MANUEL EISF À L'ATTENTION DES ORGANISATIONS NON GOUVERNEMENTALES

eisf

Gestion du risque sécurité :

Manuel de référence à l'attention des petites ONG

EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF) devenu Global Interagency Security Forum (GISF)

En Mars 2020, EISF est devenu GISF, reflétant l'extension de son réseau de membres.

GISF est un réseau de points focaux de sécurité qui représente plus de 100 organisations humanitaires opérant à l'international.

L'adjectif 'humanitaire' est ici entendu au sens large et désigne les activités non lucratives visant à contribuer au bien de l'humanité et à réduire ses souffrances.

GISF s'engage à améliorer la sécurité des opérations et du personnel, en soutenant la gestion humanitaire du risque sécurité.

A travers son réseau, il facilite les échanges entre ses membres et autres acteurs tels que l'ONU, les bailleurs de fonds, les universités et instituts de recherche, le secteur privé et autres ONGI.

GISF produit également des papiers de recherches et guides pratiques, et organise divers ateliers, événements et formations, afin de soutenir les bonnes pratiques en gestion de risque sécurité.

GISF 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), le ministère britannique du Développement international (DFID) et les contributions de ses membres.

Pour en savoir plus visiter
www.gisf.ngo

Remerciements

Ce manuel a été élaboré par Shaun Bickley (Tricky Locations) avec la participation de Lisa Reilly (Directrice exécutive de l'EISF). Adelicia Fairbanks, Conseillère Recherche de l'EISF, est directrice de ce projet, dont elle a révisé le contenu.

L'auteur et l'EISF tiennent à remercier les personnes suivantes de bien avoir voulu faire part de leurs connaissances pointues lors de l'élaboration de ce manuel : Gonzalo de Palacios, Marta Iglesias (MPDL), Nathanael Jarret, Andrew Parkes (Malaria Consortium), Laky Pissalidis, Emmanuelle Strub et Lotta Westerberg.

La traduction française de ce guide a été réalisée par Catherine Dauvergne, avec le soutien d'Emmanuelle Strub et de Léa Moutard.

Suggestion de citation

Bickley, S. (2017) *Gestion du risque sécurité : manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (EISF).

Conception et illustrations : www.wave.coop

Table des matières

Introduction 05

À propos de ce manuel 06

À qui s'adresse ce manuel ? 07

Mode d'emploi 07

1. Remplir son « duty of care » 08

Définir les attitudes face au risque 10

Instaurer une culture de sécurité 11

Affecter des ressources à la gestion du risque sécurité 14

2. Élaborer un cadre 16

3. Gouvernance et responsabilité 19

Concevoir une structure de gestion du risque sécurité efficace 19

4. Politiques et principes 23

Élaborer une politique sécurité 24

Définir les exigences en matière de sécurité 26

5. Opérations et programmes 28

Évaluations du risque sécurité 31

Plans sécurité 33

Dispositions sécuritaires et support 35

6. Gestion des déplacements et support 38

Identifier les risques associés aux déplacements 39

Procédures de sécurité lors des déplacements 41

Informations sécurité et analyse 43

Briefings sécurité 45

Suivi des déplacements 47

Assurance 48

7. Sensibilisation et renforcement des capacités 51

Initiations à la sécurité 51

Formations sécurité 52

8. Suivi des incidents 57

Processus de signalement des incidents 58

Formulaires de rapports d'incidents 59

Enregistrement et analyse des incidents 61

9. Gestion de crise 63

Instaurer une structure de gestion de crise 64

Quand peut-on parler de crise ? 66

Plans de gestion de crise 67

Prestataires d'assistance et support 68

10. Collaboration en matière de sécurité et réseaux 71

Réseaux sécurité inter-agences 72

11. Contrôle de la conformité et de l'efficacité 75

Contrôle de la conformité 76

Audits et examens de sécurité 77

12. Ressources complémentaires 79

Sites Internet 80

Directives relatives à la sécurité personnelle 80

Directives en matière de gestion du risque sécurité 80

Glossaire 81

Références 83

Annexe. Cadre de gestion du risque sécurité – aide-mémoire 86

Autres publications de l'EISF 89

Introduction

La sécurité du personnel est un défi important pour les organisations non gouvernementales (ONG) humanitaires et de développement, quelle que soit leur taille, dans un contexte marqué par une intensification de l'insécurité, des menaces et de la violence.

Si le fait de travailler et de se déplacer dans des environnements très imprévisibles comportera toujours une part de risque, les organisations ont de nombreux outils à leur disposition pour élaborer un cadre de travail plus sûr et plus sécurisé pour leur personnel. Cependant, cela nécessite de la part de l'organisation d'accorder une plus grande priorité et des ressources plus conséquentes à la gestion du risque sécurité. Pour de nombreuses ONG, les évaluations du risque sécurité, les plans sécurité, les procédures de sécurité lors des déplacements, les formations sécurité et les systèmes de signalement des incidents font désormais partie du vocabulaire courant et jouent un rôle clé dans leur manière d'opérer à travers le monde.

Pour une petite ONG, cependant, ces mécanismes peuvent sembler excessifs ou trop onéreux étant donné sa taille, les environnements dans lesquels son personnel évolue et les activités qu'elle entreprend. Cependant, quelle que soit leur taille, toutes les ONG ont une obligation de sécurité à l'égard de leur personnel. Le personnel des petites organisations travaille souvent dans les mêmes zones et s'expose à des risques similaires sans pour autant disposer du soutien dont bénéficient leurs homologues employés par des organisations de plus grande envergure, avec une architecture sécuritaire significative en place. De nombreux personnels trouvent frustrants et stressants le manque de priorité et de soutien accordé à la sécurité et l'incohérence de la gestion de la sécurité d'une organisation à une autre ; ils ont souvent le sentiment que leur organisation les place dans une situation de risque accru. Il est donc crucial d'instaurer un cadre efficace ancrant les pratiques de gestion du risque sécurité à tous les niveaux de votre organisation.

