents contextes :



D'une manière générale, les agences humanitaires internationales et nationales privilégient la stratégie d'acceptation. Cependant, celle-ci peut prendre un certain temps, et les organisations qui se déploient dans de nouvelles régions ne sauraient présumer que la communauté les accepte. Une organisation pourra choisir dans un premier temps de se concentrer sur des mesures de protection et de dissuasion, jusqu'à ce que l'acceptation se soit développée. Il est toutefois important de noter que les comportements adoptés dès le premier jour auront un impact sur les futurs efforts de développement de l'acceptation.

Acceptation

Après une situation d'urgence soudaine, lorsqu'un grand nombre de nouvelles ONG internationales et nationales et d'agences de l'ONU arrivent dans une région, les gouvernements et les communautés hôtes ont souvent du mal à faire la distinction entre les différentes organisations. La situation peut être rendue d'autant plus difficile par le roulement du personnel lors des premières semaines, les premiers intervenants étant remplacés par des personnels présents sur une plus longue durée. Tous les personnels déployés et les employés locaux – y compris les responsables, les mobilisateurs communautaires et les chauffeurs – devront être briefés sur la manière dont votre organisation compte utiliser les trois stratégies et dont l'acceptation sera établie auprès de toutes les parties prenantes.

L'acceptation ne concerne pas uniquement les communautés au sein desquelles l'organisation opère, mais toutes leurs parties prenantes. Une cartographie des acteurs aidera l'organisation à identifier les parties prenantes susceptibles d'être affectées par ses programmes et les alliés sur lesquels elle pourrait compter pour se faire accepter. N'oubliez pas que les parties prenantes n'obtiennent pas leurs informations uniquement en écoutant ce que disent localement votre organisation et ses employés. En effet, de nombreuses communautés ont désormais accès à l'Internet, par conséquent les messages transmis doivent être conformes aux informations qui figurent sur votre site Internet et sur les réseaux sociaux.

L'acceptation doit se gagner et se perd très facilement, et le comportement d'un intervenant peut affecter une communauté entière.

L'acceptation doit être envisagée de manière proactive.

Principaux points :

- Expliquez clairement qui vous êtes, le profil et les priorités de votre agence, vos sources de financement et la manière dont vos programmes sont élaborés.
- Si vous êtes une organisation religieuse ou laïque, expliquez clairement ce en quoi cet aspect affecte (ou non) votre travail, notamment dans un environnement très religieux. Faites également attention à la manière dont vous pouvez être perçus.
- Comprenez qui sont vos partenaires, comment ils sont perçus et quel impact votre relation aura sur leur acceptation et la vôtre.
- Veillez à ce que les parties prenantes se sentent impliquées avant de démarrer les travaux.
- Mettez en place un système de plaintes rigoureux et veillez à en assurer le suivi.
- N'isolez pas votre personnel des communautés. Restez visibles et accessibles.

Protection

Des mesures de protection devront être élaborées conformément à l'évaluation des risques, et appliquées de manière égale à tous les niveaux du personnel (local et international) et de la hiérarchie. Les organisations devront fournir au personnel une formation aux mesures de sécurité, conseiller les nouveaux employés et poursuivre leur coordination avec les autres agences et forums de sécurité.

▶ *Voir le Module 5 – Coordination de la sécurité des ONG et autres sources de support*

La protection physique des bâtiments, complexes et/ou centres de distribution ne devrait pas donner l'impression que l'organisation construit un bunker ou un fort. Les complexes, bureaux ou espaces de travail ne devront pas contraster avec les bâtiments alentour.

▶ *Voir le Module 7 – Sécurité des installations*

Il est important d'investir dans les meilleurs systèmes de communication possibles et disponibles – radio, internet, téléphones portables, lignes fixes, satellite, fax, coursiers, etc. Les systèmes de communication devront être accompagnés de politiques de reporting (régulier ou selon un calendrier) applicables au personnel afin d'assurer la sécurité.

▶ *Voir le Module 8 – Sécurité des communications et de l'information*

Dissuasion

La dissuasion est généralement la stratégie employée en dernier recours, lorsque l'acceptation et la protection ont échoué ou se sont révélées inadéquates. Dans certains contextes, elle peut aussi être exigée par les gouvernements hôtes (p. ex. Somalie, Tchad, Niger).

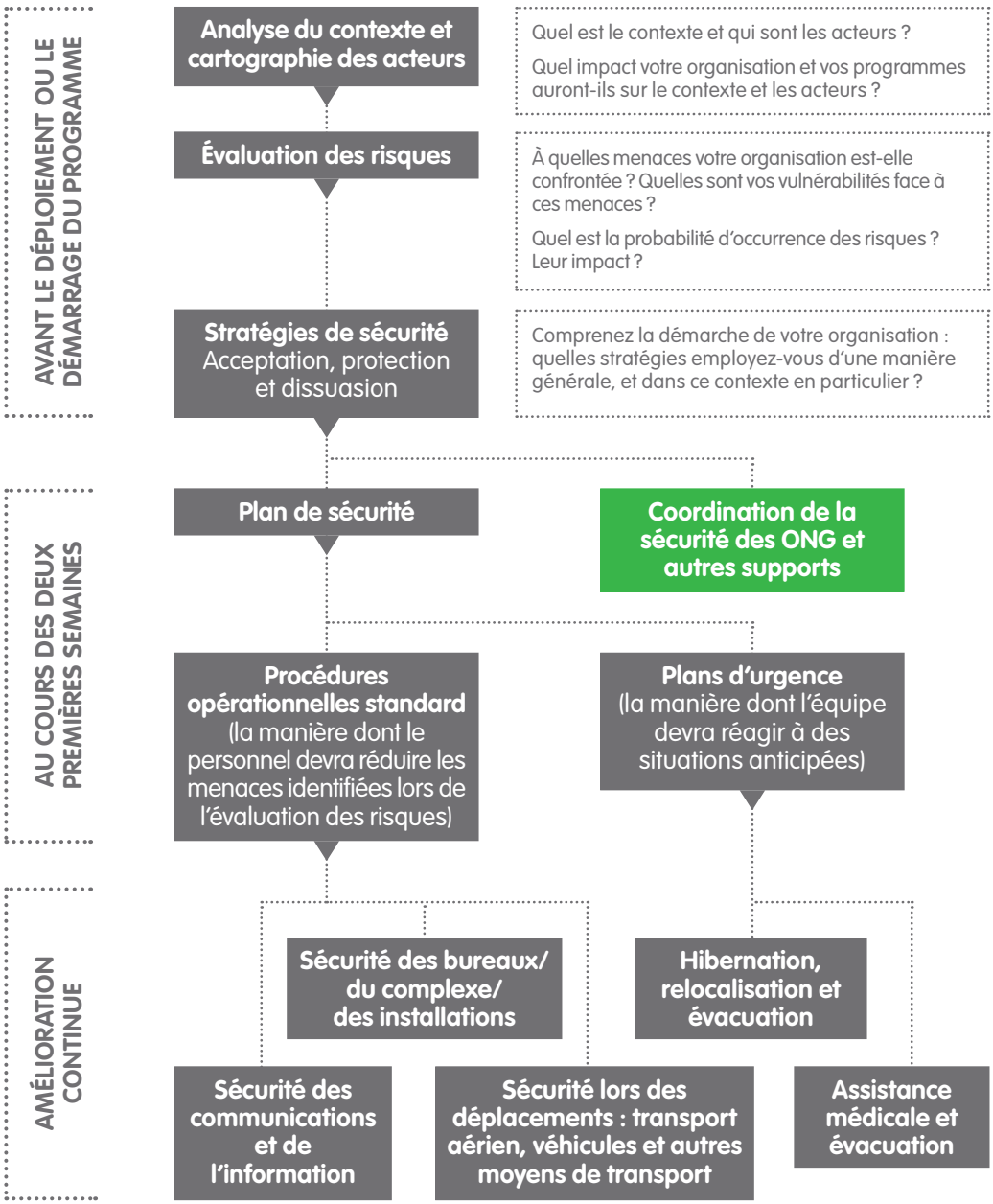
Le retrait de services est la principale menace pouvant être employée dans une région non sécurisée, mais l'organisation devra d'abord s'assurer de ne pas porter atteinte aux gouvernements locaux et aux accords passés avec les bailleurs de fonds.

Les gardes armés et les escortes militaires ou policières sont à éviter dans la mesure du possible, car ils rendront souvent l'acceptation impossible ou, du moins, très difficile – lors des phases ultérieures. Ils pourraient également accroître le risque de blessures résultant de tirs croisés, ou le risque d'extorsion ou de harcèlement.

▶ *Voir le document d'information de l'EISF « Engager les services d'entreprises de sécurité privées »*

Avant d'envisager les différentes stratégies de sécurité, il est important de comprendre la mission, la vision et le mandat de l'organisation. Les organisations sont toutes différentes, non seulement en termes de mission et de programmes, mais aussi de vulnérabilités et de capacités à y répondre. Le simple fait qu'une agence choisisse une stratégie particulière ne signifie pas que cette stratégie fonctionnera pour une autre agence, même si elles opèrent toutes les deux dans le même contexte.

5 Coordination de la sécurité des ONG et autres sources de support



Dans tous les pays où convergent des agences humanitaires pour répondre à une urgence ou une crise prolongée, différents forums et groupes de coordination sont souvent instaurés. Dans les régions où l'insécurité pose problème, des forums consacrés à la sécurité des ONG peuvent aussi être créés, que ce soit dans le cadre d'un organe de coordination d'ONG plus large, d'une entité autonome ou d'un groupe informel dont la mission est de partager et coordonner l'information.

Les forums sécurité sont généralement présidés par une organisation, et ce sont les points focaux en charge de la sécurité des organisations membres qui y participent. Ces forums servent majoritairement à partager des évaluations de contexte et des rapports d'incidents. Ils peuvent également servir à partager les coûts de la formation du personnel, à émettre des conseils concernant les recommandations des ambassades ou des gouvernements hôtes, et faire office de point de coordination centralisé avec d'autres acteurs tels que l'UNDSS. S'il existe un forum, il est vivement conseillé à l'organisation d'y participer, tant pour récolter des informations sur le contexte que pour identifier les meilleures pratiques dans ce pays.

L'adhésion à un forum sur la sécurité ne dispense pas l'organisation d'effectuer sa propre évaluation des risques et d'instaurer des relations de travail avec les acteurs clés tels que l'UNDSS ou d'autres agences.

Lorsque des membres du personnel sont désignés pour assister à ces réunions de coordination, soutenez-les en leur accordant tout le temps nécessaire pour participer au forum, et en veillant à ce qu'ils soient pleinement informés des règles de participation – en particulier en matière de gestion du partage de l'information. Aidez-les à partager les résultats des forums au sein de votre organisation afin d'optimiser les bénéfices de votre adhésion à l'organe de coordination.

Les organisations peuvent également se tourner vers des sources d'information supplémentaires pour améliorer le flux d'information sur les incidents, trouver des conseils pour réduire les risques posés par différentes menaces et améliorer leur capacité sécuritaire. Par exemple, « Saving Lives Together » (SLT) est un cadre dédié à la collaboration en matière de sécurité entre les ONG et les Nations Unies. Il comprend une série de recommandations, notamment sur le partage de l'information et des ressources, qui s'appuient sur les meilleures pratiques en matière de gestion des risques de sécurité. Si les Nations Unies n'assument aucune responsabilité en termes d'évacuation, de communications et d'autres services de support, elles peuvent coordonner ce type de services dans certains contextes.

La dernière version du cadre SLT, publiée en 2015, est accompagnée de directives sur ce qui est attendu d'une collaboration entre les ONG et l'ONU. SLT n'est pas l'apanage de l'UNDSS, mais ce dernier est l'organisme chef de file au sein du système des Nations Unies. Les interlocuteurs locaux de l'UNDSS peuvent être identifiés par l'intermédiaire des membres au siège de SLT – tels que l'EISF ou InterAction.

Autres sources d'information sur la sûreté et la sécurité :

- Gouvernements nationaux, y compris gouvernements donateurs et leurs ambassades.
- Départements gouvernementaux du pays hôte.
- Service d'aide humanitaire et de protection civile de la Commission européenne (ECHO), qui produit des documents sur la sécurité destinés aux organisations humanitaires dans certains contextes.
- Sociétés d'assurance, qui disposent souvent d'un service de conseil sur les menaces dans différents pays et/ou régions.
- Consultants sécurité d'ONG.
- Prestataires de service de sécurité commerciale locaux (sociétés de gardiennage).
- Médias internationaux et nationaux.
- Autres ONG et leurs organisations partenaires.
- Communautés hôtes et bénéficiaires.
- Personnel national.
- « Insecurity Insight ».
- Base de données « Aid Worker Security Database ».
- INSO (International NGO Safety Organisation), le cas échéant.
- European Interagency Security Forum (EISF).

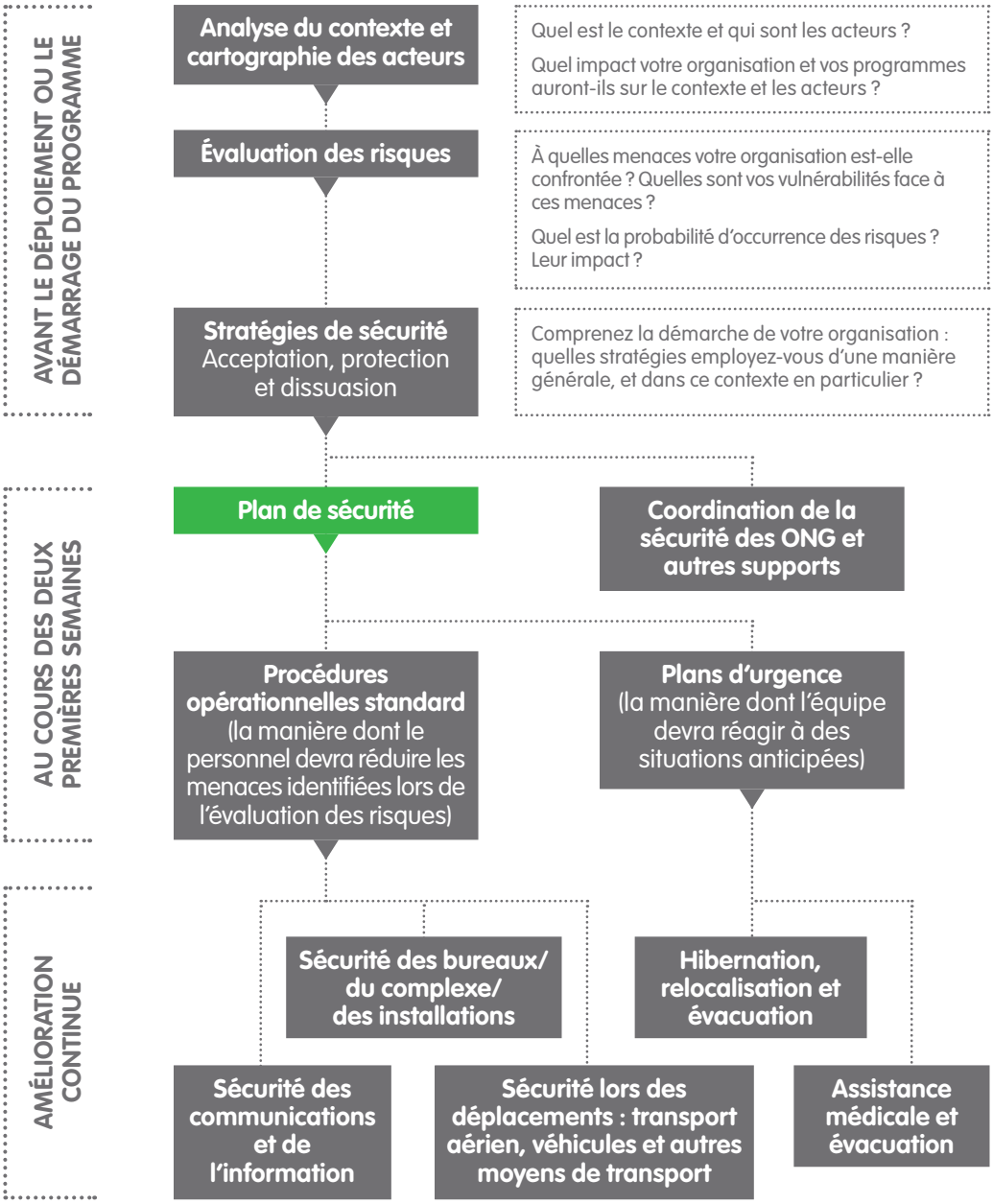
Les décisions devront s'appuyer sur des informations fiables et précises. Toutes les informations doivent être évaluées en termes de fiabilité de la source, de nombre d'organisations ou d'individus qui signalent une même information et de subjectivité au niveau local. D'une manière générale, évitez de prendre des décisions basées sur des rumeurs tant que celles-ci n'ont pas été confirmées par une source fiable.

▶ *Voir le Module 8 – Sécurité des communications et de l'information*

En cas d'urgence ou de crise, la sûreté du personnel de votre organisation voire des communautés bénéficiaires dépendra de votre capacité à prendre des décisions et à déclencher des plans d'urgence. Plusieurs systèmes peuvent servir à évaluer la qualité de l'information. La grille ci-dessous vous aidera à évaluer l'information reçue.

	Information détaillée et crédible	Information vague ou incomplète
Source fiable	Information de bonne qualité permettant de prendre une décision	Tenir compte de l'information et se la faire confirmer
Source inconnue ou peu fiable	Obtenir une confirmation d'une source connue	Ne pas ignorer cette information, mais ne pas prendre de décision sans autre source

6 Plan de sécurité



Les plans de sécurité ne sont pas des documents stratégiques. Ils doivent être simples, faciles à utiliser et fournir des informations sous un format utile pour le personnel au quotidien, faute de quoi le document ne pourra être ni lu dans sa totalité ni exploité. Pour être gérables, les plans de sécurité ne doivent pas faire plus de 20 pages – s'ils sont plus longs, le personnel ne les lira pas, ne s'en souviendra pas ou ne les utilisera pas.

Les plans de sécurité revêtent différentes formes. Cependant, la plupart sont structurés selon un format général et contiennent des informations similaires selon l'organisation, le type d'engagement, les effectifs et la taille des actifs, le lieu des projets, le contexte opérationnel et d'autres facteurs locaux.

La meilleure façon d'élaborer un plan de sécurité consiste à impliquer un large éventail de personnels, y compris les cadres supérieurs, le personnel administratif, les responsables de programme, les personnels de terrain et les chauffeurs, et en associant différents genres, nationalités et ethnicités. Chaque individu offrira une perspective différente.

En utilisant différents personnels, nationaux et internationaux, travaillant pour le bureau pays ou sur le terrain, vous pourrez susciter un sentiment d'appartenance et améliorer l'application du plan de sécurité.