Certes, cette tâche peut sembler redoutable, même pour les organisations qui reconnaissent la nécessité d'améliorer leur stratégie en matière de sécurité du personnel. Par où commencer ? Quelles doivent être les priorités ? Qui doit se charger de cette initiative ? Les individus à qui cette tâche incombe affichent souvent une expérience et une formation limitée en matière de gestion du risque sécurité et ont d'autres priorités et rôles à prendre en charge. Même si cet exercice n'est pas facile, l'amélioration de la sécurité du

personnel doit être une des principales priorités des ONG, quelle que soit leur taille.

Les organisations qui savent bien gérer les risques bénéficieront d'un meilleur accès aux environnements plus risqués, et pourront donc avoir un impact plus conséquent, tout en protégeant leur personnel.

« Sécurité » et « sûreté »

Les termes de « safety » et « security » sont utilisés chez les anglosaxons pour désigner deux types de risques.

La « security » concerne principalement les actes de violence, les agressions et/ou les actes criminels volontaires visant les personnels d'une agence ou ses biens, alors que la « safety » désigne les actes, événements ou dangers involontaires ou accidentels.

Les humanitaires francophones utilisent généralement le terme de sécurité pour désigner les deux catégories de risques. Certaines organisations peuvent cependant disposer de structures de gestion différentes pour la sécurité et pour la « safety », dites santé et bien-être au travail. La plupart des petites ONG utilisent les mêmes ressources pour gérer les questions de sécurité et de santé et bien être au travail. Pour les besoins du présent manuel, le terme « sécurité » doit s'entendre comme incluant la santé et le bien-être au travail

À propos de ce manuel

Ce document est un manuel facile à utiliser conçu pour aider les petites ONG à « démystifier » la gestion du risque sécurité. En présentant les éléments d'un cadre élémentaire de gestion du risque sécurité, ce manuel a pour objectif d'aider les ONG à traduire leurs obligations légales et morales en processus et actions clés, non seulement pour améliorer la sécurité de leurs personnels nationaux et internationaux, mais aussi pour promouvoir la réputation et la crédibilité de leur organisation. Bien que ce manuel ait été conçu à l'attention des ONG aussi bien nationales qu'internationales, il est possible que certains éléments soient plus pertinents dans un cas de figure plutôt que dans un autre.

Nombre des ressources sécurité dont disposent déjà les ONG tendent à mettre l'accent sur les exigences des organisations humanitaires et de développement de plus grande taille, autrement dit celles qui comptent d'importants effectifs multinationaux dans de multiples pays, et qui incluent souvent des personnels de sécurité dédiés. Ce manuel tient compte des ressources limitées et des défis spécifiques auxquels les petites ONG peuvent faire face lorsqu'elles tentent d'instaurer et de maintenir un cadre de gestion du risque sécurité.

Ce manuel vient compléter d'autres guides essentiels, tels que le manuel de l'EISF « Security to go » consacré aux systèmes de gestion de la sécurité dans un contexte ou un lieu spécifique ; cependant, le présent manuel offre une perspective plus étendue du cadre global qu'une organisation devrait chercher à instaurer pour améliorer sa gestion du risque sécurité. Ce manuel vise aussi à compléter le manuel de l'EISF « Security Audits », qui permet aux organisations de faire le point sur la sécurité de leur personnel et les améliorations à apporter.

En 2020, EISF est devenu GISF (Global Interagency Security Forum). Vous pouvez trouver toutes les ressources mentionnées dans ce rapport sur notre nouveau site internet : www.gisf.ngo.

À qui s'adresse ce manuel ?

Ce manuel s'adresse principalement aux effectifs des petites ONG qui assument certaines responsabilités en matière de sécurité du personnel et cherchent à améliorer la gestion du risque sécurité dans leur organisation.

Bien qu'ayant été rédigé spécifiquement à l'attention des petites ONG, ce manuel est pertinent pour les organisations de toutes tailles, même pour les ONG bien établies et de grande ampleur dont le personnel travaille ou doit se rendre dans des environnements difficiles. Ce manuel peut aussi être utile aux ONG internationales qui n'ont pas de présence dans un pays mais détachent leur personnel auprès d'organisations partenaires.

Mode d'emploi

Ce manuel est structuré autour des principaux éléments du cadre de gestion du risque sécurité. Le lecteur pourra en toute facilité parcourir le document et consulter des aspects spécifiques du cadre selon ses intérêts en matière de gestion du risque sécurité. Vous y trouverez :

- Des activités essentielles et autres, indiquées par le symbole
- Des témoignages d'experts, indiqués par le symbole
- Des renvois dans le manuel, indiqués par le symbole
- Des renvois vers d'autres ressources, outils et informations sécuritaires, y compris les publications de l'EISF accessibles sur le site www.eisf.eu, indiqués par le symbole
- Veuillez consulter la bibliographie pour des détails et liens vers les ressources citées dans le manuel.
- Des hyperliens facilitent la navigation dans le document.