Cependant, évitez de trop mettre l'accent sur l'équipe dirigeante, car le personnel en première ligne des opérations est susceptible d'être exposé à un risque plus important. De même, évitez de trop mettre l'accent sur le personnel international, et tenez compte de l'exposition au risque de l'ensemble du personnel – notamment du personnel national chargé de l'exécution des programmes. Si le plan de sécurité comprend des mesures différentes selon qu'il s'agit de personnel international, de personnel national délocalisé et de personnel local, les raisons devront en être clairement expliquées à l'ensemble du personnel. Faute d'explication, l'organisation pourrait être perçue comme ne se souciant que d'une catégorie de personnel.

Le plan de sécurité – ou au moins les sections pertinentes – devra être disponible dans la langue des usagers. Pour le personnel analphabète, et si une traduction n'est pas possible, réfléchissez à un moyen de diffuser l'information contenue dans le plan de sécurité. Il est important d'inclure et d'expliquer le plan de sécurité à l'ensemble du personnel basé dans le bureau, y compris aux agents d'entretien et aux gardiens. Les membres du personnel moins impliqués dans l'organisation que les équipes des programmes ou de gestion peuvent être plus corruptibles et donc plus susceptibles d'accepter de fournir des renseignements contre de l'argent. La connaissance de ces membres du personnel de la mission de l'agence est plus limitée et ils ont peut-être moins d'intérêt à assurer la sécurité de tout le personnel.

Si l'évaluation des risques identifie une menace, le plan de sécurité devra indiquer au personnel comment gérer le risque découlant de cette menace.

Servez-vous du modèle ci-après pour vous assurer que votre plan de sécurité contienne tous les principaux éléments.

I. Présentation générale du plan de sécurité

- Objectif du document

Pourquoi ce document est-il important pour l'ensemble du personnel ?

- Qui est chargé de préparer le plan, de l'actualiser et de former le personnel ?
- Votre seuil de risque

Quel niveau de risque votre organisation est-elle en mesure de gérer ? À quel niveau le risque devient-il trop important ?

- Votre stratégie de sécurité

De quelle manière votre organisation utilise-t-elle les stratégies d'acceptation, de dissuasion et de protection ? Comment évaluez-vous les résultats ?

▶ *Voir le Module 4 – Stratégies de sécurité : acceptation, protection et dissuasion*

- Date du document/de la mise à jour/de son examen

Quand le document a-t-il été rédigé ? Quand faudra-t-il l'actualiser ?

II. Contexte actuel – votre évaluation des risques

▶ *Voir le Module 3 – Outil d'évaluation des risques*

- Contexte global

Descriptif générique et de qualité du pays et de la région, ainsi que des défis.

- Votre système d'évaluation des risques

Comment identifiez-vous les menaces et choisissez-vous votre système ?

- Menaces dans votre contexte
- Évaluation des menaces et du classement des risques

III. Procédures opérationnelles standard (POS)

Cette partie devra comprendre les POS applicables à l'ensemble des menaces et risques identifiés dans votre évaluation des risques. Il devra s'agir de consignes simples et claires indiquant au personnel la marche à suivre pour prévenir le risque (en réduire la probabilité) et/ou réagir en cas d'incident (en réduire l'impact). Les POS doivent être présentées sous la forme de listes de contrôle, de procédures ou d'actions.

- Transport de fonds
- Communications, y compris un plan régissant l'utilisation des réseaux sociaux

Voir le Module 3 – Outil d'évaluation des risques

- Signalement des incidents
- Déplacements sur le terrain et sécurité des véhicules

Voir le Module 9 – Sécurité lors des déplacements : transport aérien, véhicules et autres moyens de transport

- Incendie dans les bureaux ou le complexe
- Accès au bureau et aux installations
- Vol
- Accident de véhicule
- Inclure les autres POS

IV. Autres sections importantes

- Santé et sécurité

Protection du personnel face aux menaces sanitaires (paludisme, VIH, etc.) et accidents, stress, trouble de stress post-traumatique (TSPT).

- Ressources humaines

Politiques relatives au recrutement, vérifications des antécédents, contrats, confidentialité, etc.

- Sécurité administrative et financière

Politiques pour empêcher le vol, la fraude, la corruption ainsi que procédures de manipulation du numéraire et politiques d'achat.

- Inclure les autres sections importantes

V. Gestion de crise

Qui sont les membres de votre équipe de gestion de crise (CMT) et de qui relèvent-ils ? De quelle manière la CMT sera-t-elle déclenchée ?

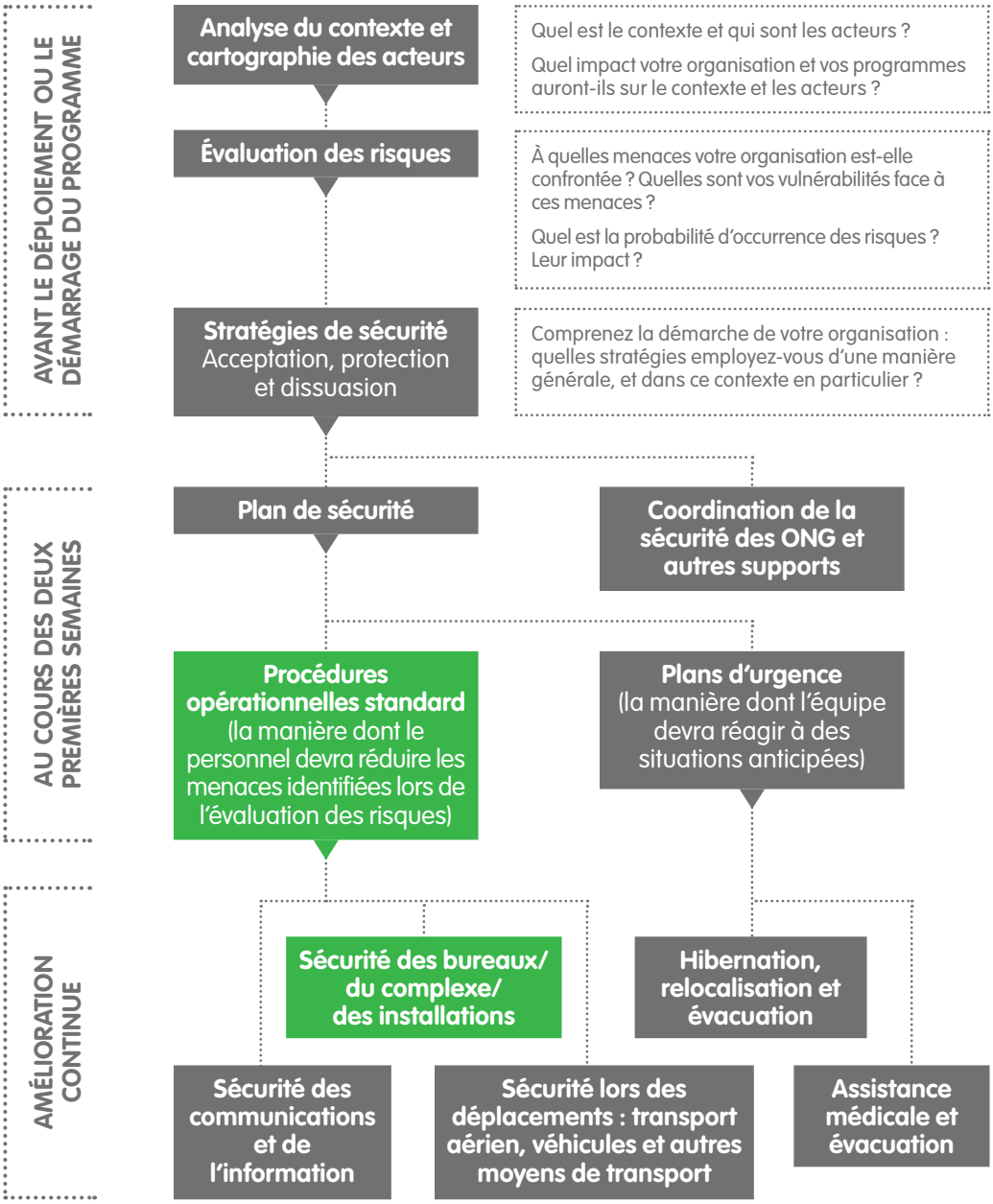
Inclure également tous les plans d'urgence pour les crises que vous estimez pouvoir se produire, notamment enlèvements, catastrophes naturelles, évacuations et conflit armé.

Contrairement aux POS, les plans d'urgence sont un outil de gestion qui n'est pas destiné à une diffusion générale.

Voir le Module 10 – Hibernation, relocalisation et évacuation

Voir le Module 11 – Assistance médicale et évacuation

7 Sécurité des installations



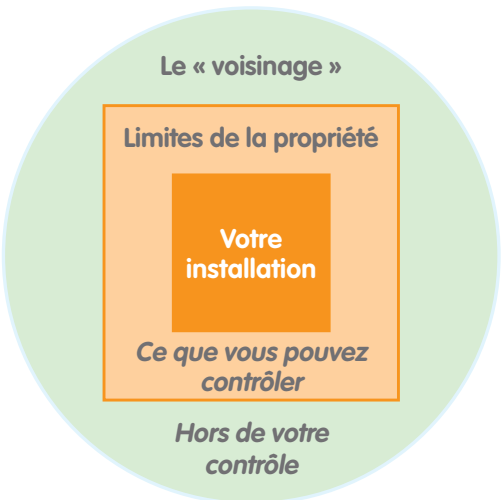
Lorsque vous recherchez un nouveau bureau, une résidence ou un complexe, passez d'abord en revue votre évaluation des risques afin de comprendre les types de menaces, le niveau de menace et le niveau de protection ou de dissuasion dont vous aurez sans doute besoin. Cela vaut également si vous emménagez dans un bureau existant avec une organisation partenaire. Demandez-vous également s'il sera possible d'élaborer une stratégie d'acceptation dans ce lieu : cela est souvent plus difficile en milieu urbain qu'en zone rurale, même s'il est toujours conseillé d'instaurer une entente mutuelle avec vos voisins.

Cela concerne tous les biens de l'organisation, à savoir ses bureaux, résidences, entrepôts, cliniques, écoles, etc.

Lors d'une réponse d'urgence, il est souvent nécessaire et/ou pratique de partager des locaux. Dans ce cas, il est important de définir qui est responsable de quoi (sécurité du périmètre, services de gardiennage, stratégie d'acceptation, etc.)

Voir le Manuel de l'EISF « Ouvrir un nouveau bureau : Manuel à l'attention des ONG »

Sécurité des bureaux, complexes et autres installations



Cercle extérieur : le voisinage

Il s'agit de la zone autour du bureau/du complexe/de l'installation/de la résidence. L'évaluation des risques devra identifier qui dans cette zone pourrait avoir un impact sur la sécurité du personnel. Vous devrez comprendre votre voisinage et les parties prenantes qui s'y trouvent pour pouvoir mettre en œuvre votre stratégie d'acceptation. Cette tâche sera peut-être plus simple en

zone rurale qu'en milieu urbain, mais notez qu'il sera essentiel d'instaurer une bonne entente avec vos voisins quel que soit le contexte.

Tenez compte des éléments suivants :

- Accès routier, tant pour se rendre au bureau que pour accéder à d'autres lieux en toute sécurité. Le bâtiment se trouve-t-il dans une impasse ? Une impasse peut être une bonne chose car elle permet d'identifier les entités hostiles, mais elle limite également vos possibilités de déplacement et vos voies d'évacuation.
- Dangers naturels tels que cours d'eau (risque d'inondation), reliefs (glissements de terrain/avalanches), marécages (paludisme/dengue) ou forêts (incendies, faune).
- Voisins – ambassades, postes militaires/commissariats, banques, bureaux gouvernementaux, autres ONG, universités.
- Distance entre le bureau et l'aéroport, les hôtels, les lieux clés en cas d'urgence.
- Structures qui constituent un obstacle/éléments naturels qui interrompraient vos communications satellite en cas d'urgence.
- Propriétaire du bien, ses antécédents et sa réputation.
- Accès fiable à de l'eau potable.
- Accès aux réseaux téléphoniques, Internet et portables.

Le cercle central : le bien immobilier

Il s'agit de la première zone placée sous le contrôle de l'organisation. L'évaluation des risques vous indiquera la procédure à suivre pour la sécuriser – mur, clôture ou haie, ou, si vous souhaitez que cette zone reste ouverte, votre stratégie de protection.

N'oubliez jamais que si vous estimez avoir besoin d'un « bunker » pour assurer votre sécurité, vous ne devriez sûrement pas vous installer dans cette zone.

Lorsque vous préparez votre périmètre, réfléchissez à l'impact que celui-ci pourrait avoir sur vos voisins et votre image, et le message qu'il transmet. Si vous préférez que votre agence passe inaperçue mais que vous entouriez ensuite votre site de barbelés, ce qui ne manquera pas d'attirer l'attention de vos voisins, cela sera contre-productif. Interrogez-vous sur la manière dont votre présence pourrait affecter vos voisins :

- Avez-vous besoin d'un groupe électrogène ? Si oui, peut-il être positionné à l'écart des autres bâtiments et/ou est-il possible de l'insonoriser ?
- Le complexe ou la zone offrent-ils suffisamment de places de parking sans gêner personne ?

- Votre présence engendre-t-elle un risque de sécurité pour vos voisins ?
- Si vous employez des gardiens, où se trouveront-ils ?

Il est tout à fait possible d'élaborer des mesures de protection qui n'affectent pas négativement l'aspect du complexe. Il s'agira par exemple de placer le barbelé en-dessous du sommet du mur, de placer les barrières de béton derrière des pots de fleurs, etc.

D'autres problèmes doivent être pris en compte au sein de votre propriété :

- Contrôle de l'accès (planifié) : de quelle manière le personnel, les visiteurs, les fournisseurs ou les membres de la communauté accèdent-ils à votre propriété ? Tenez compte des portails permettant aux véhicules/au personnel d'entrer et de sortir, des contrôles d'identité, des zones de parking sécurisées, des cartes d'identité, des zones d'attente et des méthodes de gestion des foules (le cas échéant).
- Contrôle de l'accès (non planifié) : est-il facile d'entrer dans le site ? Le périmètre que vous occupez est-il mitoyen de voisins ou d'espaces ouverts ? Y a-t-il des arbres en surplomb et à quelle distance les bâtiments se trouvent-ils des murs d'enceinte ?
- Risques d'incendie, y compris entreposage de carburants et de combustibles, câbles électriques et zones fumeurs désignées.
- Les ordures sont-elles collectées et prises en charge d'une manière sécurisée et écologique ?
- Sorties de secours : si votre complexe a un mur ou un portail principal qui fait face à la rue, de quelle manière procéderez-vous à une évacuation sans vous faire remarquer si le danger se trouve devant l'installation ? Où irez-vous ? Peut-être vers un complexe voisin/une installation de l'ONU/une autre ONG/une résidence ?

Intérieur du ou des bâtiment(s)

La sécurité des bâtiments de l'organisation, qu'il s'agisse de bureaux, de complexes, d'entrepôts ou de résidences, est cruciale car c'est là que se trouvent vos actifs les plus précieux, y compris le personnel, les équipements, les avoirs, les liquidités, les archives, et les équipements et fournitures nécessaires aux premiers secours. Les bâtiments devront avoir été conçus en tenant compte des risques naturels, par exemple construction parasismique, isolation thermique (chaud et/ou froid).

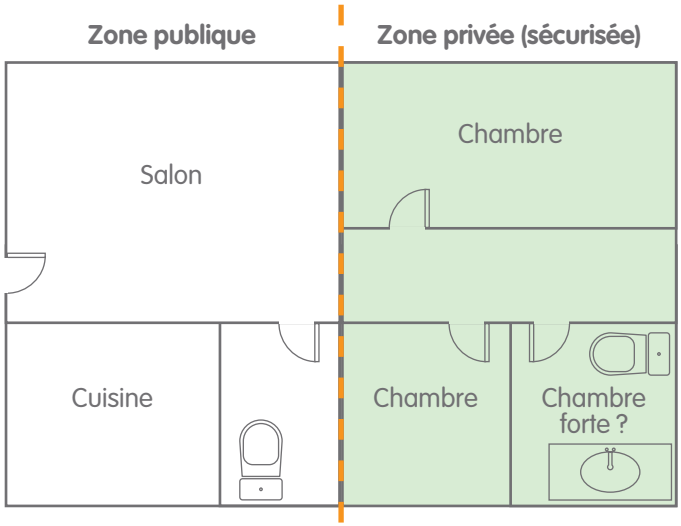
Pour veiller à fournir un travail efficace, il est important que le personnel se sente en sécurité dans son bureau et dans son logement. Tenez compte des points suivants :

- Sécurité des portes/fenêtres pour empêcher un accès non autorisé, sans pour autant empêcher le personnel de quitter les lieux en cas d'incendie/d'évacuation.

- Sécurité des zones de toiture (souvent un point d'entrée privilégié des cambrioleurs en dehors des heures de bureau).
- Zone de réception chargée de contrôler l'accès à d'autres zones vulnérables.
- Procédures de contrôle de l'accès afin que les visiteurs autorisés à pénétrer dans le bâtiment ne s'y déplacent pas sans surveillance.
- Calendrier des inspections du système électrique afin de réduire le risque d'incendie, et règles strictes visant à éviter de surcharger les prises de courant.
- Stockage sécurisé des documents, y compris coffre-fort ignifuge fixé au mur ou au sol.
- Itinéraires et procédures d'évacuation d'urgence clairement affichées et ayant fait l'objet d'exercices de simulation.
- Si nécessaire, une chambre forte capable d'accueillir tout le personnel occupant le bâtiment en temps normal ; cette chambre forte devra contenir toutes les fournitures d'urgence (trousse de premiers secours, lampe électrique, couvertures, nourriture, dispositif de communication chargé/branché, extincteur). Assurez-vous que l'équipement de communication d'urgence fonctionne dans la chambre forte. Les téléphones satellite devant se connecter à un satellite, une antenne externe sera éventuellement requise.
- Unités d'alimentation sans interruption pour protéger les ordinateurs et autres appareils électriques si l'alimentation en électricité est peu fiable ou risque de faire l'objet de coupures.
- Alarmes incendie ou effraction, et mesures à prendre lorsque ces alarmes sont activées, y compris entraînements.

Sécurité des lieux de résidence du personnel

Les résidences du personnel peuvent être considérées de la même manière, mais avec certaines précautions supplémentaires. La totalité de la résidence devra être sécurisée comme il se doit ; les objets de valeur (postes de télévision, ordinateurs, appareils ménagers, etc.) se trouvant généralement à des emplacements « publics » de la maison où des amis ou invités peuvent se trouver, ces objets peuvent être la principale cible des voleurs. Les zones privées de la résidence comprendront les zones de couchage, qui devront être davantage sécurisées que les zones « publiques ».