1 Remplir son « duty of care »

Bien que la plupart des ONG, quelle que soit leur taille, reconnaissent la nécessité de protéger leur personnel, un grand nombre d'entre elles n'apprécient toujours pas toute la portée et les implications de leurs obligations légales vis-à-vis de la sécurité de leurs employés. Ces obligations de sécurité de l'employeur à l'égard de son personnel sont appelées « duty of care » dans le milieu humanitaire, anglophone comme francophone, et nous privilégierons cette expression à ses équivalents français de devoir de diligence, de vigilance ou de protection.

Le « duty of care », ou obligations de sécurité, est devenu bien plus rigoureux au cours de la dernière décennie, et ce qui autrefois était considéré comme suffisant est loin de l'être aujourd'hui.

Bien que le « duty of care » soit un terme juridique désignant les devoirs des organisations envers leur personnel, il existe aussi une obligation morale que les organisations devraient envisager.

Pour simplifier, le « duty of care », c'est s'assurer que des mesures d'atténuation des risques et un soutien appropriés soient en place pour empêcher et faire face aux incidents, et veiller à ce que l'ensemble du personnel soit informé des risques et des mesures d'atténuation connexes.

Il est important de souligner que le « duty of care » est plus qu'une simple question de sécurité. La gestion du risque sécurité n'est en effet qu'un des éléments représentant la responsabilité globale de l'organisation dans les domaines de la sécurité, de la santé et du bien-être de son personnel.

Les obligations relevant du « duty of care » ne se limitent pas aux relations contractuelles, par exemple entre employeur et employé. En effet, les organisations doivent aussi assumer un « duty of care » à l'égard de ceux qui agissent pour le compte de l'organisation, tels que les sous-traitants indépendants, les consultants, les bénévoles, les personnes à charge et les visiteurs officiels.

Le niveau de responsabilité d'une organisation à l'égard d'un individu est souvent déterminé par la mesure dans laquelle cette personne maîtrise son environnement de travail et ses fonctions, ainsi que par son accès à l'information relative aux éventuels risques : plus l'organisation exerce un degré élevé de contrôle ou d'influence, plus grande sera sa responsabilité. Par exemple, lorsqu'une ONG organise la visite d'un consultant, y compris son itinéraire, son transport et son logement, sa responsabilité à l'égard du

consultant augmente. Cela vaut plus particulièrement lorsque l'organisation, de par sa présence ou ses activités dans le pays, est mieux placée que le visiteur pour surveiller les risques.

Les petites ONG ne disposent souvent pas de bureaux fixes dans le pays, aussi le personnel se déplacera-t-il de manière individuelle et/ou sera-t-il intégré à une organisation partenaire. L'employeur conservera alors ses obligations de sécurité à son égard et devra s'assurer que la gestion du risque sécurité de l'organisation partenaire est adaptée afin de pouvoir assumer ces responsabilités.

Votre duty of care

Toutes les organisations ont une obligation juridique et morale d'instaurer des normes de sécurité permettant de protéger les employés et individus travaillant pour le compte de l'organisation des risques raisonnablement prévisibles. Pour remplir votre « duty of care » vous devez :

- **Connaître les risques** – les organisations doivent pouvoir prouver qu'elles ont identifié et tenu compte de tous les risques prévisibles se rattachant à un lieu ou une activité spécifique. Les évaluations des risques doivent être régulièrement actualisées et documentées.
- **Instaurer des mesures d'atténuation** – les organisations doivent prendre toutes les mesures raisonnables pour gérer les risques. Des plans, procédures et mécanismes exhaustifs et actualisés doivent être en place et respectés pour pouvoir répondre aux risques dans un lieu donné ou associés à une activité spécifique. Le respect des normes communautaires locales vous permettra de démontrer que vous savez quelles sont les meilleures pratiques employées par les autres ONG de la région dans laquelle vous travaillez.
- **Elaborer des plans d'urgence** – des plans, des mesures et une assistance doivent être en place pour répondre aux situations d'urgence impliquant le personnel, où qu'il se trouve.
- **Obtenir un consentement éclairé** – le personnel doit comprendre et accepter les risques auxquels il fait face et les mesures en place pour gérer ces risques. Un processus doit être en place pour documenter sa compréhension des risques et le rôle qu'il doit jouer dans leur gestion. A noter toutefois que ces documents ne constituent pas une clause de renonciation devant un tribunal.
- **Sensibiliser** – le personnel doit recevoir des informations et conseils détaillés et actualisés et, dans bien des cas, une formation, se rapportant aux risques auxquels il s'expose.
- **Apporter un soutien adapté** – les organisations doivent disposer d'un soutien et d'une assurance pour aider le personnel affecté par un incident.

Les responsabilités en matière de « duty of care » s'appliquent aux environnements à haut risque tout comme aux environnements à faible risque. Il est toutefois attendu des organisations qu'elles assument une responsabilité accrue à l'égard du personnel qui travaille dans des situations à haut risque. Il faut reconnaître que les risques ne peuvent pas tous être supprimés, notamment dans les environnements à haut risque. Une grande importance doit donc être accordée au caractère « raisonnable » des actions entreprises, et le personnel doit avoir les informations nécessaires pour prendre une décision éclairée sur les risques résiduels auxquels il pourrait rester exposé.

Complément d'information

Article de l'EISF « Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications », Edward Kemp et Maarten Merkelbach

Manuel de l'EISF « Security Audits »

« Can you get sued? Legal liability of international humanitarian aid organisations towards their staff », Edward Kemp et Maarten Merkelbach

« Voluntary Guidelines on Duty of Care to Seconded Civilian Personnel », Maarten Merkelbach

Définir les attitudes face au risque

Les ONG affichent différents niveaux d'exposition et attitudes face au risque, selon leur mandat et leurs valeurs, le besoin perçu de mener leurs activités ou l'impact espéré, et en fin de compte, leur capacité à absorber ou gérer les risques auxquels s'expose leur personnel.