Tenez compte des points suivants :

- Porte solide et verrouillable entre les zones publiques et privées de la résidence.
- Sécurité renforcée des fenêtres et toits des zones privées, verrouillables de l'intérieur mais ne devant pas gêner une évacuation en cas d'incendie.
- Pièce sécurisée ou chambre forte contenant des trousses de premiers secours, des couvertures, une lampe électrique, un extincteur et un dispositif de communication chargé et testé régulièrement.
- Moustiquaires (prévention des maladies).
- Contrôle rigoureux des clés et des doubles.
- Éclairage extérieur, surtout autour des entrées.

Il est également important de tenir compte de la culture locale. Dans un environnement conservateur, vous devrez éventuellement envisager d'instaurer des zones hommes/femmes séparées, ainsi qu'une séparation entre le personnel national (gardiens, chauffeurs) et international – pour que le personnel international puisse se détendre sans offenser ni faire mauvaise impression (alcool, danse, port de tenues courtes pour les femmes, etc.).

Veilleurs et gardiens

De nombreuses organisations commencent par chercher à embaucher localement des veilleurs et/ou gardiens pour développer leurs systèmes de sécurité autour de leurs installations. Les organisations utilisent souvent le terme de « veilleurs » au lieu de « gardiens » pour faire comprendre qu'il n'est pas attendu du personnel qu'il se mette personnellement en danger pour protéger le complexe et ses actifs.

Les gardiens sont souvent le premier point de contact entre la communauté d'accueil et l'ONG. Leur comportement, leur façon de travailler et leur professionnalisme ont souvent une incidence sur la réputation de leur employeur. Par conséquent, pour tous les veilleurs et gardiens :

- Veillez à ce qu'ils aient connaissance du mandat et du code de conduite de votre organisation.
- Donnez-leur des consignes claires sur leurs fonctions et sur la manière dont ils seront supervisés.
- Fournissez-leur une liste d'« actions » à mettre en œuvre – visiteurs, activités suspectes, vol, incendie, blessures ou autres incidents susceptibles de se produire, tels qu'identifiés dans votre évaluation des risques.
- Veillez à ce que les membres du personnel traitent les gardiens avec respect et comprennent leur fonction.
- Remettez aux gardiens une liste des contacts d'urgence et fournissez-leur un moyen de communiquer en cas d'incident.

Voir le document d'information de l'EISF 'Engager les services d'entreprises de sécurité privées'

La quasi-totalité des gardiens d'ONG ne sont pas armés. Cependant, dans des environnements à haut risque, il peut arriver que des organisations disposent d'une réponse armée en cas d'urgence, qui sera déclenchée soit par un bouton d'alerte, soit par les gardiens. Si tel est le cas, l'organisation devra se renseigner pour savoir qui est le prestataire du service armé (entreprise privée, police, armée), quel est son but (protéger le personnel et les actifs de l'organisation ou appréhender les assaillants), son niveau de formation et la responsabilité de l'organisation au cas où quelqu'un (personnel, gardien, passant) se ferait tirer dessus lors d'une réponse armée.

Il existe trois grandes catégories de gardiens de sécurité : les gardiens commerciaux, les gardiens contractuels et les bénévoles communautaires. Chacune présente des avantages et des inconvénients.

Services de gardiens commerciaux

Ces agents sont fournis par une entreprise de services de gardiennage avec laquelle l'organisation a signé un contrat. L'entreprise est susceptible de faire tourner son personnel pour qu'une trop grande confiance ne s'instaure pas. Il est important, notamment dans les lieux de résidence, que les membres du personnel connaissent le gardien qui ouvre le portail. Sinon, le gardien pourra susciter une certaine insécurité au lieu de rassurer.

Avantages	Inconvénients
Le prestataire peut fournir des services supplémentaires tels qu'une équipe d'intervention rapide (assurez-vous de bien savoir ce que cela signifie), des alarmes, des réseaux radio, des patrouilles de véhicules et des gardiens de nuit.	L'organisation n'a que peu voire pas de contrôle sur les consignes que reçoit le gardien et la qualité de son travail.
Le recrutement, la formation, la paie, les RH, l'administration et le planning sont tous pris en charge par l'entreprise.	Les entreprises de sécurité cherchent surtout à faire du chiffre.
	Les gardiens sont mal payés et peu motivés.

Gardiens contractuels

Les gardiens contractuels sont employés directement par l'organisation.

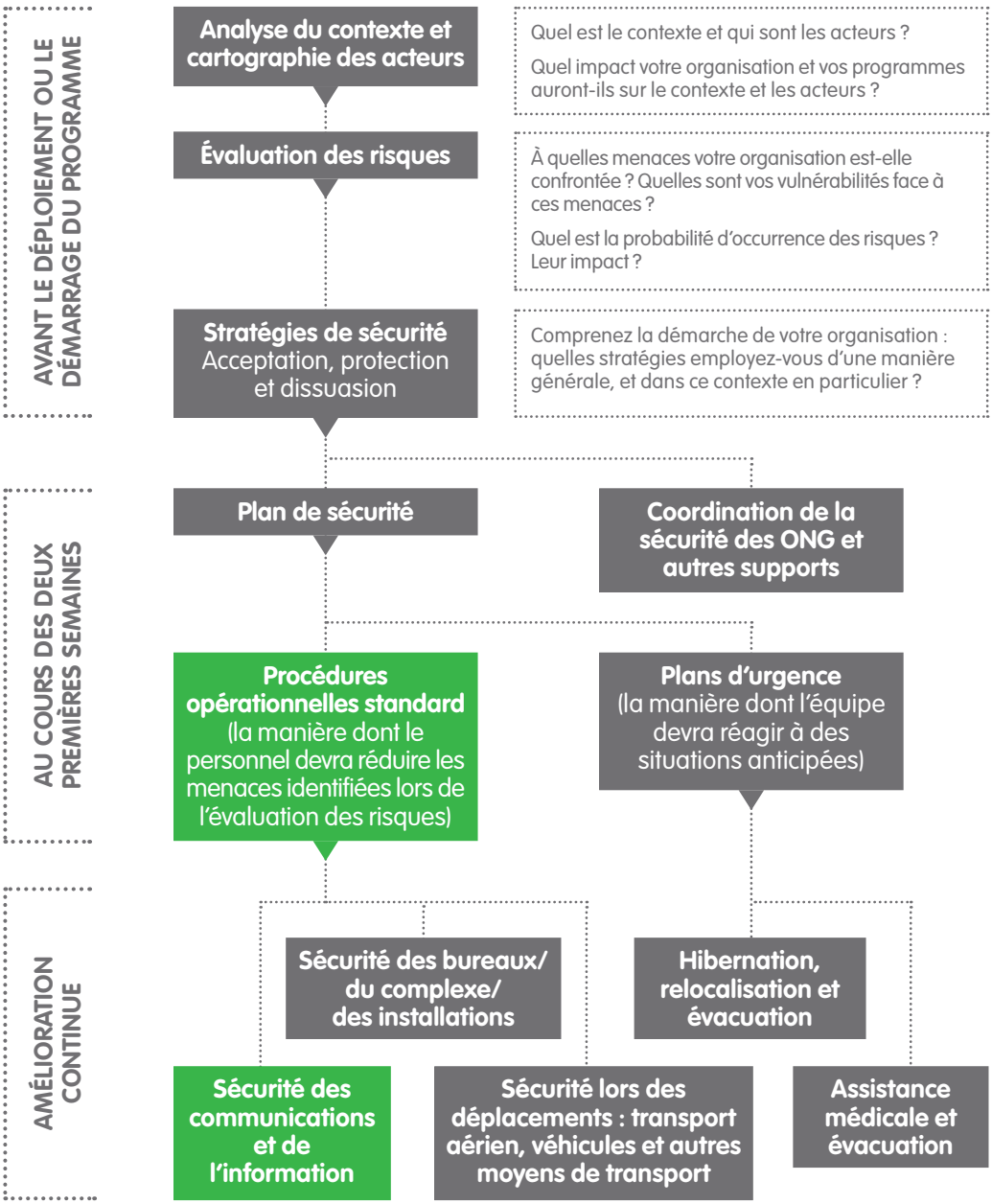
Avantages	Inconvénients
Les gardiens sont parfois mieux payés puisque l'ONG ne paie pas une entreprise.	L'organisation doit se charger elle-même de la formation, des uniformes, des équipements, de l'administration et de la supervision.
En tant que membres du personnel, leur loyauté est meilleure et ils connaissent mieux les normes, règlements et codes de conduite de l'organisation.	Aucun support supplémentaire.

Bénévoles communautaires

En temps normal, il s'agit de gardiens fournis par la communauté d'accueil dans les zones de programme. Dans les zones reculées, ils sont souvent la seule option disponible. Ils ont normalement un coût en termes de salaire, de formation et d'équipement de base.

Avantages	Inconvénients
Recours à la « stratégie d'acceptation » en faisant participer la communauté à la sécurité.	Pas de normes homogènes pour leurs fonctions.
	Manque de redevabilité.
	Susceptibles de donner lieu à des abus.

8 Sécurité des communications et de l'information



Lors de la mise en œuvre d'un nouveau déploiement, d'un nouveau projet ou d'une nouvelle mission, il est important de prendre le temps de s'interroger sur les types de communications qui seront disponibles (réseaux fixe et mobile, téléphones satellite, Internet, courrier postal, service de coursiers, etc.) et sur leur fiabilité. De nos jours, les communications sont tout aussi essentielles pour la « survie » que l'accès à de la nourriture, à de l'eau et à un abri.

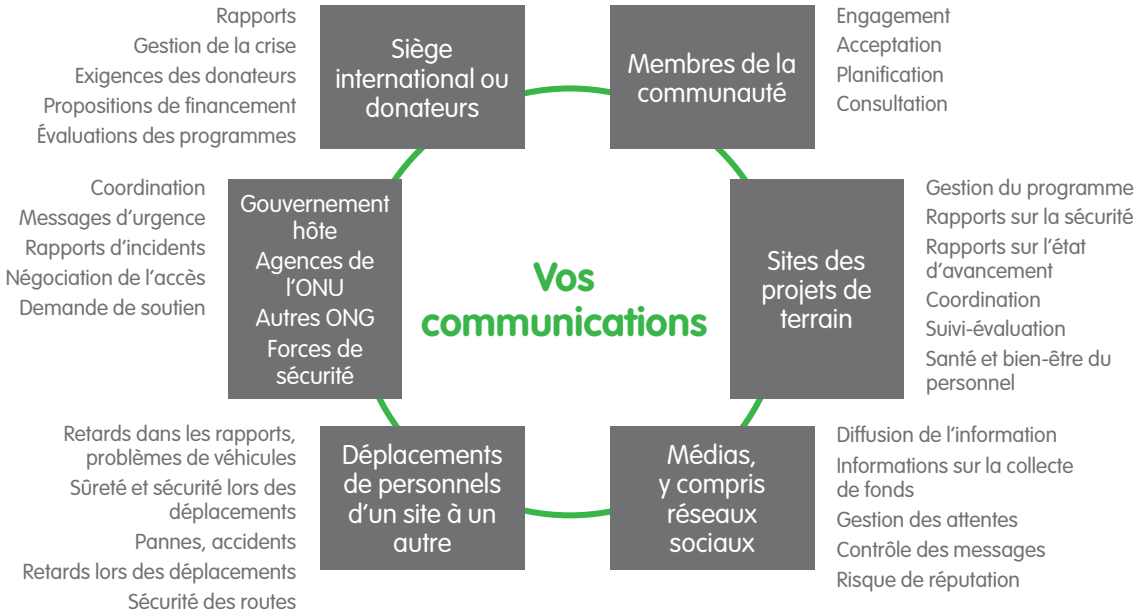
Que ce soit pour assurer la sécurité des personnels ou la réussite des programmes, il est crucial de prévoir à un stade précoce votre budget dédié à des systèmes de communications fiables – y compris à des systèmes alternatifs et de secours pour remplacer les équipements endommagés, perdus ou volés. En outre, certaines formes de communications telles que la radio et le satellite peuvent nécessiter une licence. Les Nations Unies pourront éventuellement vous aider à obtenir cette licence. Votre organisation devra prévoir un budget pour le temps d'antenne et/ou l'obtention de licences le cas échéant.

Renseignez-vous sur les nouvelles technologies susceptibles d'améliorer de manière rentable vos communications, par exemple les « sacs-à-dos satellite » pour téléphone portable ou les dispositifs de messagerie par satellite, au lieu des téléphones vocaux traditionnels. Investissez dans le meilleur équipement possible pour votre budget.

Mais les organisations doivent aussi tenir compte de l'image que donnent ses équipements de communication. Si la discrétion fait partie de leur stratégie de sécurité, la pose de radios HF et d'antennes sur les véhicules les distingueront autant qu'un logo.

Dans les régions en proie à un conflit ou à des troubles civils, ou bien après une catastrophe naturelle, ne présumez jamais que vous pourrez vous servir d'Internet et des réseaux mobiles. Lors d'urgences sécuritaires ou de catastrophes naturelles, il est fréquent que les gouvernements prennent le contrôle des réseaux (voire les verrouillent) – juste au moment où vous en avez le plus besoin. Il est important de ne jamais se fier à un seul système – réseau fixe, mobile, téléphones satellite, Internet, etc.

Faites preuve de créativité. Dans une situation d'urgence, les ONG recourent à toute une chaîne de chauffeurs de taxi se relayant pour maintenir la communication avec leur personnel lorsque les téléphones ou Internet ne fonctionnent plus, ou utilisent des dromadaires pour transporter des messages et maintenir le contact avec les communautés de zones reculées.



Sécurité et procédures en matière de communications

L'instauration et l'entretien d'un vaste réseau de communications sont essentiels pour la sûreté, la sécurité et la réussite des opérations. Si vous disposez de réseaux radio ou de téléphones satellite, apprenez au personnel à s'en servir pendant leur formation initiale et montrez-leur où utiliser les équipements de communication installés (p. ex. faut-il être dehors pour s'en servir ? Y a-t-il certains endroits où ils ne fonctionneront pas ?). Veillez à ce que les membres du personnel puissent communiquer avec leur famille et leurs amis lors de déploiements, surtout en cas d'urgence.

De plus en plus d'organisations et d'organismes de coordination utilisent WhatsApp et d'autres applications sociales de ce type pour diffuser l'information directement entre membres du personnel. Cela peut être bénéfique car l'information est ainsi partagée en temps réel, mais elle n'est pas vérifiée. Veillez à mettre en place des directives claires sur les informations pouvant être partagées ou non, et des procédures à suivre une fois l'information reçue.

D'une manière générale, il faut discuter avec le personnel de toutes les procédures et directives relatives aux communications. Affichez les procédures écrites, ainsi que les informations sur les contacts en cas d'urgence, y compris les numéros de téléphone, les fréquences et les codes, dans le bureau, à bord de chaque véhicule et sur une carte que les membres du personnel garderont sur eux.

Il est important de tester les systèmes régulièrement et d'avoir des équipements et fournitures de secours pour recharger les radios et les téléphones mobiles et satellite.

Bonnes pratiques :

- Le personnel ne transmet jamais d'informations sensibles – notamment sur le transfert d'argent liquide ou des projets de voyage – en langage clair par radio ou via les réseaux téléphoniques.
- Les équipements de communication, dont les radios, les téléphones cellulaires et satellite, ont l'accord du gouvernement du pays hôte et disposent des licences nécessaires avant d'être utilisés.
- En cas d'utilisation de radios, différentes fréquences VHF et HF sont, si possible, obtenues pour chaque bureau.
- L'utilisation de réseaux radio d'autres organisations – par exemple des Nations Unies – a été coordonnée.
- L'envoi de SMS, d'appels par téléphone satellite ou de vérifications par radio avec des bureaux éloignés et les personnes en déplacement a lieu régulièrement, en fonction des besoins. Il existe des règles pour les cas où un membre du personnel ou une équipe ne se signalerait pas ou ne serait pas joignable. Tout le personnel a connaissance de ces règles, qui sont appliquées de manière systématique.
- Des codes de contrainte (mots ou phrases) ont été choisis pour les conditions d'urgence communes telles que les enlèvements et les intrusions. Leur utilisation a été présentée au personnel.
- Les radios et téléphones d'urgence font l'objet d'une surveillance 24 heures sur 24 si nécessaire.

Sécurité de l'information

Quelle que soit l'image que nous ayons nous-mêmes de notre agence, les organisations humanitaires internationales ne sont plus considérées comme des entités neutres et indépendantes. Elles interviennent, exigent des comptes, défendent certains principes et souvent assument des tâches plus généralement associées aux pouvoirs publics (soins de santé, eau, assainissement, secours d'urgence) et, dans de nombreux cas, tout en étant financées par des gouvernements « occidentaux » avec un agenda politique bien précis. Ainsi, aux yeux d'un grand nombre de personnes, toutes les activités des ONG humanitaires semblent suspectes.

▶ *Voir le document d'information de l'EISF « The future of humanitarian security in fragile contexts: an analysis of transformational factors affecting humanitarian action in the coming decade »*

Les gouvernements ont généralement les moyens de contrôler les appels téléphoniques passés par les organisations, leur activité Internet, leurs communications via Facebook, Twitter et RSS, et de récupérer des informations sur vos disques durs. Les organisations criminelles peuvent aussi estimer que les ONG sont riches étant donné les véhicules, les ordinateurs portables et les téléphones satellite qu'elles utilisent, et les annonces publiques relatives aux niveaux de financement des donateurs. Tout cela expose l'information des agences humanitaires à un risque de sécurité. N'oubliez pas que tout ce que vous écrivez dans un courriel peut être lu par des criminels ou des agents du gouvernement.

▶ *Voir le document d'information de l'EISF « Communications technology and humanitarian delivery: challenges and opportunities for security risk management »*

Réfléchissez aux documents que vous voulez enregistrer sur un lecteur commun. Le personnel d'urgence, qui arrive souvent avec ses propres ordinateurs, copiera tout sur un lecteur commun à son départ, dans un souci de continuité. Parmi les documents copiés, il pourrait se trouver des photos inappropriées, des informations personnelles et des analyses de contexte susceptibles d'être jugées injurieuses par d'autres acteurs ou employés. En outre, faites attention à l'information – professionnelle et personnelle – qui se trouve sur les appareils mobiles, par exemple dans les téléphones portables, qui peuvent facilement être perdus ou volés.

Évaluez l'impact que l'information pourrait avoir si elle parvenait en de mauvaises mains – harcèlement du personnel, diffusion de photos inappropriées, accès aux courriels ou au VPN/serveur du bureau, et ainsi de suite.

Bonnes pratiques :

- Une sauvegarde de tous les fichiers est effectuée régulièrement et les copies de tous les documents et dossiers clés (accords gouvernementaux, documents juridiques, fichiers bancaires, dossiers RH) sont conservées hors site pour les préserver en cas d'incendie, d'inondation, de vol ou de tout autre événement susceptible de détruire les originaux.
- Les documents papier facilitent également les fuites d'information s'ils sont laissés dans une poubelle ou sur un bureau, permettant ainsi aux agents d'entretien, à d'autres membres du personnel ou aux visiteurs de les lire/copier/dérober. Veillez au déchiquetage de tous les fichiers qui ne sont pas gardés en lieu sûr.
- Veillez à doter tous les serveurs de bons systèmes de pare-feu de sécurité et à minimiser l'accès du personnel aux réseaux via des ordinateurs, des

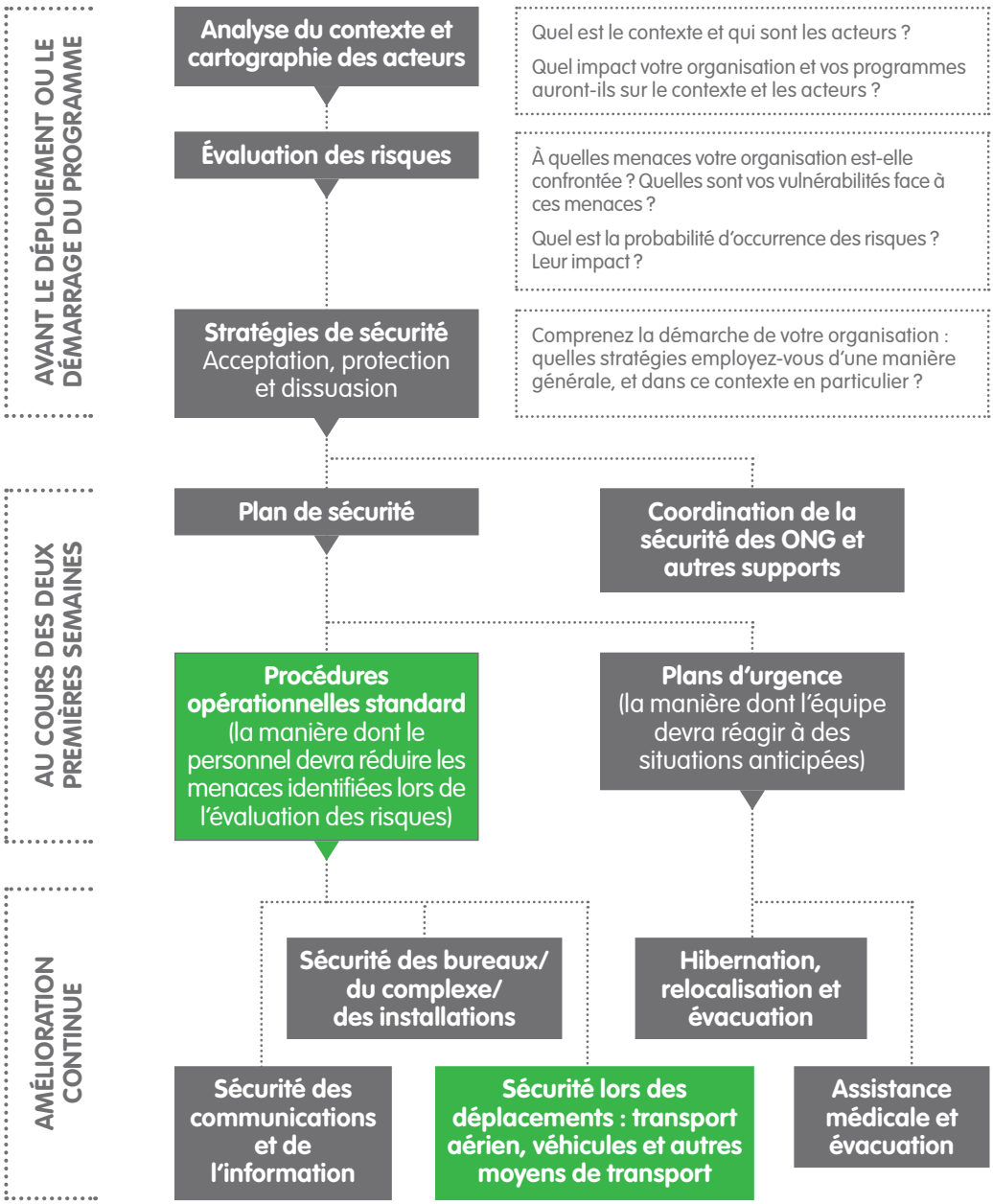
tablettes ou des téléphones n'appartenant pas à l'organisation, ce afin d'éviter de propager des virus.

- Notez que Skype est tout aussi peu sécurisé contre le piratage que les autres modes de communication.
- Ne donnez jamais l'impression de collecter des « renseignements » ou de transmettre des informations militaires ou de sécurité à des gouvernements étrangers (y compris donateurs ou votre siège). De même, le cryptage de l'information peut donner une impression erronée de votre travail. Surtout si votre ONG fait valoir ses qualités d'ouverture et de redevabilité, on risque de vous interroger sur les raisons qui vous poussent à crypter des documents.
- Dans la mesure du possible, évitez les ordinateurs de bureau. Même si les ordinateurs portables sont plus faciles à voler, ils sont aussi plus transportables en cas de relocalisation du bureau ou du projet.
- Envisagez de mettre en place des processus de vérification des informations reçues par WhatsApp et d'autres applications sociales qui facilitent le partage d'informations directement entre membres du personnel. Publiez également des directives claires sur l'information qui peut ainsi être diffusée ou non.
- Veillez à disposer d'un règlement en matière de réseaux sociaux qui indique clairement au personnel ce qu'il peut et ne peut pas publier sur les réseaux sociaux.

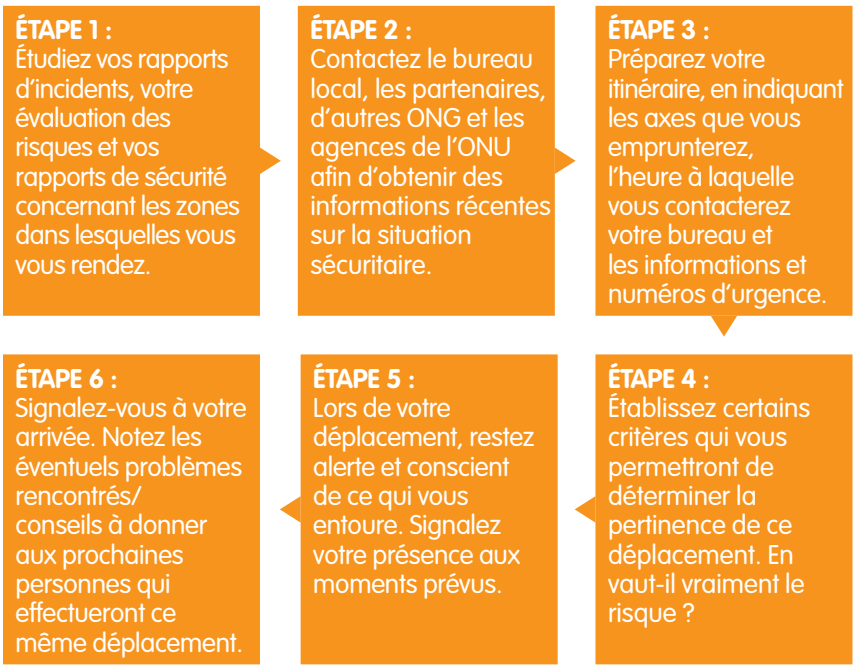
▶ *Voir le manuel de l'EISF « Gérer le message : Gestion de la communication et des médias en cas de crise de sécurité »*

Concernant les outils techniques et directifs, « Front Line Defenders » et « Tactical Technology Collective » ont développé le guide *Security in-a-Box* consacré à la sécurité numérique des activistes et des défenseurs des droits humains. Ce guide couvre les principes fondamentaux, et fournit notamment des conseils sur l'utilisation sécurisée des plates-formes de réseaux sociaux et des téléphones portables. Il donne aussi des consignes détaillées sur l'installation et l'utilisation des logiciels et services essentiels en matière de sécurité numérique.

9 Sécurité lors des déplacements : transport aérien, véhicules et autres moyens de transport



D'après le rapport *Aid Worker Security Annual Report* de 2014, sur les 795 travailleurs humanitaires tués entre 2006 et 2013, 263 (33 %) ont trouvé la mort sur la route suite à une embuscade. C'est lors des déplacements que les personnels d'ONG sont le plus susceptibles de faire l'objet de vols, d'attaques, d'enlèvements, d'actes de corruption, et d'être blessés ou de trouver la mort. Cela comprend les déplacements internationaux par avion, les trajets par route depuis l'aéroport vers le bureau ou le lieu de résidence, depuis le bureau vers le lieu de résidence, depuis les projets de terrain aux réunions et inversement, et partout où le personnel se déplace.



Bonnes pratiques :

- Restez joignable autant que possible lors de vos déplacements.
- Laissez une copie de votre itinéraire, des documents clés et des coordonnées de vos interlocuteurs locaux pour le cas où une communication directe ne pourrait être établie.
- Confirmez tous les visas, lettres d'invitation, devises locales, adresses et numéros de téléphone avant votre départ.
- Faites une copie de tous les documents importants que vous emporterez – passeport, visa, assurance, carte de crédit – et confiez ces copies au point de contact de votre département. Dans certains cas, il pourra être utile de vous munir d'une copie de votre passeport (y compris des pages où figure votre visa) et de conserver l'original dans un coffre-fort.

- Envoyez-vous par courriel une copie des documents importants pour pouvoir y accéder facilement depuis n'importe quel ordinateur.
- Procurez-vous un permis de conduire international, si nécessaire.
- Prenez votre carnet de vaccination.
- Selon la situation, prévoyez une assurance médicale/évacuation/autre.
- Renseignez-vous sur la nécessité de prendre certaines précautions sanitaires (médicaments, trousse de secours, purificateur d'eau).

Il peut être utile de répéter certains scénarios avant un déplacement, surtout si vous vous rendez dans une région nouvelle ou dans un contexte instable. Tout le personnel impliqué pourra débattre des scénarios possibles et des réponses à y apporter, et sera ainsi mieux préparé en cas d'incident.

Avant un déplacement pour raison professionnelle, il est utile que votre agence vous remette un document d'identité personnalisé de l'organisation. Ce document vous permettra de montrer rapidement que vous êtes en déplacement pour le compte de l'organisation. Ce n'est pas un moyen d'identification formel, mais il pourra vous être utile pour communiquer l'objectif de votre visite, en vous conférant un statut spécifique. Ayez toujours ce document sur vous. Si nécessaire, munissez-vous également d'une lettre de garantie. Celle-ci indiquera l'objectif de votre visite et les personnes auprès desquelles vous vous rendez.

Voyages en avion

Pour parcourir de longues distances, l'avion est souvent inévitable. En cas de voyages aériens, et notamment régionaux et nationaux, il est important d'étudier le bilan de sécurité de la compagnie aérienne en question et d'identifier si elle est certifiée IATA, EU et FAA, faute de quoi votre assurance pourrait ne pas être valide. Parmi les sites Internet permettant de consulter le bilan de sécurité des compagnies aériennes, citons FlightSafe, SkyTrax et AirlineRating.

Bonnes pratiques :

- Si possible, choisissez un avion de plus de 30 places. En principe, ceux-ci observent des règles de sécurité plus strictes et des normes de fabrication plus rigoureuses.
- Choisissez des vols directs – la plupart des accidents ayant lieu au décollage ou à l'atterrissage.
- Choisissez un siège situé à proximité d'une issue de secours et mémorisez l'emplacement.
- Choisissez si possible un siège côté allée pour que vous puissiez vous lever et réagir plus vite en cas d'urgence. C'est également meilleur pour votre

circulation sanguine car vous pourrez plus facilement vous lever et vous étirer.

- Ne buvez pas (ou que peu) d'alcool, la pressurisation de la cabine amplifiant les effets de l'alcool sur l'organisme.
- Renseignez-vous pour savoir quels bagages peuvent être pris en cabine, et préparez-vous à ce qu'ils soient fouillés.
- Ne laissez jamais de bagage, en cabine ou destiné à être placé en soute, sans surveillance.
- Veillez à ce que votre bagage cabine contienne tous les articles dont vous aurez besoin si votre bagage en soute est égaré, endommagé ou retardé.

À votre arrivée à l'aéroport, vous devrez avoir une liste de contacts répertoriant les principaux interlocuteurs et, ainsi, vous saurez quoi faire si vous ne voyez pas de chauffeur – où attendre ? Devez-vous prendre un taxi ou non ? Si oui, quel type de taxi ? Vous devrez avoir un moyen de contacter le personnel du siège et du bureau local en cas de problème, par exemple si votre vol a du retard ou si vous avez manqué votre correspondance. Convenez avant votre départ du lieu de rencontre et du mode de transport depuis l'aéroport – ces détails font partie des spécifications sécurité que tout membre du personnel doit prévoir avant son départ.

Selon le contexte, le nom et une photo du chauffeur, ou un moyen de l'identifier, vous seront transmis. Les chauffeurs doivent avoir un carton faisant apparaître le logo de l'organisation et non pas le nom de la personne qu'ils sont venus chercher.

En effet, si votre nom est inscrit sur ce carton, il sera facile pour une personne mal intentionnée de vous aborder ; un nom peut aussi être facilement copié sur une fausse pancarte.

Des informations de sécurité actualisées devront vous être données dès que possible après votre arrivée, de même qu'une carte indiquant les principaux sites et numéros de téléphone.

Voyages par route

Si vous achetez ou louez votre propre véhicule, veillez à ce qu'il soit adapté à votre mission. Tenez compte de votre évaluation des risques – marquage, visibilité, statistiques des vols par catégorie de véhicule, état des routes et du terrain, possibilité d'obtenir des pièces de rechange et autres questions d'ordre logistique.

Si vous louez un véhicule, déterminez s'il vaut mieux le louer avec chauffeur ou bien utiliser les chauffeurs de l'organisation. Si vous souhaitez faire appel aux chauffeurs de l'organisation, ceux-ci devront être en mesure d'effectuer des travaux d'entretien de base – changer un pneu, vérifier le moteur, les

freins, la batterie et le liquide de refroidissement. Si vous envisagez de vous déplacer à bord de véhicules d'un partenaire local, vérifiez ses politiques en matière de formation et de supervision du conducteur, les carnets d'entretien et les procédures de sécurité lors de déplacements. Les chauffeurs doivent observer le code de la route local et rouler à une vitesse adaptée aux conditions. Les passagers sont également chargés de s'en assurer.

L'ensemble du personnel – national et international – devra aussi être informé de la politique relative aux passagers non autorisés, notamment aux militaires ou aux membres de milices armées. De même, un règlement clair concernant l'utilisation des véhicules à des fins personnelles pendant et après la journée de travail, le week-end et les vacances devra être en place et communiqué à tous les membres du personnel. Le personnel national et international devra disposer de tous les papiers nécessaires, y compris d'un permis de conduire.

Lors de leurs déplacements, il est important que tous les occupants du véhicule (y compris le conducteur) aient une certaine connaissance de l'organisation, au cas où ils seraient arrêtés et interrogés séparément. En outre, il faudra veiller à désigner un porte-parole avant le départ.

Si possible, déplacez-vous en compagnie d'au moins une autre personne. Signalez par avance votre temps de trajet et votre destination conformément aux procédures établies. Un plan de communication indiquera dans le détail l'heure à laquelle vous devrez vous signaler et les mesures à prendre en cas de non-signalement ; la marche à suivre en cas d'accident du véhicule devra être élaborée et tout le personnel informé. Si vous n'arrivez pas à l'heure prévue, la politique de communication devra être mise en œuvre de manière systématique.

▶ *Voir le Module 8 – Sécurité des communications et de l'information*

Pour que les signalements puissent être effectués tout au long du déplacement, tous les téléphones portables devront être entièrement chargés et fonctionner dans la région de la mission. Dans le cas contraire, des équipements et protocoles de communication alternatifs devront être envisagés. Lors de votre évaluation des différents systèmes, tenez compte du fait que leur disponibilité variera selon l'itinéraire emprunté. Si vous avez le choix entre plusieurs routes, choisissez les axes primaires et alternatifs afin d'éviter les zones qui présentent un danger et adaptez-vous à l'évolution des conditions sécuritaires. Il est utile de disposer au bureau d'une carte routière du pays ou de la région et de l'actualiser régulièrement en indiquant les zones dangereuses ainsi que celles où le réseau cellulaire est inaccessible.

Bonnes pratiques :

- Les véhicules sont équipés d'outils élémentaires, d'une roue de secours, du matériel nécessaire pour changer une roue, d'une trousse de premiers secours, de couvertures, d'une réserve d'eau potable (2 litres par personne et par jour), d'un triangle de signalisation, d'une lampe électrique, d'un extincteur et de tout le matériel nécessaire au vu des conditions géographiques/climatiques.
- Des ceintures de sécurité/harnais sont installés et en bon état de fonctionnement, et leur port est systématique à l'avant comme à l'arrière du véhicule.
- Les véhicules sont vérifiés tous les jours. Une personne a été désignée pour en assurer l'entretien et les réparations.
- Les documents d'immatriculation et autres papiers se trouvent à bord de chaque véhicule.
- Le port du casque est systématique lors des déplacements à moto.
- Les réservoirs de carburant du véhicule sont toujours au moins à moitié pleins, si possible.
- Un double des clés du véhicule est conservé en lieu sûr dans chaque bureau.
- Les portières du véhicule sont verrouillées lors des déplacements et le nombre de vitres ouvertes est réduit au minimum.
- Les véhicules n'ont pas de vitres foncées ou teintées pouvant gêner la visibilité.
- Un système basé sur les formulaires de déplacement, les titres de transport ou la géolocalisation du véhicule est en place pour contrôler les déplacements.
- À bord de chaque véhicule se trouve une liste indiquant les coordonnées des contacts en cas d'urgence de tous les individus pertinents, des organisations, des hôpitaux et des commissariats de la région.

Il est bon de tenir à jour un carnet de bord de chaque véhicule et de disposer à bord du véhicule d'une copie de la liste de contrôle et du carnet d'entretien, des titres de transport, des procédures de communication, des documents, cartes, etc. Cependant, tenez aussi compte de la manière dont cette information sera perçue si le véhicule était fouillé à un poste de contrôle.