Soyez conscient/informé plutôt qu'opposé à tout risque

Il est primordial que toutes les organisations identifient leur propre profil de risque et déterminent le niveau de risque qu'elles sont prêtes à accepter. Les risques auxquels s'expose le personnel doivent toujours rester proportionnels à la nécessité de mener des activités spécifiques ou d'en tirer des bénéfices, à la capacité de l'organisation à gérer ces risques, et aux conséquences si un incident venait à se produire. Le fait de fournir à votre personnel une référence quant à votre attitude face au risque, parfois appelée « seuil de risque », permettra d'orienter la prise de décisions, par exemple pour déterminer s'il convient d'autoriser un déplacement ou de démarrer une activité dans un certain lieu présentant un risque plus élevé, ainsi que pour savoir quand arrêter ou suspendre des activités ou retirer du personnel en raison d'une dégradation de la situation sécuritaire ou de menaces spécifiques.

Tout le personnel doit bien comprendre le niveau de risque que l'organisation est prête à assumer pour certaines activités, ainsi que quand et de quelle manière il faut soumettre une décision à un supérieur hiérarchique. Les principaux documents sécuritaires de l'organisation, tels que la politique sécurité de votre ONG, doivent comprendre une déclaration claire sur l'attitude de l'organisation face au risque, ainsi que des informations sur la manière dont ces seuils de risque sont évalués, et les processus d'autorisation et mesures de sécurité requis pour les différents niveaux de risque.

▶ *Voir section 6 : Gestion des déplacements et support*

Complément d'information

Document d'information de l'EISF, « Risk Thresholds in Humanitarian Assistance »

« Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management », Oliver Behn et Madeleine Kingston

ISO 31000:2009

Instaurer une culture de sécurité

Une culture de sécurité positive est essentielle pour la sécurité du personnel de votre organisation. La « culture » d'une organisation peut simplement se définir comme « la manière de faire les choses ici ». Chaque organisation a une attitude culturelle à l'égard de la sécurité et des risques en général. Ce qui fait la différence, c'est que certaines organisations encouragent un environnement de travail sécurisé, et d'autres non. Il ne sert à rien pour une organisation de déclarer qu'elle prend la question de la sécurité très au sérieux et qu'elle dispose de politiques et de procédures si sa culture n'engendre pas une approche positive à l'égard de la sécurité. Tout le personnel doit comprendre et démontrer les valeurs de l'organisation au quotidien.

« Si l'organisation n'a pas de culture de sécurité bien ancrée, la culture qui prévaut en chaque lieu dépendra des individus qui s'y trouvent ; ce qui signifie qu'il existera différentes approches à travers l'organisation en matière de sécurité, certaines étant de qualité mais d'autres étant insuffisantes – le résultat global étant que l'organisation ne disposera pas d'une culture de sécurité qui lui soit propre ; le personnel s'en rendra rapidement compte et en tiendra rigueur à l'organisation. »

Un conseiller en sécurité d'une ONG

Pour créer une culture positive de sécurité au sein de votre organisation, il faut sensibiliser et inculquer un sens de la responsabilité parmi l'ensemble du personnel ; chaque membre du personnel, y compris les membres de

l'équipe dirigeante, doit assumer une responsabilité personnelle à l'égard de sa sécurité et veiller activement à l'intégrer dans tous les aspects des programmes et activités. Des actions simples, telles que la récompenser le respect des procédures, ou encourager la participation du personnel tels que les chauffeurs dans l'élaboration des mesures de sécurité, par exemple, peuvent avoir un impact notoire sur les attitudes et les comportements, sans nécessiter de nombreuses ressources supplémentaires.

11 mesures pour instaurer une culture positive de la sécurité

1. **Concevoir un cadre** – présentez la stratégie de l'organisation en matière de sécurité, y compris les politiques, procédures et mécanismes mis en œuvre pour assurer une gestion efficace du risque sécurité.
2. **Rédiger une politique** – présentez l'attitude de l'organisation face aux risques et les principes de sécurité essentiels, et définir les rôles et responsabilités. Inclure les responsabilités et obligations en matière de sécurité dans les descriptifs de poste de tous les personnels et cadres.
3. **Sensibiliser** – consultez différents membres du personnel, pour vous assurer que tout le monde a connaissance et est d'accord avec les priorités en matière d'amélioration de la gestion du risque sécurité, depuis le conseil d'administration jusqu'aux échelons inférieurs. S'assurer que les cadres émettent des déclarations claires sur l'importance de la sécurité du personnel. Le personnel devra « s'approprier » les mesures prises, qui ne devront pas être perçues comme ayant été imposées depuis le sommet de la hiérarchie sans consultation ni accord du personnel.
4. **Donner l'exemple** – veillez à ce que toute pratique sécuritaire, par exemple les formations à la sécurité personnelle ou les formulaires de planification des déplacements, soient obligatoires pour tout le monde, jusqu'au PDG.
5. **Proposer des alternatives** – la gestion du risque sécurité n'est pas un modèle « taille unique ». Assurez-vous que les mesures et plans pertinents au niveau local soient mis en œuvre dans différents contextes de sécurité et environnements de risque.
6. **Rechercher des « victoires rapides »** – identifiez les mesures ou exigences pouvant être imposées rapidement, sans nécessiter beaucoup de temps et de ressources, susceptibles d'avoir un effet positif sur la sécurité du personnel.
7. **Signaler, toujours signaler, encore signaler** – insistez auprès du personnel sur l'importance du signalement des incidents et des accidents évités de justesse. Veiller à ce que des mécanismes faciles et efficaces soient en place pour signaler et enregistrer ces incidents.
8. **Instaurer des forums sécurité** – créez différents mécanismes ou réunions au sein de l'organisation pour pouvoir soulever et discuter des

problèmes et défis. S'assurer que la sécurité est systématiquement à l'ordre du jour des principales réunions.