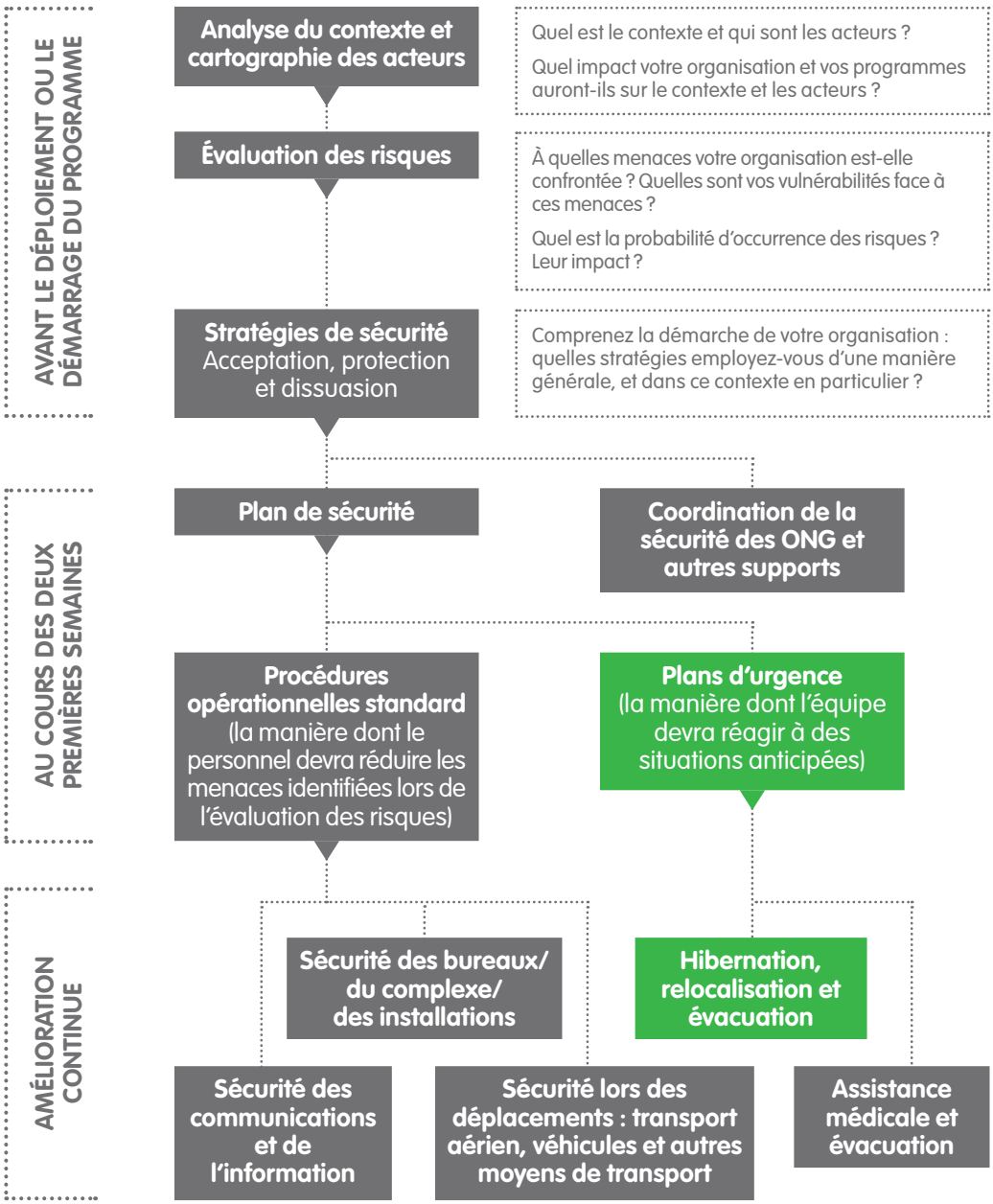
Autres moyens de transport

Dans certains contextes, il sera nécessaire, ou plus économique, d'utiliser des moyens de transport alternatifs. Citons notamment le bateau, le train, les transports en commun et les taxis. Effectuez une brève évaluation des risques pour chaque moyen de transport, notamment en étudiant les risques et en élaborant autant de stratégies de réduction du risque.

Les organisations devront prendre des précautions supplémentaires en cas de déplacements en bateau. Il est important de s'assurer que le conducteur de l'embarcation ou l'organisation dispose d'équipements tels que des gilets ou bouées de sauvetage et des radiobalises de localisation des sinistres (RLS). En outre, l'organisation devra éventuellement fournir des cours de natation ou de sauvetage.

En cas d'utilisation de transports en commun, tenez compte des besoins du personnel national et international pour ses déplacements entre le lieu de résidence et le bureau, pendant et après les heures de travail, et pendant son temps libre et/ou ses congés.

10 Hibernation, relocalisation et évacuation

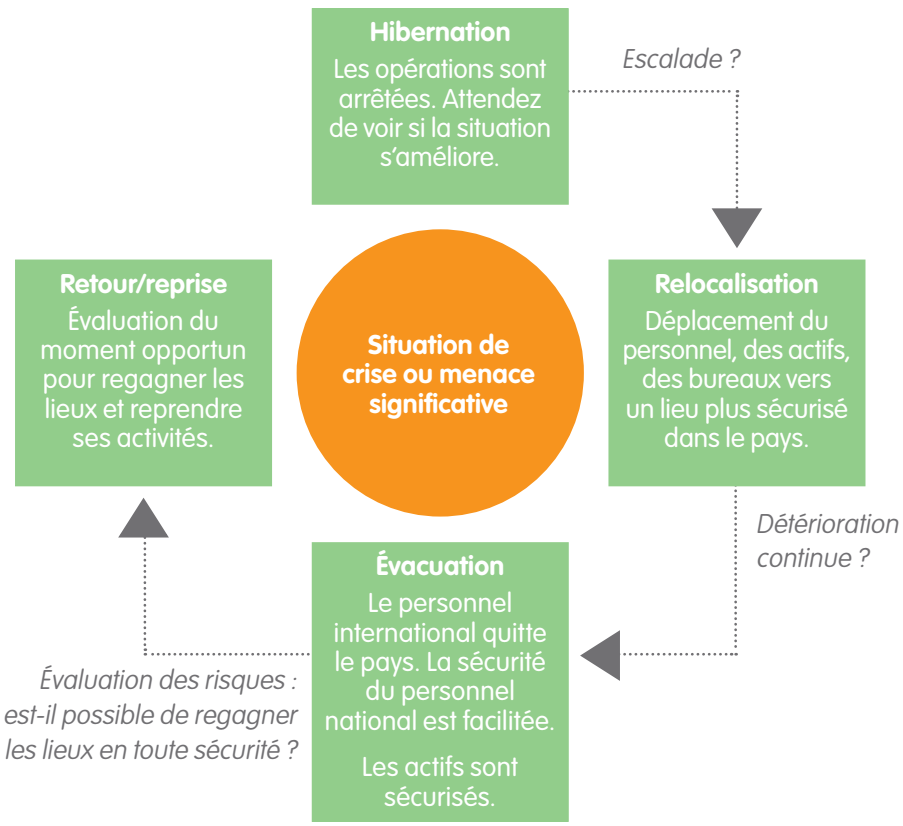


Les agences d'aide humanitaire opèrent souvent dans des régions frappées par des catastrophes naturelles ou par des conflits qui menacent l'environnement humain. Il est donc important de réfléchir à la façon dont votre organisation réagira face à une situation qui la place dans une situation d'insécurité, que ce soit pour une durée courte ou plus longue. Il existe trois niveaux de réponse à un changement significatif au niveau du contexte de menace :

L'hibernation : Pendant une période de crise, le personnel reste à son domicile et le programme est provisoirement interrompu. Dans certains cas, le personnel devra trouver refuge au bureau ou au sein du complexe.

La relocalisation : Déplacement des bureaux et/ou activités vers un site plus sécurisé, généralement de manière provisoire et dans le même pays.

L'évacuation : Suspension des opérations dans un pays, évacuation du personnel international vers un autre pays et du personnel national depuis les zones de déploiement vers leur zone d'habitation d'origine. Une programmation limitée peut se poursuivre grâce à des outils de gestion à distance, selon la situation.



Il est important d'identifier les critères convenus entre le personnel pays et le siège pour déterminer le moment où les plans d'urgence doivent être déclenchés. Par exemple, dans le cas d'inondations, les plans d'urgence d'hibernation ou de relocalisation peuvent être déclenchés lorsque les niveaux de précipitations atteignent des niveaux historiques susceptibles d'engendrer des inondations. Si un conflit armé dans une autre région du pays prend de l'ampleur ou se propage à une zone dont il aura été convenu, les plans de relocalisation peuvent être activés.

▶ *Voir le Glossaire*

En convenant par avance de ces critères, le personnel pays, le gouvernement hôte, le siège et les donateurs comprendront votre décision. Mais il peut être malvenu de faire part de ces critères ou des mesures qui en résultent à certains acteurs. Par exemple, si vous vous interrogez sur la nécessité de relocaliser vos activités au cas où le conflit armé se rapprocherait de votre site actuel, il vaudra peut-être mieux ne pas en informer les acteurs du conflit car cela pourrait affecter leurs décisions ou accroître votre vulnérabilité en tant que cible.

Dans la mesure du possible, il est important d'élaborer ces critères lorsque la situation est calme. Si des décisions sont prises en pleine crise, la perception du risque affectera les décisions.

Chaque crise est unique, mais certains signes indiquent généralement que la situation est en train de se dégrader ou qu'une catastrophe naturelle est imminente. Si certaines catastrophes naturelles se produisent sans avertissement (comme c'est le cas de nombreux tremblements de terre), il existe pour d'autres certains signes avant-coureurs ou indicateurs (tempêtes tropicales, inondations ou aggravation d'un conflit). Chaque plan d'urgence devra comporter trois phases :

- Phase d'alerte : avertir toutes les parties prenantes qu'il est temps de se préparer.
- Phase de déclenchement : le plan d'urgence est mis en œuvre.
- Phase de reprise : comment l'organisation reprendra ses opérations en toute sécurité.

La relocalisation et l'évacuation du personnel peuvent être progressives, différents critères s'appliquant à différentes catégories de personnel. Par exemple, dans une zone sujette aux inondations, les critères peuvent être :

- Fortes pluies pendant six jours avec possibilité d'inondation : aucun membre du personnel essentiel n'est relocalisé ;
- Fortes pluies pendant huit jours et des cours d'eau qui atteignent un niveau convenu : tout le personnel est relocalisé.

La définition de ce qui constitue le personnel essentiel sera différente selon l'organisation, le contexte, voire les risques. Le rôle, le programme, l'expérience et le rapport personnel au risque sont autant de facteurs qui influeront sur l'identification du personnel essentiel. L'ethnicité et la nationalité devront également être prises en compte en cas de risques liés à un conflit.

La plupart des organisations ont une politique qui autorise leurs membres à circuler librement, et qui leur donne ainsi le droit de choisir d'être relocalisés ou évacués si leur perception personnelle du risque est trop élevée. Les individus doivent être au courant des politiques de l'organisation dans les contextes où une relocalisation et/ou une évacuation sont susceptibles d'être requises.

Hibernation

Bonnes pratiques :

- Les bureaux ont stocké des réserves de nourriture, d'eau et de fournitures de premiers secours pour le nombre de personnes prévu et pour le nombre de jours convenu.
- Ces réserves doivent être adaptées : denrées non périssables, transportables et non congelées, car elles ne pourraient être conservées si le groupe électrogène ne fonctionnait plus.
- Elles doivent être accessibles (p. ex. dans une zone de tremblements de terre, ne pas stocker les réserves dans un lieu à l'abri des voleurs mais qui empêche le personnel de récupérer ces réserves en cas de tremblement de terre).
- Veillez à disposer d'équipement de communication approprié sur le lieu d'hibernation (p. ex. si vous devez vous abriter dans une chambre forte, le téléphone satellite ne fonctionnera pas).
- Veillez à disposer d'un groupe électrogène de secours et de carburant, le cas échéant.
- Versez au personnel 2-3 semaines de salaire en liquide pour lui permettre de survivre.
- Contactez les fournisseurs et les banques et informez-les de vos intentions.
- Demandez aux membres du personnel de travailler depuis chez eux mais de se signaler tous les jours en rendant compte de leur situation et de leurs observations.
- Minimisez l'activité au bureau, effectuez une sauvegarde hors site des fichiers, et immobilisez les véhicules s'ils risquent d'être volés lors d'une période difficile.
- Contactez les autres ONG qui se trouvent dans une situation similaire.
- Maintenez le contact avec les communautés pour obtenir des informations et leur faire savoir que vous ne les oubliez pas.

Relocalisation

Bonnes pratiques :

- Identifiez à l'avance les lieux vers lesquels vous pouvez vous relocaliser provisoirement si le centre des opérations ou une région spécifique ne sont plus sécurisés. Par exemple :
  - Bureaux qui existent déjà sur le terrain
  - Complexes d'autres ONG
  - Pavillons des invités
  - Autres lieux sécurisés
- Veillez à pouvoir utiliser le téléphone et Internet dans ces lieux provisoires.
- Maintenez de bonnes communications avec les communautés pour qu'elles ne se sentent pas abandonnées et que votre stratégie d'acceptation ne soit pas affectée.

Voir le Module 4 – Stratégies de sécurité : acceptation, protection et dissuasion

- Si des membres du personnel ont été relocalisés, veillez à ce que les plans d'évacuation soient mis à jour, au cas où la situation se dégrade encore davantage. Si le personnel est inscrit auprès des Nations Unies, de l'ambassade ou d'une compagnie d'assurance d'un lieu spécifique, mettez à jour cette information.
- Tenez également compte des membres du personnel national et de leurs familles : le personnel ne devra pas être contraint de laisser sa famille dans un endroit dangereux alors que lui-même ira travailler dans une zone sécurisée.

Voir le manuel de l'EISF « Office Closure »

Évacuation

Bonnes pratiques :

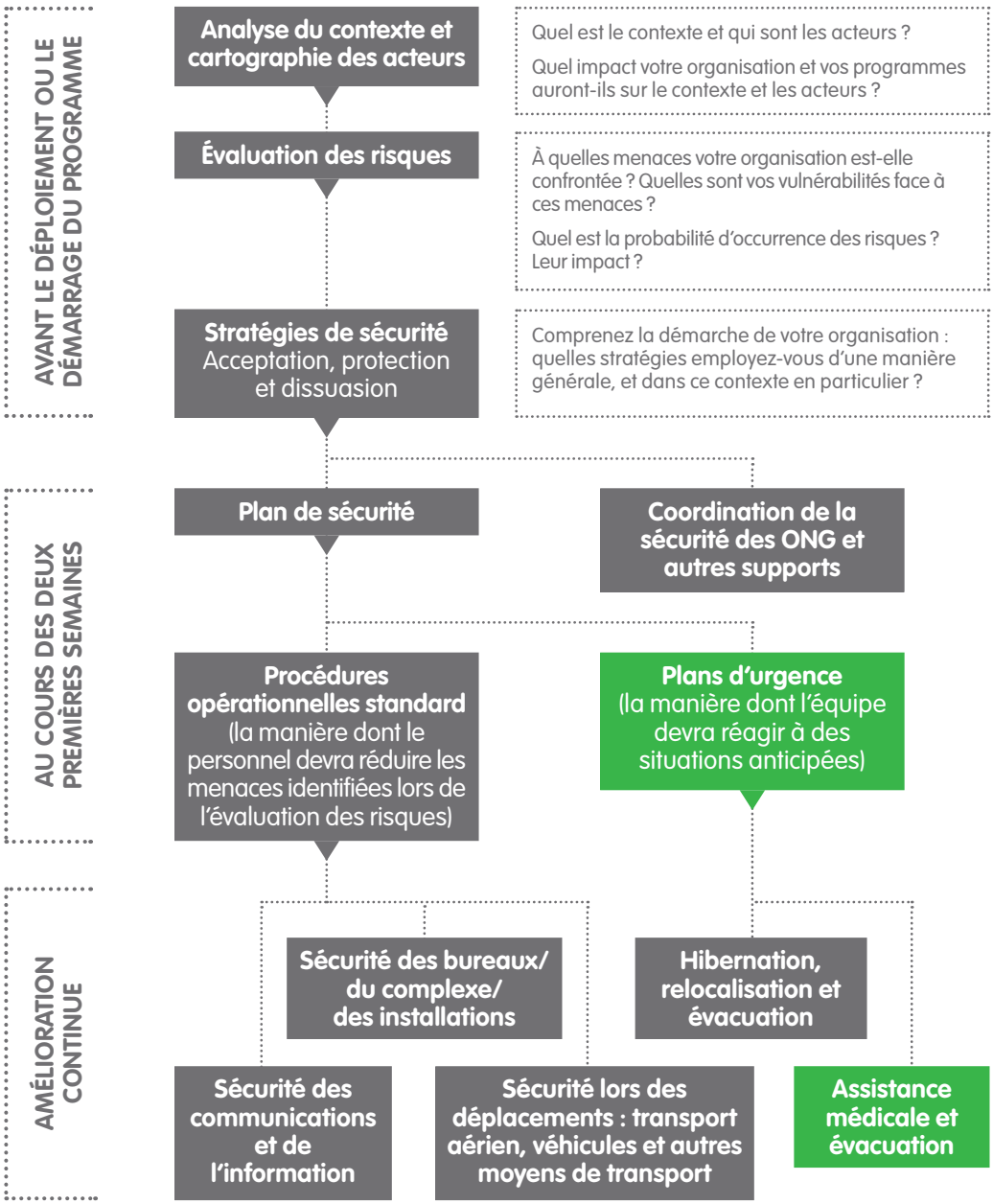
- Ne vous focalisez pas uniquement sur le personnel international. Le personnel national recruté dans une région et employé dans une autre (donc relocalisé) s'expose souvent à des risques plus importants que les employés étrangers. Avant de vous retirer, veillez à l'évacuation interne des employés nationaux pour qu'ils regagnent leur région d'origine.
- Ne promettez pas d'évacuer le personnel national. Les ONG ne doivent pas créer des réfugiés, et il n'est pas légal d'employer du personnel dans un pays tiers.
- Versez au personnel un mois de salaire en liquide avant l'évacuation.
- Établissez des voies de communication avec le personnel national restant

et les communautés pour contribuer à déterminer si vous pouvez retourner sur place en toute sécurité.

- Organisez la sécurisation des actifs (véhicules, matériel informatique) dans le pays ou les aspects juridiques associés à un déplacement de ces actifs vers un pays voisin.
- Ne comptez pas sur les Nations Unies pour évacuer votre personnel international. Prenez vos propres dispositions.
- Ne vous fiez pas aux promesses des ambassades relatives à une évacuation de tout votre personnel, surtout si certains membres du personnel international ne sont pas ressortissants de ce pays.
- Si vous avez une assurance, sachez clairement quels aspects sont couverts. Par exemple, certaines assurances spécifient que seule une piste de décollage standard, qui ne se trouvera que dans la capitale, peut être utilisée.