9. Contrôler et réviser – menez des examens périodiques de la stratégie sécuritaire de l'organisation et de son cadre de gestion, ainsi que de sa mise en œuvre, pour veiller à l'efficacité durable du cadre.

10. Appliquer l'obligation de rendre des comptes – instaurez un mécanisme pour responsabiliser les personnes en matière de sécurité, et veiller à ce que les responsabilités relatives à la gestion du risque sécurité soient incluses dans les bilans de performance du personnel.

11. Célébrer les réussites – identifiez les approches positives et trouver des champions pour motiver les autres personnels sur les impacts positifs d'une sécurité améliorée : sécurité améliorée = accès amélioré = meilleurs résultats.

Une culture positive de sécurité ne peut s'instaurer du jour au lendemain : il faut du temps pour transformer les attitudes et comportements du personnel, et donc l'approche globale de l'organisation à l'égard de la gestion du risque sécurité. Vous rencontrerez certainement des obstacles et des difficultés, et un certain niveau de résistance interne, de non-conformité et d'insuffisance des ressources. Soyez réalistes en reconnaissant que l'instauration d'une culture positive de sécurité est un processus de longue haleine, et organisez-vous en conséquence. Il vaut mieux commencer par des objectifs facilement atteignables pour donner une impulsion à ce « changement culturel » et partir de là. Il vaut mieux avoir un système de gestion du risque sécurité partiel qu'aucun système.

« Nous disposions de toutes les politiques et procédures de sécurité, mais la culture organisationnelle ne s'est transformée qu'une fois que le PDG a suivi une formation sur la sécurité personnelle. »

Responsable humanitaire d'une ONGI

Complément d'information

« Developing a Security-Awareness Culture – Improving Security Decision Making », Chris Garrett

Affecter des ressources à la gestion du risque sécurité

La gestion de la sécurité implique des coûts inévitables. Le développement et le lancement d'une stratégie globale de gestion du risque sécurité sont des tâches qui peuvent exiger beaucoup de temps et d'importantes ressources financières – qui font défaut dans toutes les organisations.

Pour les petites ONG, les limitations en termes de capacités et de fonds sont souvent perçues comme un obstacle majeur à une gestion efficace de la sécurité. Il faut cependant noter que de nombreux aspects de la gestion du risque sécurité ne nécessitent pas du temps et des budgets considérables. Par exemple, il existe de nombreux modèles de gestion des risques de type « open source » et autres outils et ressources (accessibles par exemple par le biais de l'EISF et d'InterAction) qui peuvent facilement être adaptés et employés par les ONG. En outre, si la formation sécurité peut représenter un investissement majeur pour les petites organisations, de nombreux cours en ligne sont disponibles pour sensibiliser le personnel aux questions sécuritaires et améliorer ses capacités.

▶ *Voir section 7 : Sensibilisation et renforcement des capacités*

En outre, les bailleurs de fonds sont de plus en plus nombreux à admettre que la sécurité du personnel fait partie intégrante du travail de programmation dans les zones non sécurisées. De nombreux bailleurs de fonds de premier plan sont disposés à financer certains coûts sécuritaires. Par exemple, la réalisation d'évaluations et d'audits de la sécurité, l'identification des postes dédiés à la sécurité, l'acquisition d'équipements sécuritaires essentiels, l'amélioration de la sécurité des principales installations et les formations sont autant de coûts que de nombreux donateurs sont désormais prêts à financer. Il est primordial que les ONG identifient et justifient les coûts de la sécurité par une évaluation des risques et veillent à englober les considérations et coûts sécuritaires dans les propositions de programmes et les budgets, sans se contenter de les inclure dans les frais généraux (indirects).

Voir le document d'information de l'EISF « The Cost of Security Risk Management for NGOs »

Au fur et à mesure que votre organisation améliorera sa stratégie relative à la sécurité de son personnel, vous constaterez de nombreuses « victoires faciles », mais en fin de compte, tout est question de priorisation et de ressources. L'élaboration d'un cadre de gestion du risque sécurité efficace nécessitera d'engager des ressources financières et humaines suffisantes ; il est donc

important d'aborder ces questions au plus tôt et de veiller à ce que l'équipe dirigeante s'engage à prioriser la sécurité et à lui octroyer des ressources adaptées.

Complément d'information

Voir le document d'information de l'EISF « The Cost of Security Risk Management for NGOs »

« The Risk Management Expense Portfolio (RMEP) Tool » dans le document d'information « The Cost of Security Risk Management for NGOs »

2 Elaborer un cadre

La première étape de l'élaboration d'un système capable de protéger le personnel consiste à développer un cadre de gestion du risque sécurité présentant l'architecture, les rôles, les responsabilités et les différentes dispositions mises en place par votre organisation. Celles-ci visent à améliorer l'accès aux populations affectées, à travers l'optimisation de la sécurité du personnel.

Un cadre de gestion du risque sécurité consiste en une série de politiques, protocoles, plans, mécanismes et responsabilités qui contribuent à réduire les risques sécuritaires encourus par le personnel.

Votre organisation a un large éventail de risques à gérer, aussi bien financiers, opérationnels et juridiques que de réputation. La gestion du risque sécurité n'est qu'un des éléments de la gestion globale des risques incombant à l'organisation, et elle doit s'aligner sur sa stratégie globale de gestion des risques ainsi que sur les politiques et processus existants. Un cadre de gestion du risque sécurité (GRS) est un système intégré unique composé de deux éléments principaux :

- Les **bases**, qui comprennent une bonne gouvernance sécuritaire et une structure responsable, ainsi qu'une politique et des principes de sécurité.
- Les **mécanismes**, qui comprennent les différents plans, procédures, activités et ressources servant à gérer le risque sécurité du personnel.

Notez que le cadre de gestion du risque sécurité n'est PAS un document unique. Vous devrez toutefois commencer par élaborer un document de travail ou « schéma » présentant la manière dont ce cadre confère à votre organisation une stratégie de gestion du risque sécurité, et les liens entre les différents documents et processus qui en font partie.

Le graphique suivant illustre les principaux éléments constituant un cadre de gestion du risque sécurité et articulation.

Cadre de gestion du risque sécurité

3 Gouvernance et responsabilité

Une gouvernance et des structures responsables de qualité sont des caractéristiques essentielles du cadre de gestion du risque sécurité. À tous les niveaux de l'organisation – des membres du conseil d'administration aux employés – le personnel – doit assumer une responsabilité collective à l'égard de la gestion et de la réduction des risques. S'il incombe à chaque employé d'assumer un certain degré de responsabilité pour sa propre sécurité, chaque organisation, quelle que soit sa taille, doit veiller à disposer d'une structure de gestion efficace, propice à une culture de sécurité positive et qui l'aide à remplir son « duty of care ».

Concevoir une structure de gestion du risque sécurité efficace

La responsabilité finale de la sécurité du personnel incombe au conseil d'administration, lequel délègue ensuite cette responsabilité au Directeur

exécutif/PDG ou à un cadre similaire, pour s'assurer de disposer d'une gestion efficace du risque sécurité. Au quotidien, la gestion et la responsabilité relative à la sécurité sont réparties entre différents niveaux de l'organisation et suivent généralement le modèle de la ligne managériale. Le descriptif de poste de tout le personnel qui assume des responsabilités en matière de sécurité doit préciser clairement quel rôle lui incombe et son obligation de rendre des comptes doit être évaluée lors des bilans de performance.

Il est essentiel de bien choisir les personnes chargées de la sécurité. Un grand nombre de grandes organisations disposent désormais de conseillers sécurité dédiés, voire d'équipes sécurité, chargés de superviser le cadre sécurité de l'organisation et de fournir un support et des conseils en matière de sécurité. Cependant, ce modèle est irréaliste pour les petites ONG.

Il vous faut identifier une personne voire un groupe de personnes au sein de votre organisation capable de servir de point focal de la sécurité et de prendre l'initiative d'élaborer et de mettre en œuvre le cadre sécurité. Il est important que ces personnes se voient octroyer le temps, l'appui et la formation nécessaires pour assumer ce rôle en plus de leurs fonctions habituelles.

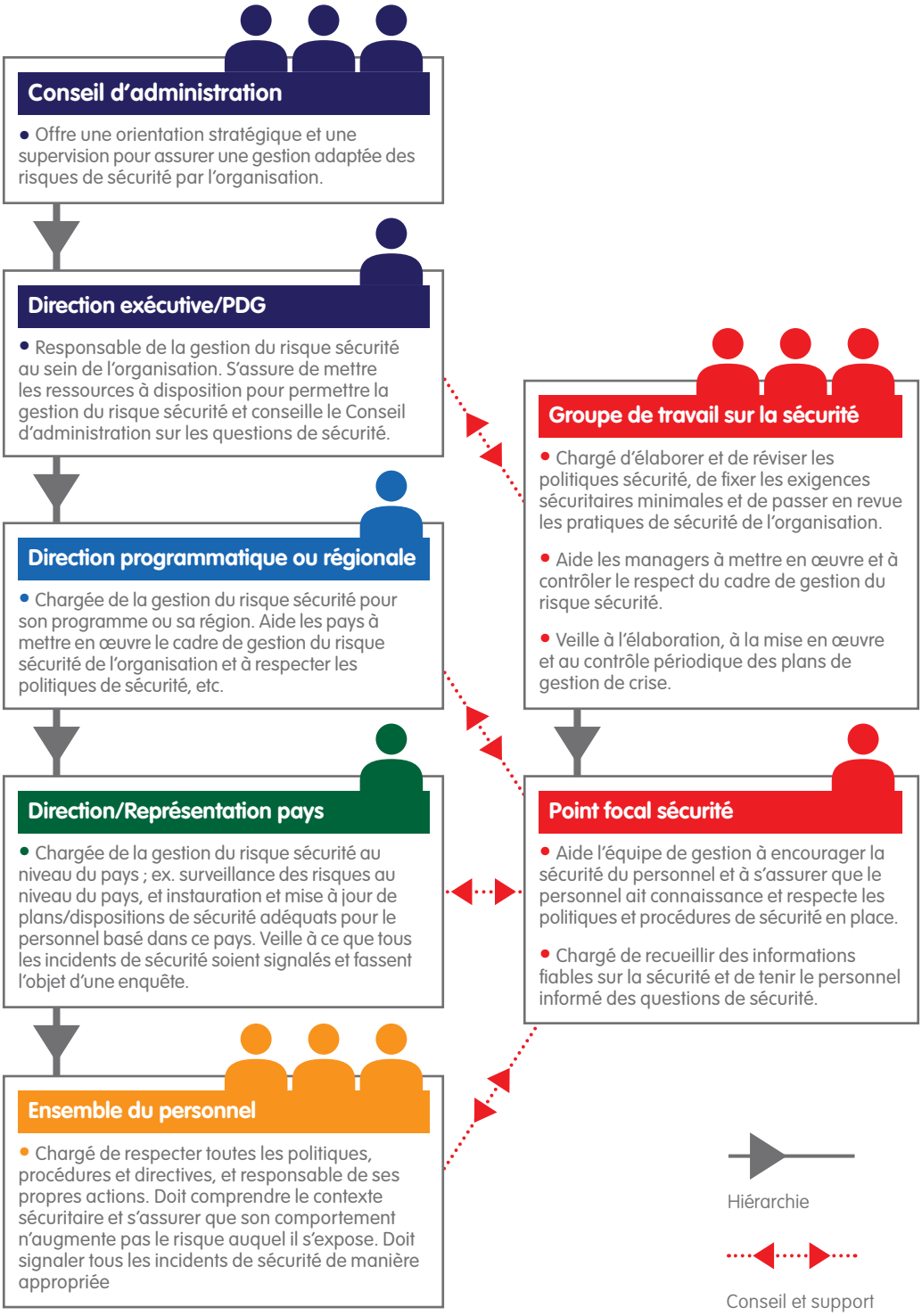
La gestion des risques est une responsabilité partagée. La concrétisation d'une bonne gestion du risque sécurité nécessite des rôles et des responsabilités clairement définis, ainsi que des structures capables d'apporter et de maintenir un soutien efficace.