Une fois le personnel évacué, il peut être très difficile de revenir sur les lieux. Lors de l'élaboration du plan d'évacuation, tenez compte d'indicateurs relatifs au retour et demandez-vous comment maintenir les relations que vous avez développées avec les différentes parties prenantes. Les évacuations doivent toujours être décidées en dernier recours.

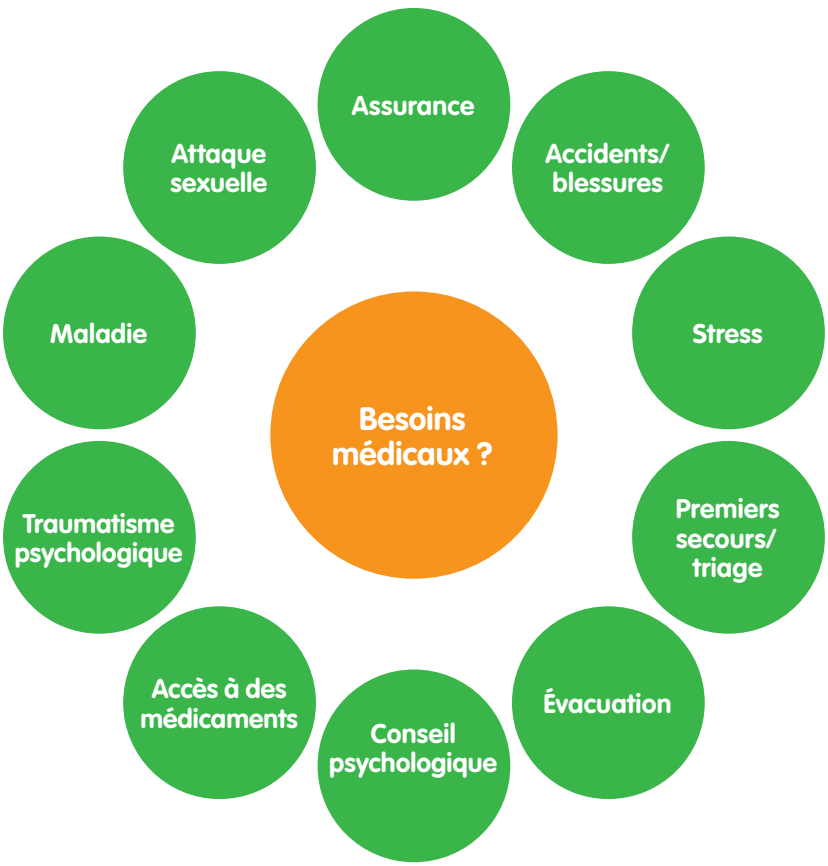
11 Assistance médicale et évacuation



Risques sanitaires et évaluation des besoins

Lorsqu'une organisation se déploie dans un nouveau pays ou une nouvelle région, il est important d'évaluer les risques sanitaires – physiques et psychiques, y compris le stress – auxquels le personnel pourrait être exposé. Cette évaluation des menaces ou dangers sanitaires vous aidera dans votre travail de préparation. Outre les problèmes de santé universels, les menaces sanitaires peuvent être regroupées dans les catégories suivantes :

- Traumatisme balistique
- Violence sexuelle
- Accidents de la route
- Maladie (endémique et épidémique)
- Hygiène
- Psycho-social
- Environnemental (faune, chaleur, altitude)
- Chimique, biologique, radiologique, nucléaire



Il est également important d'évaluer l'assistance médicale disponible et sa capacité de réaction – y compris les infrastructures –, ainsi que de tenir compte de l'assurance ou de questions liées au genre susceptibles de se poser.

Assistance médicale et capacité de réaction

- Quel est le niveau de services disponible ? (p. ex. urgences, chirurgie, soins palliatifs ?)
- Des médicaments sont-ils disponibles ? Les patients doivent-ils avoir leurs propres aiguilles, seringues ou antibiotiques ?
- Les équipements médicaux sont-ils capables de prendre en charge les troubles communs graves tels que les crises cardiaques, les défaillances d'organe ou les urgences médicales similaires ?
- La région compte-t-elle des ONG médicales ? Quels services médicaux peuvent-elles ou sont-elles disposées à fournir à votre personnel ?
- Y a-t-il des ambulances ? Sont-elles fiables ? Peuvent-elles se rendre dans des zones reculées ?
- En l'absence de services ambulanciers dans votre région d'opération, ou si ces services ne sont pas fiables, comment le personnel pourra-t-il être évacué s'il est blessé ?
- S'il vous faut envisager une auto-évacuation, il vous est fortement conseillé de former le personnel afin qu'il exécute cette tâche en toute sécurité.

Infrastructure

Si une évacuation aérienne est envisageable, établissez des liens à un stade précoce et comprenez les exigences de ce service :

- Comment indiquer votre emplacement à l'équipe d'évacuation médicale (latitude et longitude GPS, MPRS, autre ?)
- La région compte-t-elle des sites d'évacuation déjà enregistrés ?
- Quel type de transport aérien est utilisé par ce service et lui faut-il une piste d'atterrissage goudronnée, en terre, ou une zone sans obstacles pour se poser (hélicoptère – de quelle superficie ?) ?
- Comment les blessés sont-ils stabilisés/sécurisés en vue de leur évacuation ?
- Comment communiquer avec l'avion/l'hélicoptère ?
- Comment enregistrer/sécuriser les papiers d'identité et les informations sur le traitement des blessés ?
- Où les blessés sont-ils généralement emmenés ?

Assurance

Les organisations disposent généralement d'une assurance médicale. Il peut s'agir d'une politique standard pour le personnel national, une évacuation médicale étant éventuellement prévue pour le personnel international. Il est

important que tout le personnel en soit informé avant d'être déployé sur place et connaisse son numéro de police d'assurance et les coordonnées de l'assureur. Certaines organisations demandent aux consultants de prévoir leur propre assurance médicale.

Veillez à ce que le personnel administratif dans le pays soit au courant des dispositions prises auprès de l'assureur et de la couverture dont dispose chaque membre du personnel – y compris des consultants, du personnel détaché et des bénévoles –, surtout si le personnel international et/ou des visiteurs du siège sont assurés auprès de compagnies différentes.

Tenez un registre des polices d'assurance en cas d'urgence et mettez en place un système permettant de partager des informations spécifiques avec le personnel pays, p. ex. formulaire RED. Si l'assureur a approuvé au préalable des hôpitaux et/ou médecins spécifiques, il est conseillé de s'y rendre et d'instaurer une relation et des voies de communication au niveau local. Il est important de comprendre les procédures d'admission de l'hôpital approuvé – le simple fait que l'hôpital ait été approuvé par la compagnie d'assurance ne signifie pas forcément que le personnel y sera automatiquement admis.

Plusieurs étrangers de deux agences différentes ont été blessés dans l'explosion d'une bombe (…). Tous les membres du personnel étaient assurés auprès de la même compagnie et ont été amenés dans le même service de triage initial. L'une des deux agences avait déjà rendu visite à l'équipe d'administration de l'hôpital et instauré des relations ; les membres de son personnel ont été admis au bout d'une heure. L'autre agence a suivi la procédure indiquée par l'assureur médical, et il a fallu plus de trois heures avant que le personnel ne soit admis.

Autres points à prendre en compte :

- La compagnie d'assurance médicale a-t-elle approuvé des hôpitaux et/ou médecins dans cette région ?
- Y a-t-il certaines restrictions (p. ex. maladies contagieuses) ?
- Tous les membres du personnel sont-ils couverts par la même police (personnels nationaux, internationaux, détachés, consultants, bénévoles) ?
- Y a-t-il certaines restrictions au niveau des types d'évacuation médicale que la compagnie d'assurance peut prendre en charge ? Où ces évacuations peuvent-elles se produire par rapport aux risques ? Par exemple, si un type particulier de piste d'atterrissage est requis pour permettre une évacuation aérienne.
- La compagnie d'assurance a-t-elle des lieux d'évacuation spécifiques dans le pays ? Où se trouvent-ils et comment le personnel s'y rendra-t-il ?
- Les troubles liés au stress sont-ils couverts ?

- Un soutien psychologique est-il proposé à ceux qui ont subi une forme de traumatisme mental/psychologique quel qu'il soit ?

Considérations liées au genre

- Existe-t-il certaines restrictions d'ordre culturel quant aux acteurs pouvant prodiguer des soins d'urgence selon le genre, que ce soit parmi votre personnel ou au sein de la population locale ?
- Existe-t-il des services gynécologiques ou obstétriques ? Des contraceptifs sont-ils disponibles ?
- Une grossesse est-elle considérée comme présentant des risques élevés dans le pays hôte ?
- Existe-t-il des prophylactiques post-exposition ?

Préparatifs avant le déploiement

Lorsque l'évaluation des risques médicaux a été faite, et en fonction des considérations ci-dessus, les préparatifs et contrôles à effectuer avant un déploiement pourront notamment inclure :

- Dossiers médicaux, mécanismes de dépistage (y compris des troubles mentaux), vérifications et vaccinations.
- Dossiers médicaux personnels (p. ex. signes vitaux de base, groupe sanguin, maladies, médicaments, coordonnées du médecin traitant).
- Fournitures médicales personnelles et trousses de premiers secours (date, capacité, et si les fournitures peuvent être importées dans le pays hôte).
- Équipements ou fournitures disponibles et obtenues dans le pays.
- Formation requise (y compris remise à niveau) pour les premiers secours ou des compétences médicales plus avancées.

Les plans d'urgence médicale semblent simples sur le papier, mais ils peuvent souvent s'effondrer en temps de crise, ce qui ne fera qu'ajouter du stress à la situation et aggraver l'issue de l'incident. Nos hypothèses logistiques peuvent être irréalistes, les plans inadaptés, et les informations obsolètes. Consacrez d'importants efforts à la planification des situations d'urgence médicale, et ce, dès que possible, avant votre arrivée et à votre arrivée, et testez et actualisez ces plans régulièrement pour que les incidents médicaux ne se transforment pas en crise.

Les responsables devront également discuter de manière spécifique avec les points de contact de l'ONG du support, des processus et des exigences dont l'organisation dispose ou qu'elle peut offrir. Citons notamment :

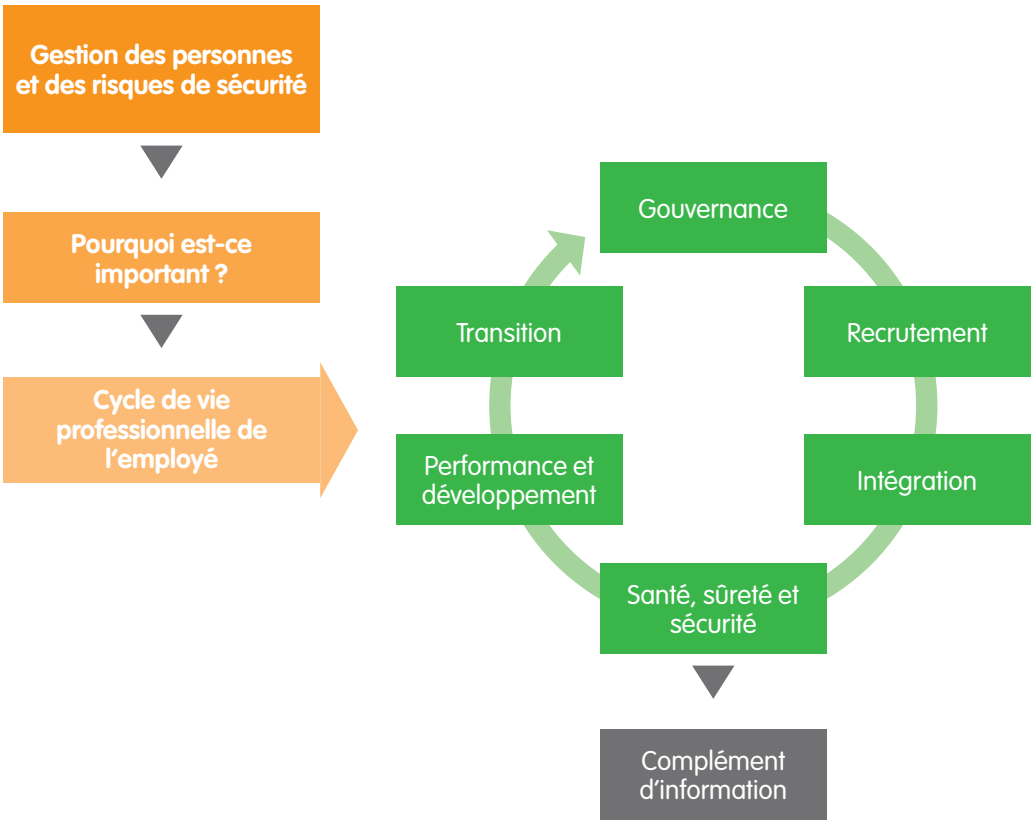
- Plan de gestion de la crise et plans d'urgence pour les situations médicales critiques.

- Détails de la police d'assurance (qui est couvert, qu'est-ce qui est couvert, quel type de réponse apportera la compagnie d'assurance et quelles sont ses limites, les lacunes, quelles informations sont requises et à quel moment, coordonnées).
- Expériences préalables de la gestion des incidents médicaux par l'organisation.
- « Gouvernance clinique » (qui est autorisé à traiter qui, à quel niveau, y compris traitements médicamenteux).

Lors du déploiement d'une équipe, chargez un membre de réaliser une évaluation des risques médicaux plus détaillée. Pour les individus déployés, identifiez le point de contact local pour les questions d'assistance médicale et obtenez des renseignements complets. Notamment :

- Qui est formé, équipé et disponible pour apporter des soins de premiers secours à l'ensemble du personnel et à n'importe quel moment ?
- Qui peut apporter des soins sur le terrain pour stabiliser les blessés dans un état critique, où se trouvent ces personnes, et comment les contacter ?
- Qui peut transporter les blessés de manière appropriée jusqu'à un centre où ils pourront recevoir des soins d'urgence, où et comment ?
- Qui est chargé de contrôler et coordonner ces questions au niveau du pays (organisation, compagnie d'assurance, autre) ?
- Qui communique quoi, à qui, quand et comment ?
- De quelles informations les prestataires de l'assurance médicale ont-ils besoin ? Qui doit les leur transmettre, et pourquoi ? Par exemple, un rapport établi par un médecin est-il nécessaire pour lancer une évacuation médicale ?
- Les Nations Unies ou d'autres entités, par exemple le CICR, ont-elles les capacités logistiques nécessaires pour effectuer les évacuations médicales dans le pays ? Les ONG peuvent-elles bénéficier de ce service et, si oui, comment ?

12 Gestion des personnes



Gestion des personnes et des risques de sécurité

Une bonne gestion des personnes, c'est obtenir les meilleurs résultats d'un employé en assurant son bien-être et sa sécurité. Les personnes sont notre ressource la plus précieuse, et les employés heureux, sécurisés et motivés étant plus susceptible d'être engagés et productifs, il est logique de vouloir apporter à son personnel un soutien de qualité et de lui offrir un environnement de travail sain et sécurisé.

La gestion des personnes est une discipline vaste et complexe qui confère des responsabilités d'ordre juridique et éthique, l'organisation devant assurer la santé physique et psychique d'un employé avant, pendant et après sa période d'emploi. Nombreuses sont les obligations juridiques et déontologiques que les organisations doivent assumer au titre de leur duty of care et, dans les environnements à haut risque, elles doivent aller encore

plus loin dans leurs efforts, en ne se contentant pas du minimum exigé par la loi.

Les personnes qui occupent un poste à responsabilité – trustees, administrateurs et managers – doivent investir du temps et des ressources dans les pratiques de gestion des personnes et veiller à ce que des spécialistes des ressources humaines et de la sécurité fournissent les conseils nécessaires au bon moment et d'une manière appropriée.

Gestion des personnes et des risques de sécurité – pourquoi est-ce important ?

La gestion des personnes a un impact direct sur la gestion des risques de sécurité, par exemple :

1. **Recrutement** – le fait d'employer des personnes inadaptées peut entraîner des risques de sécurité. Un manque de connaissances et de compétences peut se solder par de mauvais résultats et un processus décisionnel inapproprié ; un comportement inadéquat peut faire peser des risques sur le personnel et les programmes ; et le fait de ne pas tenir compte des implications de la mixité ethnique dans certaines régions peut créer des problèmes entre membres du personnel et projeter une image négative au sein de la communauté locale.
2. **Intégration** – le fait de bien préparer les membres du personnel aura un impact direct sur la rapidité et la qualité de leur intégration à leur nouveau poste, ainsi qu'au sein de l'équipe et de l'environnement de travail, tout en réduisant le risque d'incidents sécuritaires.
3. **Fermeture de bureau et fin de contrats** – Lorsqu'un bureau ferme et que des contrats arrivent à expiration, une procédure claire et transparente doit être mise en œuvre avant le début de la période de préavis, faute de quoi l'organisation s'expose à des risques sécuritaires graves.
4. **Gestion du stress** – les situations dangereuses et tendues peuvent entraîner un stress important parmi le personnel, ce qui peut avoir des répercussions sur les comportements, les relations et la capacité à prendre des décisions sécuritaires appropriées.
5. **Politique et pratiques en matière d'emploi** – les employés se sentiront valorisés et protégés si les politiques d'emploi (p. ex. récompenses, performance et comportement) sont claires et appliquées de manière cohérente. Un employé mécontent et insatisfait peut générer des risques sécuritaires pour l'organisation, le personnel et les programmes.

Au fil de votre lecture, veuillez garder à l'esprit les points suivants :

- Les employés doivent disposer des compétences et des outils nécessaires pour assumer leur fonction comme il se doit.
- L'environnement de travail doit permettre aux employés de se sentir bien et en sécurité.
- Les employés doivent connaître leurs devoirs en termes de santé, de sécurité et de sûreté, comprendre les risques et accepter tout risque résiduel lié à leur fonction, en sachant que leur organisation a effectué une évaluation adaptée et pris les précautions nécessaires.
- Les employés doivent avoir la possibilité de refuser d'exécuter une tâche qui leur est demandée s'ils estiment qu'elle comporte un risque.

Cycle de vie professionnelle de l'employé et comment assurer une gestion des personnes appropriée

Pour garantir une bonne gestion des personnes conforme à vos obligations de protection, tous les membres de votre organisation doivent être impliqués, à commencer par les principaux dirigeants, en veillant à inclure chaque niveau hiérarchique.