De nombreuses organisations font appel à un groupe de travail chargé de la sécurité ou à un comité de représentants regroupant différents rôles et niveaux de hiérarchie au sein de l'organisation. Cette approche collective aide au partage des tâches, rapproche un large éventail d'expériences et de perspectives, et incite les différents acteurs à s'approprier le processus, ce qui favorise sa mise en œuvre et son application.

Il convient de noter que le point focal ou groupe de travail sécurité n'est pas responsable de la gestion du risque sécurité (le risque ne lui « appartient » pas). En effet, les responsabilités en matière de gestion de la sécurité doivent faire partie intégrante de la gestion normale des programmes. Le rôle du point focal ou du groupe de travail sécurité est d'appuyer l'élaboration d'un cadre de gestion du risque sécurité pour l'organisation et de s'assurer de l'existence des politiques et procédures convenues, ainsi que de fournir des conseils à la hiérarchie le cas échéant.

Pour identifier les rôles et responsabilités relatifs à la sécurité, il vous faudra réfléchir à ce qui convient le mieux et est le plus réaliste pour votre organisation en tenant compte de sa taille, de la complexité de sa structure, des rôles et capacités existants et du type de travail que fait votre organisation.

Exemple de structure et de responsabilités



Identifiez d'abord les postes existants qui jouent un rôle crucial dans la sécurité du personnel, y compris les managers basés au siège et les équipes pays (si votre organisation dispose d'une présence permanente dans le pays). Ensuite, définissez clairement les responsabilités en matière de sécurité et les rôles décisionnels à associer à chacun de ces postes. Ces postes et leurs responsabilités sécurité devront être clairement décrits dans la politique sécurité de l'organisation afin que l'ensemble du personnel en soit informé.

Complément d'information

Exemple de descriptif de poste : Agent Logistique et sécurité

Exemple de descriptif de poste : Coordinateur de la sécurité sur le terrain

Exemple de descriptif de poste : Directeur adjoint de la sécurité mondiale

Exemple de descriptif de poste : Directeur de la sûreté et de la sécurité du personnel

4 Politiques et principes

La politique sécurité de votre organisation est la pierre angulaire de son cadre de gestion du risque sécurité. L'élaboration d'une politique sécurité globale vous aidera à démontrer l'engagement de votre organisation envers la sécurité de votre personnel. La politique est aussi une déclaration claire de la stratégie de l'organisation face aux risques de sécurité, des principes clés sous-jacents à cette stratégie, et des rôles et responsabilités qui incombent aux membres du personnel pour gérer ces risques.

Une politique sécurité est un impératif pour toutes les organisations, quelle qu'en soit la taille. Elle permet d'informer le personnel sur les principes, approches et responsabilités relatifs à la gestion du risque sécurité et veille à ce que le personnel agisse d'une manière adaptée à l'organisation.

Élaborer une politique sécurité

Pour être en mesure d'élaborer ou de réviser la politique sécurité de votre organisation, vous devez d'abord en préciser l'envergure :

- S'agit-il uniquement de sécurité, ou santé et sécurité au travail ? Les politiques sécurité de certaines ONG ne comprennent pas la santé et le bien-être au travail, celle-ci étant déjà prise en compte dans une politique distincte.
- Quels aspects sont couverts par la politique ? Elle s'applique bien évidemment au personnel, mais qu'en est-il des consultants, des sous-traitants, des bénévoles, des visiteurs, des personnes à charge ou des autres parties associées ? La politique devra porter sur la sécurité de tous, en indiquant clairement les éventuelles différences d'un groupe à un autre.

La politique sécurité doit être un document court et accessible traduit dans les principales langues de travail de l'organisation. La plupart des politiques sécurité se composent de quatre parties clés :

1. Une **déclaration** sur l'importance de la sécurité et de la santé du personnel, la portée de la politique et les entités auxquelles elle s'applique.
2. Une partie sur les **« principes »** expliquant la culture de sécurité de l'organisation, son attitude face au risque et les principes clés qui façonnent la stratégie de l'organisation en matière de sécurité du personnel.
3. Une partie sur les **« responsabilités »** décrivant la structure de gestion du risque sécurité de l'organisation et les rôles et actions attribués aux différents postes.
4. Une partie sur les **« exigences de sécurité minimales »** indiquant les exigences sécurité spécifiques de l'organisation devant être en place ; par exemple, chaque pays doit disposer d'un plan sécurité.