Le cycle de vie professionnelle de l'employé permet d'identifier les pratiques liées à la gestion des personnes qui impliquent des obligations ou des risques. Le meilleur moyen d'assurer une bonne gestion des personnes consiste à intégrer la gestion des risques de sécurité à tous les niveaux du cycle de la vie professionnelle de l'employé.

La stratégie du cycle de vie professionnelle de l'employé peut également permettre de déterminer qui est chargé des différentes pratiques au sein de l'organisation. Bien souvent, plusieurs personnes sont impliquées, ou bien la responsabilité incombe à une entité ou à un groupe, p. ex. le groupe de gestion des risques (parfois appelé comité de santé et de sécurité).

Cycle de vie professionnelle de l'employé et comment assurer une gestion des personnes appropriée

Gouvernance

La première étape du cycle de vie professionnelle de l'employé est la gouvernance, autrement dit les structures et règles sur lesquelles repose votre organisation. La culture de votre organisation en matière de santé, de sûreté et de sécurité est fortement tributaire de la fiabilité des systèmes et pratiques en place. Les plus importants sont souvent les plus élémentaires. Un employé se sentira plus valorisé si les politiques et pratiques sont claires et appliquées de manière systématique. Des pratiques qui manquent de cohérence et sont

mal appliquées auront une incidence préjudiciable sur l'employé, augmentant les risques auxquels il s'expose en matière de santé, de sûreté et de sécurité. Vous trouverez ci-après les principales pratiques à adopter et les prestations minimales à assurer pour chacune d'entre elles.

Les pratiques doivent être : axées sur les valeurs, de grande qualité, durables, accessibles, pertinentes, connues, utilisées, suivies et évaluées.

Pratique	Niveau minimum de prestation
Mission, objectifs, valeurs	Une mission, des objectifs et des valeurs clairs sont propices à l'instauration d'une vision et d'attentes précises. La mission permet à l'organisation de montrer sa raison d'être et la manière dont elle compte procéder pour changer le monde. Pour que le personnel soit motivé, cette mission doit être clairement définie. Les objectifs permettent de s'assurer que les employés œuvrent tous en faveur d'un même but. Quant aux valeurs, elles indiquent la manière dont l'organisation compte accomplir son travail et le type d'employés dont elle a besoin pour y parvenir. Tout doit en permanence s'appuyer sur la vision globale.
Seuil de risque pour l'organisation	Le seuil de risque permet d'identifier ce que le conseil d'administration ou l'équipe dirigeante d'une organisation considère comme représentant un niveau acceptable de risque pour l'organisation. Ce seuil peut varier en fonction de l'activité (p. ex. sauver des vies/développement). Le seuil de risque forme la base de l'ensemble des politiques et plans de gestion des risques de sécurité à tous les niveaux de l'organisation. Il permet également aux différents membres du personnel de comparer leur propre niveau de risque acceptable à celui de l'organisation.
Stratégie et structure organisationnelles	La stratégie sert à fixer les orientations de l'organisation en indiquant quelles tâches doivent être accomplies, par qui, où et quand. La structure permet quant à elle de savoir qui fait quoi au sein de l'organisation. Elle sert à définir la description, la classification et l'intitulé des postes, et indique quels effectifs sont rattachés aux différentes lignes hiérarchiques. Elle contribue à la gestion du recrutement et de l'intégration, ainsi qu'à la gestion et à la communication au sens plus large à tous les niveaux de l'organisation.
Contrat de travail et manuel de l'employé	Des contrats précis et accessibles et des manuels indiquant les principes qui régissent les pratiques d'embauche doivent être établis pour toutes les catégories de personnel définies, y compris pour les contrats de courte durée auxquels recourent souvent les organisations au début d'une réponse humanitaire. Pour les contrats locaux, veillez à obtenir des conseils juridiques au niveau local. Le manuel de l'employé est un outil de référence à destination des managers et des employés qui contient des informations utiles sur l'organisation et les modalités et conditions d'emploi et renseigne sur les politiques de l'organisation.

Pratique	Niveau minimum de prestation
Salaires et avantages sociaux	Les salaires et avantages sociaux (y compris les indemnités) doivent être appliqués selon des principes cohérents, conformes aux pratiques locales et pouvant être adaptés lors des étapes initiales d'une réponse humanitaire. Les employés doivent être consultés sur les changements affectant leur salaire et leurs avantages sociaux. Les différences entre catégories de personnel – international, délocalisé, national, bénévole, etc. – doivent être clairement définies. Parmi les démarches relevant des avantages sociaux, citons notamment : **Congés** – assurer un suivi des congés annuels et des jours non pris à reporter, des jours fériés, des temps de repos et de récupération (« R&R »), des congés maladie et des congés maternité/paternité. Apporter le soutien nécessaire lors d'absences pour cause de maladie et organiser une réunion lorsque l'employé reprend son travail. **Retraite** – fournir des renseignements sur les régimes de retraite facultatifs. **Assurance** – fournir un récapitulatif des prestations offertes aux employés (assurance santé, assurance voyage et assurance vie), proposer des évaluations annuelles et tenir un registre.
Heures de travail	Heures de travail et paiement des heures supplémentaires, en prévoyant une certaine flexibilité pour les cas où le personnel devra répondre rapidement à une situation d'urgence.

Implications pour la sécurité

Les organisations humanitaires doivent veiller à ce que leurs valeurs soient conformes aux principes humanitaires fondamentaux. En effet, ces principes, et plus particulièrement les principes de neutralité et d'impartialité, peuvent aider les organisations à se faire accepter au niveau local et à bénéficier d'un accès sécurisé à certains environnements susceptibles d'être dangereux. Un employé qui ne respecterait pas ces principes ou ignorerait les valeurs de l'organisation peut s'exposer – ou exposer son organisation – à des risques.

Si la structure organisationnelle (ou organigramme) est inadéquate, il pourra être difficile de déterminer qui est responsable de la sécurité au sein de l'organisation, y compris la structure décisionnelle à employer en cas d'incident critique, par exemple en cas d'enlèvement de membres du personnel.

Un employé se sentira rassuré et plus satisfait si l'organisation fait preuve de transparence à l'égard des classifications, des salaires et des avantages dont bénéficient toutes les catégories de personnel. En effet, si les modalités du contrat ne sont pas suffisamment claires, p. ex. en cas de résiliation anticipée d'un contrat de travail, un employé mécontent risque de réagir et de compromettre la sécurité des autres employés, de l'organisation et des programmes. Des procédures disciplinaires précises doivent être en place pour gérer les employés qui constituent une menace pour leurs collègues.

Recrutement

Dans les environnements à risque, les employés ont besoin de compétences et d'une expérience spécifiques. L'organisation ne doit jamais sous-estimer l'importance du processus de recrutement et les risques qui découleront du fait qu'une personne inadéquate a été embauchée. Cela risque d'être coûteux et improductif ; les employés dont le profil est mal adapté à leur fonction seront probablement insatisfaits dans leur travail, et leurs résultats ne seront pas à la hauteur des attentes, ce qui aura un impact direct sur la mise en œuvre des programmes, la charge de travail incombant à leur responsable, le moral de l'équipe et le niveau de sécurité. Il est impératif d'évaluer les risques avant de lancer le processus de recrutement afin de comprendre les principales exigences du rôle et d'inciter des candidats au profil adapté à postuler.

Les managers doivent s'impliquer totalement dans le recrutement de leurs équipes.

L'identification des qualités des candidats et des domaines dans lesquels il leur faut encore développer leurs compétences, et l'évaluation de ces attributs par rapport aux valeurs, aux connaissances et aux compétences requises sont une étape cruciale de ce processus. Les managers, en collaboration avec les ressources humaines et la sécurité, doivent effectuer des évaluations afin de déterminer les risques qu'il convient d'atténuer pour tel ou tel candidat à un poste donné. Pour les rôles qui présentent un risque élevé ou se déroulent dans un contexte dangereux, les interventions sanitaires et de sécurité obligatoires devront être identifiées. Le programme d'intégration devra s'appuyer sur le processus de recrutement.

▶ *Voir le Module 3 – Outil d'évaluation des risques*

Pratique	Niveau minimum de prestation
Recrutement	Profil de poste précis et processus de recrutement géré de manière adéquate grâce à des techniques axées sur les compétences mettant l'accent sur la diversité. Les références et les antécédents sont vérifiés, et des évaluations des risques associés au rôle et au candidat sont effectuées, y compris des évaluations de l'état de santé et de la résilience. Les managers sont pleinement formés au processus de recrutement. Si le manager ne parle pas la langue locale, il faudra veiller à ce que les candidats ne soient pas présélectionnés par des membres du personnel local, ce afin d'éviter de privilégier injustement une partie de la communauté locale.
Égalité et diversité	Une politique en faveur de l'égalité et de la diversité doit être en vigueur et les employés doivent en comprendre les principes et les appliquer à leur travail et leur comportement. Les aspects discriminatoires doivent être mis en évidence et de lourdes sanctions doivent être imposées en cas de violation de cette politique. À noter que si, lors du processus du recrutement, la discrimination basée sur l'ethnicité, le genre ou la sexualité est inacceptable d'un point de vue moral et juridique, la capacité d'une organisation peut dans de nombreux environnements être affectée par les caractéristiques d'un individu, et l'évaluation des risques associés au rôle devront en tenir compte.

Implications pour la sécurité

Le manager, en collaboration avec les ressources humaines et la sécurité, doit procéder à une évaluation des risques rigoureuse pour tous les rôles visés par la phase de recrutement ; cela permettra d'identifier les risques inhérents au rôle et le type de candidats susceptible de remplir les critères recherchés.

Une fois les candidats identifiés, chaque individu devra faire l'objet d'une évaluation des risques. Celle-ci servira à évaluer l'impact sur leur sûreté et leur sécurité personnelles de leurs compétences, expérience, âge, genre, identité sexuelle, handicap ou ethnicité, tout en veillant au respect de la législation relative à l'égalité des chances.

Plus spécifiquement, l'ethnicité, que ce soit des personnels nationaux ou internationaux, peut avoir des répercussions sérieuses sur la manière dont votre organisation est perçue et sur les risques auxquels les individus et l'organisation peuvent être exposés.

L'objectif du manager est de recruter la personne la mieux qualifiée et de prévoir des mesures d'atténuation des risques pour permettre à cette personne de travailler dans un environnement présentant le moins de risques de sécurité possible. Une bonne compréhension de la diversité de votre personnel vous aidera à instaurer de meilleurs systèmes de sécurité et des ressources confidentielles et accessibles pour appuyer leur sûreté.

Il est extrêmement important de consacrer tout le temps nécessaire à la vérification des antécédents et des références des nouvelles recrues pendant la phase de recrutement, surtout si votre organisation travaille avec des personnes vulnérables, par exemple des enfants, et si une atteinte au code peut entraîner des risques de réputation et de sécurité pour l'employé et l'organisation.

Intégration

L'une des plus importantes fonctions de l'organisation consiste à préparer un employé en vue d'une mission. Il serait malavisé d'envoyer un employé dans un environnement à haut risque sans l'y avoir préparé. Un employé mal préparé risquerait ainsi de devoir prendre des décisions qui compromettent sa sécurité personnelle (et celle d'autrui), ce qui serait irresponsable et porterait atteinte au devoir de protection de l'organisation. Notons en particulier les trois points suivants :

1. Les employés doivent avoir connaissance des politiques et procédures sécuritaires de l'organisation :
   - Ils doivent avoir connaissance du niveau acceptable de risque pour l'organisation, et des politiques régissant la culture de sécurité.
   - Ils doivent avoir confiance en la capacité des systèmes de l'organisation à assurer leur sécurité et leur bien-être.
2. Les employés doivent avoir conscience des risques pesant sur leur propre sécurité personnelle :
   - Ils doivent pleinement comprendre le contexte dans lequel ils évoluent (les modes de fonctionnement et de communication de la société qui les entoure) et les répercussions que leur comportement peut avoir sur leur vulnérabilité.
   - Ils doivent savoir ce que l'on attend d'eux (p. ex. mesures d'atténuation des risques) pendant et en dehors des heures normales de travail, et adopter un comportement en conséquence.

3. Les employés doivent avoir conscience de la manière dont le stress peut affecter leur comportement :
   - Il peut arriver que certaines personnes cherchent à évacuer leur stress par des moyens préjudiciables, par exemple par une consommation d'alcool ou une « promiscuité » excessives.
   - Les organisations doivent fournir aux managers et aux employés les informations nécessaires pour prendre conscience de leur stress et le gérer comme il se doit, et systématiquement imposer des sanctions aux employés qui mettent leur vie ou celle d'autrui en danger.

Pratique	Niveau minimum de prestation
Intégration	Le manager doit mener un programme d'intégration pour chaque employé ; le personnel recevra ainsi des informations et une formation sur les questions suivantes : mission, objectifs, comportements, structure et organisation hiérarchiques ; stratégie ; mandat de l'équipe/du programme ; relations clés ; rôle ; passation de poste ; informations contextuelles relatives à la santé, à la sûreté et à la sécurité ; objectifs de la période d'essai ; principales politiques et pratiques.
Consentement éclairé	Le consentement éclairé signifie que les employés ont accepté et signé un document indiquant que les risques de sécurité associés au rôle et au contexte leur ont été entièrement expliqués, et qu'ils les comprennent ; qu'ils comprennent les mesures prises par l'organisation pour gérer les risques dans ce contexte ; qu'ils comprennent ce que l'on attend d'eux ; et qu'ils acceptent un certain risque résiduel, autrement dit le risque qui peut subsister malgré les mesures que l'organisation a prises. La démarche axée sur le consentement éclairé doit également inclure une discussion sur les vulnérabilités spécifiques.

Le consentement éclairé permet de s'assurer que les employés comprennent la situation et qu'ils s'engagent – il ne s'agit PAS d'une renonciation juridique.

Implications pour la sécurité

Un employé mal préparé ne comprenant pas parfaitement le contexte sécuritaire local risque de prendre des décisions de sécurité malavisées. Les employés qui acceptent un poste sans avoir été sensibilisés aux limitations opérationnelles ou personnelles que cette nouvelle fonction implique (couvre-feu, par exemple) sont plus susceptibles de porter atteinte aux procédures de sécurité, de se mettre en danger, ainsi que leur programme, et d'être démotivés et mécontents de l'organisation, ce qui peut se solder par une rotation du personnel plus élevée.

Il est essentiel que chaque nouvel employé bénéficie d'un processus de passation de poste et d'intégration adéquat soutenu par ses responsables hiérarchiques. Cela vaut d'autant plus lorsque le poste en question exige de prendre des décisions impliquant la santé et la sécurité du personnel dans un environnement à haut risque. Ainsi, l'une des principales préoccupations soulevées dans l'affaire « Dennis vs Norwegian Refugee Council » jugée devant un tribunal norvégien en 2015 était le fait que le directeur pays nouvellement nommé connaissait mal le contexte sécuritaire local.

Santé, sûreté et sécurité

L'importance qu'une organisation accorde au rôle de ses employés pour le bon déroulement d'une mission se traduit souvent dans les politiques et pratiques relatives à la santé, à la sécurité et au bien-être du personnel. La santé et la sécurité des employés font partie des principales responsabilités de toute organisation, et elles doivent être gérées d'une manière appropriée à tous les niveaux. Les employeurs doivent prendre toutes les « mesures raisonnables » pour empêcher leurs employés de subir des préjudices physiques et psychiques « raisonnablement prévisibles ».

Il est important de préparer les employés à leur rôle au moyen de différents outils – formation à l'autogestion de la santé, premiers soins psychologiques, sensibilisation aux environnements hostiles, gestion de la sécurité et du stress – afin de leur permettre de rester en bonne santé et d'avoir une réaction appropriée en cas de crise ou d'incident de sécurité. La formation et le renforcement des capacités doivent constituer des priorités.

Les principales questions ci-dessous vous aideront à tester la fiabilité des politiques et pratiques de votre organisation en matière de santé, de sûreté et de sécurité.

Santé

- Les employés sont-ils suffisamment résilients sur les plans physique et psychique pour pouvoir assumer leur rôle ? Ont-ils conscience de leurs principaux facteurs de stress ?
- L'organisation dispose-t-elle de procédures régissant les incidents critiques, ainsi que d'une politique relative aux violences sexuelles, et d'une équipe qualifiée pour répondre à ce type d'incidents ?
- L'organisation propose-t-elle un service confidentiel de conseils, avec la possibilité d'aiguiller l'employé en question vers des services de conseil ou un traitement appropriés ?

On se fait parfois de fausses idées au sujet de la résilience psychique des employés. Ce sont souvent les employés internationaux chevronnés qui sont désignés pour assumer des fonctions à haut risque. Évaluez-vous en permanence leur niveau de résilience, et savez-vous comment les soutenir ? N'oubliez pas non plus que les employés issus de la communauté locale sont tout aussi susceptibles d'être traumatisés par des événements graves que n'importe quel membre de la population locale qu'ils sont chargés d'aider.

▶ *Voir le Module 11 – Assistance médicale et évacuation*

Sûreté

- Une évaluation des risques se posant dans les domaines de la santé et de la sûreté a-t-elle été effectuée pour chaque site, et est-elle régulièrement révisée ?
- Les accidents sont-ils signalés, et une assistance médicale est-elle disponible, y compris un support psychosocial ?
- Le bureau dispose-t-il de personnes formées aux premiers secours, et le personnel sait-il comment les contacter en cas de problème ?

L'employeur doit veiller à ce que le lieu de travail et les systèmes en place soient aussi sécurisés que possible. Si un site présente provisoirement certains dangers, l'employeur devra prendre des mesures raisonnables pour réduire les risques, y compris en envisageant de cesser l'activité de l'organisation.

▶ *Voir le Module 9 – Sécurité lors des déplacements : transport aérien, véhicules et autres moyens de transport*

▶ *Voir le Manuel EISF « Ouvrir un nouveau bureau : Manuel à l'attention des organisations non gouvernementales »*

▶ *Voir le Manuel EISF « Office Closure »*

Sécurité

- L'organisation dispose-t-elle d'un cadre dédié à la gestion des risques de sécurité et d'un plan de sécurité local pour identifier, atténuer et gérer les risques de sécurité, ainsi que pour répondre aux incidents sécuritaires le cas échéant ?
- L'organisation bénéficie-t-elle d'une culture positive de sécurité, autrement dit tous les membres du personnel comprennent-ils et s'engagent-ils à respecter les directives de sécurité pour garantir leur propre sécurité, ainsi que celle de leurs collègues et de leurs opérations ?

▶ *Voir le Module 1 – Processus de planification de la gestion des risques*

▶ *Voir le Module 6 – Plan de sécurité*

Pratique	Niveau minimum de prestation
Santé, sûreté et sécurité	Une politique et une formation propices au bien-être et à la sécurité des employés doivent être en place sur chaque site et conformes aux pratiques relatives à la gestion du stress, à la résilience personnelle, à la santé physique et psychique et à la gestion des risques de sécurité. Il est essentiel de tenir un registre précis des accidents, des maladies ou des incidents critiques. Les managers ont suivi une formation pour apprendre à déterminer l'état de santé de leur équipe lors de conversations, de réunions d'information et de bilans informels, et déceler des signes précoces de stress afin d'empêcher un stress cumulatif ou un burn-out au sein de leur équipe. Pour les managers dont le responsable se trouve sur un autre site, il faudra prévoir un système de soutien par les pairs. L'organisation doit régulièrement passer en revue ses pratiques en matière de santé et de sûreté pour s'assurer qu'elles sont pertinentes et que des mesures appropriées ont été prises pour garantir la sûreté du personnel. Les principales parties prenantes devront tirer des enseignements des situations qui constituent un danger pour le personnel, les programmes ou l'organisation.

Implications pour la sécurité

Les connaissances d'un individu, son comportement et son attitude sont autant de facteurs qui ont un impact sur sa vulnérabilité et son exposition au risque. Plus les employés comprennent la raison d'être des procédures de santé et de sécurité, plus ils seront susceptibles de les observer. Par exemple, les membres du personnel qui ne savent pas ou ne comprennent pas qu'ils risquent de tomber malade lors de leurs déplacements seront moins susceptibles de se faire vacciner comme cela leur a été conseillé.

Les accidents de la route sont l'un des dangers les plus graves pour les travailleurs humanitaires sur le terrain. S'assurer que les conducteurs ont reçu une formation propice à un style de conduite sécurisé et veiller au port de la ceinture de sécurité sont autant de mesures qui peuvent considérablement réduire le risque d'accidents de la route et leur impact.

Le personnel chargé de répondre à une crise humanitaire, et plus particulièrement à une situation d'urgence soudaine, est plus susceptible de connaître un niveau de stress élevé en raison des longues heures de travail qu'il lui faut fournir dans un environnement sous haute pression. La mise en place de mesures pour empêcher et gérer le stress du personnel, et pour montrer au personnel comment identifier et gérer ce stress, permettra d'améliorer le bien-être du personnel et son processus décisionnel. En effet, les individus surmenés et extrêmement stressés sont plus susceptibles de prendre des décisions néfastes pour la sécurité.

Les mesures visant à réduire le stress, par exemple l'octroi de périodes de repos, doivent être appliquées de manière cohérente, faute de quoi certains membres du personnel pourraient être incités par leurs pairs à les ignorer alors qu'ils en auraient bien besoin.

Voir le Manuel EISF « Évaluations de la sécurité »

Performance et développement

Pour que le travail défini au titre de la stratégie de l'organisation soit mené à bien, il est essentiel que les employés soient en mesure d'assumer leurs fonctions d'une manière saine et sécurisée.

Les employés doivent recevoir des consignes et une supervision appropriées. Pour les aider à réussir, il faudra préciser les attentes en mettant l'accent sur l'impact, et leur fournir tout le soutien nécessaire. Grâce à une communication régulière, que ce soit de façon formelle ou informelle, le manager saura entendre les préoccupations de son personnel et reconnaître le niveau de performance ; si les résultats ne sont pas bons, il devra appliquer des politiques et des pratiques pertinentes pour gérer la performance, les griefs et les manquements.

Il ne faut pas confondre manque de capacité et manque de volonté. Une mauvaise performance peut être gérée de deux manières : en renforçant les capacités de l'employé si celui-ci n'a pas les connaissances ou les compétences requises ; ou en appliquant une politique disciplinaire s'il refuse de faire son travail.

Les communications régulières entre le manager et l'employé doivent notamment porter sur le développement personnel nécessaire au rôle actuel ou futur de cet employé. Un employé dont les activités actuelles et les objectifs de carrière sont activement soutenus aura plus de chances d'être motivé et d'améliorer sa performance et son efficacité.

Pratique	Niveau minimum de prestation
Gestion de la performance	Il faut prévoir une supervision et des consignes appropriées. Les profils de poste et les objectifs doivent être clairement définis. Le manager doit régulièrement communiquer et informer les employés sur la façon dont ils s'acquittent de leurs tâches, en récompensant les bons résultats et, en cas de mauvaise performance, en prenant des mesures pour améliorer les compétences ou en appliquant une politique disciplinaire, selon le cas. Le bilan de performance de tous les membres du personnel assumant des responsabilités dans le domaine de la sécurité devra comprendre un suivi de la gestion des risques de sécurité.
Griefs et procédures disciplinaires	L'organisation doit proposer à ses employés un moyen sûr de soulever des préoccupations et des plaintes informelles et formelles. Une politique disciplinaire et de traitement des griefs servira à définir comment gérer et suivre les dossiers de manière équitable et cohérente, et comment en tirer des enseignements.
Dénonciation des abus	La dénonciation des abus ou « whistleblowing » est un moyen de soulever des plaintes ou des préoccupations graves de manière anonyme ; les dossiers légitimes feront ainsi l'objet d'une enquête confidentielle.
Apprentissage et développement de l'employé	Des discussions fréquentes doivent porter sur le comportement, le développement et les objectifs de carrière.

La sécurité doit faire partie intégrante de chaque bilan de performance.

Implications pour la sécurité

L'insatisfaction du personnel est un des plus grands dangers pour l'organisation. Les employés qui estiment ne pas recevoir un traitement équitable risquent de réagir de diverses manières : vols, attaques physiques et verbales, menaces de mort, ou propos médisants sur des individus ou sur l'organisation à des parties externes telles que des bénéficiaires, des anciens, des agents du gouvernement ou des organes médiatiques. Ces réactions peuvent avoir des répercussions graves sur la sécurité du personnel, des programmes et de l'organisation.

La gestion de la performance repose sur une relation employé—manager de qualité. Si cette relation est médiocre, cela aura un impact sur la confiance et les répercussions sécuritaires pourraient être graves, par exemple si les recommandations d'un responsable en matière de sécurité sont ignorées ou si des employés prennent des décisions sans consulter leurs responsable, d'où un danger pour eux-mêmes et leurs collègues.

En l'absence d'un moyen fiable pour communiquer leurs préoccupations, les employés risquent de se sentir obligés d'accepter toutes les décisions de leurs managers, même s'ils sont mécontents des risques impliqués. Le personnel de première ligne est susceptible de mieux comprendre le contexte sécuritaire, mais l'absence de voies de communication peut empêcher l'information d'être transmise aux différents niveaux hiérarchiques et accroître le risque d'incident sécuritaire.

Transition

Tout employé sera tôt ou tard appelé à quitter l'organisation. La façon dont se déroule ce départ peut avoir un impact sur le bien-être de l'individu et de ses collègues ainsi que sur la réputation de l'organisation. Un employé dont le départ se passe « bien » peut devenir un ambassadeur pour l'organisation. Plus l'individu dispose de temps et d'informations pour préparer son départ, mieux cela vaudra. Dans la mesure du possible, les managers devront entamer des discussions sur le départ de l'employé avant le début de la période de préavis. Il est également important de comprendre les raisons pour lesquelles un membre du personnel décide de quitter l'organisation.

Voir le manuel de l'EISF « Office Closure »

Pratique	Niveau minimum de prestation
Mesures à prendre avant le départ de l'employé	Des discussions claires et transparentes avec le personnel, et plus particulièrement le personnel national, sur l'avenir du projet ou du bureau peuvent aider les employés à mieux se préparer à la transition et garantir une bonne passation de poste. L'organisation doit prendre des mesures pour appuyer la transition du personnel, surtout si elle est contrainte de réduire ses effectifs suite à un manque de fonds ou pour d'autres raisons qui ne dépendent pas d'elle.
Entretiens de départ	Ces entretiens servent à recueillir des informations auprès des employés qui s'apprêtent à quitter l'organisation. Veillez à leur poser des questions sur l'équilibre travail-vie privée, les valeurs, le développement, la qualité des briefings/débriefings et les raisons qui les poussent à partir. Le fait que plusieurs membres d'une même équipe décident de quitter l'organisation peut être révélateur d'un problème plus grave, et des mesures devront être prises en conséquence.
Savoir organisationnel	Le fait de recueillir des informations auprès de l'employé avant son départ permettra à l'organisation de développer et gérer son savoir.

Implications pour la sécurité

Les employés qui quittent l'organisation mécontents font peser un risque sécuritaire pour l'organisation. Un licenciement suite à une procédure disciplinaire, une perte de financement, la fermeture de bureaux et l'intensification des mesures de sécurité sont autant de facteurs qui peuvent entraîner différents types de risques.

Les employés mécontents sont susceptibles de perturber l'issue d'un projet et la qualité des relations, et d'instaurer un environnement malsain. Dans un environnement à haut risque, gérer le départ d'un employé dans des circonstances difficiles peut être l'une des tâches les plus importantes mais aussi les plus complexes qui incombent à un manager.

Partager les informations avec d'autres employeurs, et autoriser les employés à bénéficier d'horaires de travail plus souples pour pouvoir chercher un nouvel emploi ou bénéficier d'opportunités de formation (p. ex. cours d'informatique ou d'anglais) font partie des mesures qui peuvent faciliter la transition des employés et, ainsi, réduire les risques sécuritaires.

Si l'organisation s'abstient de recueillir des informations auprès d'un employé qui s'apprête à partir (généralement par le biais d'un processus de passation de poste et d'entretiens de départ), il est probable que les leçons ne seront pas transmises et que les erreurs se reproduiront. Si la passation de poste s'est mal déroulée, le nouvel employé risque de commettre des erreurs et de mettre en danger sa santé, sa sûreté et sa sécurité, ainsi que celles d'autrui.

Pour s'adapter et tirer des enseignements utiles, les organisations doivent procéder régulièrement à des évaluations de la sécurité et mettre en application les conclusions de ces évaluations. Il est également primordial que l'équipe dirigeante effectue des exercices de gestion de crise.

Un bureau en Indonésie allait fermer, le programme s'étant soldé par un échec. Les employés de ce bureau ne l'ont appris que deux jours avant la fin de leur contrat. Des rumeurs circulaient déjà, et les employés étaient très mécontents. Le bureau a été cambriolé la veille du jour de la dernière paie – l'argent qui se trouvait dans le coffre et des objets de valeur ont été dérobés. Les managers avaient pensé que, dans l'intérêt de la sécurité, il valait mieux que les employés ne connaissent pas la date exacte de la fermeture du bureau. Mais ce manque de transparence a entraîné une riposte plus agressive qui a compromis la sécurité du personnel. Une démarche plus honnête et plus coopérative à l'égard du personnel du programme aurait permis de réduire les incidents et de favoriser la sécurité.

Complément d'information

Le site de CHS Alliance (www.chsalliance.org) contient des ressources pour aider les organisations à soutenir la santé, la sécurité et le bien-être de leurs employés. La norme 8 de la « Norme humanitaire fondamentale » indique les politiques devant être en place pour la sécurité et le bien-être du personnel.

Duty of Care International (http://dutyofcareinternational.co.uk/) regroupe plusieurs ressources, notamment :

- Le manuel « Human Resource Management (Roots 12) » publié par Tearfund. Il s'agit d'un outil de gestion des personnes à l'attention des managers, d'autant plus utile si le pays ne dispose pas d'experts en ressources humaines.
- « The Importance of HR Management in Supporting Staff Working in Hazardous Environments » de Roger Darby et Christine Williamson.
- « Can you get sued? Legal liability of international humanitarian aid organisations towards their staff » de Edward Kemp et Maarten Merkelbach.

La International SOS Foundation (www.internationalsosfoundation.org) tient à disposition plusieurs ressources utiles, notamment le manuel « Managing the safety, health and security of mobile workers: an occupational safety and health practitioner's guide » produit conjointement par la International SOS Foundation et IOSH.

Le site de l'EISF (www.eisf.eu) regroupe plusieurs publications pertinentes pour appuyer les organisations dans le domaine du bien-être du personnel, ainsi qu'une liste de ressources supplémentaires relatives à la santé, la sûreté et la sécurité du personnel.

Glossaire

Acceptation : Instauration d'un environnement opérationnel sécurisé grâce au consentement, à l'approbation et à la coopération des individus, des communautés et des autorités au niveau local.

Déclencheur : Facteur dont il aura été convenu entre le personnel pays et le siège pour déterminer le moment où les différents plans d'urgence doivent être déclenchés.

Dissuasion : Réduction du risque en limitant la menace au moyen d'une contre-menace (p. ex. protection armée, pressions diplomatiques/politiques, suspension provisoire).

Duty of care : L'obligation légale et morale qui incombe à une organisation de prendre toutes les mesures possibles pour réduire le risque de préjudice causé aux personnes qui travaillent pour elle ou opèrent pour son compte. L'expression anglaise, souvent aussi utilisée en français, est employée dans ce manuel et correspond aux expressions « devoir de diligence », « devoir de protection » ou « responsabilité de l'employeur ».

Évacuation : Suspension des opérations dans un pays, évacuation du personnel international vers un autre pays et du personnel national depuis les zones de déploiement vers leur zone d'habitation d'origine. Une programmation limitée peut se poursuivre grâce à des outils de gestion à distance, selon la situation.

Hibernation : Le personnel reste à son domicile et le programme est provisoirement interrompu. Dans certains cas, le personnel devra trouver refuge au bureau ou au sein du complexe.

Menace : Toute forme de défi, que ce soit en termes de sûreté, de sécurité ou autre, auxquels sont confrontés vos personnels, vos actifs, votre organisation, votre réputation ou vos programmes dans votre contexte opérationnel.

Protection : Réduction du risque, mais pas de la menace, en amoindrissant la vulnérabilité de l'organisation (p. ex. clôtures, gardiens, murs).

Relocalisation : Déplacement des bureaux et/ou activités vers un site plus sécurisé, généralement de manière provisoire et dans le même pays.

Risque : Différentes manières dont une menace pourrait affecter l'organisation, son personnel, ses actifs, sa réputation ou ses programmes.

Vulnérabilité : Le degré d'exposition d'une organisation à une menace. Elle varie selon la nature de l'organisation, son mode de fonctionnement, ses programmes, son personnel et sa capacité à gérer le risque.

Autres publications de l'EISF

Pour contribuer à un prochain projet de recherche ou suggérer des thématiques, veuillez contacter **eisf-research@eisf.eu**.

Documents d'information et rapports

Communications Technology and Humanitarian Delivery : Challenges and Opportunities for Security Risk Management – 2nd Edition
Décembre 2016
Vazquez Llorente, R. et Wall, I. (éd.)

Security Risk Management and Religion : Faith and Secularism in Humanitarian Assistance
Août 2014
Hodgson, L. *et al.* Édité par Vazquez, R.

The Future of Humanitarian Security in Fragile Contexts
Mars 2014
Armstrong, J. avec le soutien du Secrétariat de l'EISF

The Cost of Security Risk Management for NGOs
Février 2013
Finucane, C. Édité par Zumkehr, H. J. – Secrétariat de l'EISF

Security Management and Capacity Development: International Agencies Working with Local Partners
Décembre 2012
Singh, I. et Secrétariat de l'EISF

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
Septembre 2012 – versions esp. et fr. disponibles.
Persaud, C. Édité par Zumkehr, H. J. – Secrétariat de l'EISF

Engaging Private Security Providers : A Guideline for Non-Governmental Organisations
Décembre 2011 – version fr. disponible
Glaser, M. avec le soutien du Secrétariat de l'EISF (éd.)

Risk Thresholds in Humanitarian Assistance
Octobre 2010
Kingston, M. et Behn, O.

Abduction Management
Mai 2010
Buth, P. avec le soutien du Secrétariat de l'EISF (éd.)

Crisis Management of Critical Incidents
Avril 2010
Buth, P. avec le soutien du Secrétariat de l'EISF (éd.)

The Information Management Challenge
Mars 2010
Ayre, R. avec le soutien du Secrétariat de l'EISF (éd.)

Joint NGO Safety and Security Training
Janvier 2010
Kingston, M. avec le soutien du Groupe de travail dédié à la Formation de l'EISF

Humanitarian Risk Initiatives : 2009 Index Report
Décembre 2009
Finucane, C. Édité par Kingston, M.

Articles

Digital Security for LGBTQI Aid Workers: Awareness and Response
Décembre 2017
Kumar, M.

Demystifying Security Risk Management
Février 2017, (dans Pear Insights Magazine)
Fairbanks, A.

Duty of Care : A Review of the Dennis v Norwegian Refugee Cuncil Ruling and its implications
Septembre 2016
Kemp, E. and Merkelbach, M. Édité par Fairbanks, A.

Organisational Risk Management in High-risk Programmes : The Non-medical Response to the Ebola Outbreak
Juillet 2015 (dans Humanitarian Exchange, Issue 64).
Reilly, L. et Vazquez Llorente, R.

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
Mars 2012.
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
Décembre 2010
Van Brabant, K.

Whose Risk Is it Anyway? Linking Operational Risk Thresholds and Organisational Risk Management
Juin 2010 (dans Humanitarian Exchange, Issue 47)
Behn, O. et Kingston, M.

Risk Transfer through Hardening Mentalities?
Novembre 2009
Behn, O. et Kingston, M.

Manuels

Abduction and Kidnap Risk Management
Novembre 2017
EISF

Security Incident Information Management Handbook
Septembre 2017
RedR UK, Insecurity Insight, EISF

Security Risk Management : a basic guide for smaller NGOs
Juni 2017
Bickley, S.

Security to go: a risk management toolkit for humanitarian aid agencies – 2nd edition
Mars 2017 – versions esp. et fr. disponibles.
Davis, J. *et al.*

Office Opening
Mars 2015 – version fr. disponible.
Source8

Security Audits
Septembre 2013 – versions esp. et fr. disponibles.
Finucane C. Édité par French, E. et Vazquez Llorente, R. (esp. et fr.) – Secrétariat de l'EISF

Managing the Message : Communication and Media Management in a Crisis
Septembre 2013 – version fr. disponible.
Davidson, S. Édité par French, E. – Secrétariat de l'EISF

Family First: Liaison and Support during a Crisis
Février 2013 – version fr. disponible.
Davidson, S. Édité par French, E. – Secrétariat de l'EISF

Office Closure
Février 2013
Safer Edge. Édité par French, E. et Reilly, L. – Secrétariat de l'EISF

eisf

Directrice exécutive de l'EISF
T : +44 (0) 203 195 1360
M : +44 (0) 77 6099 2239
eisf-director@eisf.eu

Conseiller en recherche de l'EISF
T : +44 (0) 203 195 1362
M : +44 (0) 77 6099 2240
eisf-research@eisf.eu

www.eisf.eu

Édition en anglais : Première publication septembre 2015 / mise à jour mars 2017.
Édition en français : Première publication mai 2018.