La politique sécurité est un important document de gouvernance qui doit être avalisé par la direction exécutive ou par une personne qui occupe un poste similaire, puis approuvé par le conseil d'administration. La politique sécurité doit renvoyer aux autres politiques et codes régissant l'organisation qui indiquent les exigences en matière de gestion du risque sécurité, tels que la politique santé et bien-être au travail, le code de conduite du personnel, les protocoles de déclenchement d'alerte et les politiques relatives au bien-être matériel et sanitaire du personnel, à la fraude et à la corruption, ainsi qu'à la sécurité de l'information.

Principes communs en matière de sécurité

- **Responsabilité partagée** – la gestion et la réduction des risques pour le personnel constituent une responsabilité partagée impliquant le personnel à tous les niveaux de l'organisation.
- **Reconnaissance du risque** – gérer la sécurité ne signifie pas que tous les risques seront éliminés. Chaque membre du personnel doit comprendre, dans le cadre de son consentement éclairé, qu'il reste exposé au risque.
- **Primauté de la vie** – la sécurité du personnel est de la plus haute importance pour l'organisation, et le personnel ne doit jamais se placer dans une situation lui faisant courir un risque excessif pour remplir les objectifs du programme ou protéger des biens.
- **Risque proportionnel** – le risque pour le personnel doit être constamment évalué et être proportionnel à la nécessité de mener certaines activités, ou d'en dégager des avantages, ainsi qu'à la capacité de l'organisation de gérer ce risque.
- **Sécurité équitable** – certains individus sont susceptibles d'être plus exposés à certains dangers que leurs collègues. Ils devront être informés des risques, mais les restrictions/mesures de sécurité ne doivent pas être discriminatoires à l'égard d'individus sur la base de leurs caractéristiques personnelles.
- **Droit de rétractation** – tout le personnel doit avoir le droit de se retirer, ou de refuser un travail dans une zone particulière pour des raisons de sécurité.
- **Aucun droit de rester** – l'organisation a le droit de suspendre des activités ou de retirer du personnel des situations qu'elle juge trop dangereuses. Le personnel n'a pas le droit de rester en un lieu si ses supérieurs lui ont ordonné d'en partir.
- **Stratégies de sécurité** – il s'agit de la stratégie employée par l'organisation pour réduire le risque. Pour la plupart des ONG, il s'agira de trouver un juste équilibre entre l'« acceptation » et la « protection », la « dissuasion » étant une approche moins commune.
  Voir le manuel de l'EISF « Security to go » et le manuel d'ODII « GPR8 – Operational Security Management in Violent Environments »

La politique sécurité devra clairement décrire la position de l'organisation par rapport aux armes et au personnel armé, ses relations avec les acteurs armés et le recours aux ressources militaires, ainsi que sa position sur les questions de rançon et de pots-de-vin.

Complément d'information

Exemple de cadre de politique sécurité organisationnelle

« Open NGO Security Policy », Centre for Safety and Development

Manuel de l'EISF « Security to go: a risk management toolkit for humanitarian aid agencies

Manuel de l'EISF « Security Audits »

Manuel ODI « GPR8 - Operational Security Management in Violent Environments »

Page thématique de l'EISF « Policy, Procedure and Practice in GRS »

Définir les exigences en matière de sécurité

Votre politique sécurité doit présenter les exigences sécuritaires de base que l'organisation compte trouver de manière systématique sur tous les sites vers lesquels elle envoie son personnel ou dans lesquels il est basé. Par exemple, l'ensemble du personnel doit-il assister aux initiations et réunions d'information sur la sécurité ? Un type spécifique de formation sécurité est-il nécessaire pour pouvoir se rendre ou travailler dans certains lieux ? Les déplacements vers des sites présentant un risque plus élevé nécessitent-ils une autorisation ? Tous les bureaux pays sont-ils tenus de compléter une évaluation des risques et d'élaborer des plans sécurité ?

▶ *Voir « Plans sécurité » au chapitre 5 : Opérations et programmes*

« Soyez réalistes quant aux capacités et aux ressources dont dispose votre organisation. Il ne sert à rien d'imposer d'énormes exigences minimales si votre organisation n'a pas les capacités ou les ressources nécessaires. Même si une exigence peut être reconnue comme étant une bonne pratique, la crédibilité de la politique sécurité sera mise à mal si le personnel est obligé d'ignorer une exigence faute de ressources. Cela dit, il est impératif de toujours assumer son « duty of care », quelles que soient les ressources et les capacités de votre agence. »

Conseiller sécurité d'une ONG

Étant donné la diversité des pays et donc des contextes sécuritaires dans lesquels votre personnel travaille ou voyage, il est évident que tous les pays n'auront pas besoin des mêmes mesures de sécurité. Les exigences de sécurité doivent être adaptées au niveau de risque. Les systèmes doivent toutefois être le plus simples possible pour ne pas dérouter le personnel et veiller à ce qu'ils soient suivis. Par exemple, la politique pourra indiquer que tout le personnel doit assister à une réunion d'information avant son départ, même si le contenu de cette réunion peut changer. Par conséquent, les employés qui se rendent dans des environnements à plus haut risque auront

besoin d'assister à une séance d'information sécurité détaillée avant leur départ, tandis que ceux qui se rendent dans une destination à risque modéré n'auront éventuellement besoin que de conseils élémentaires.

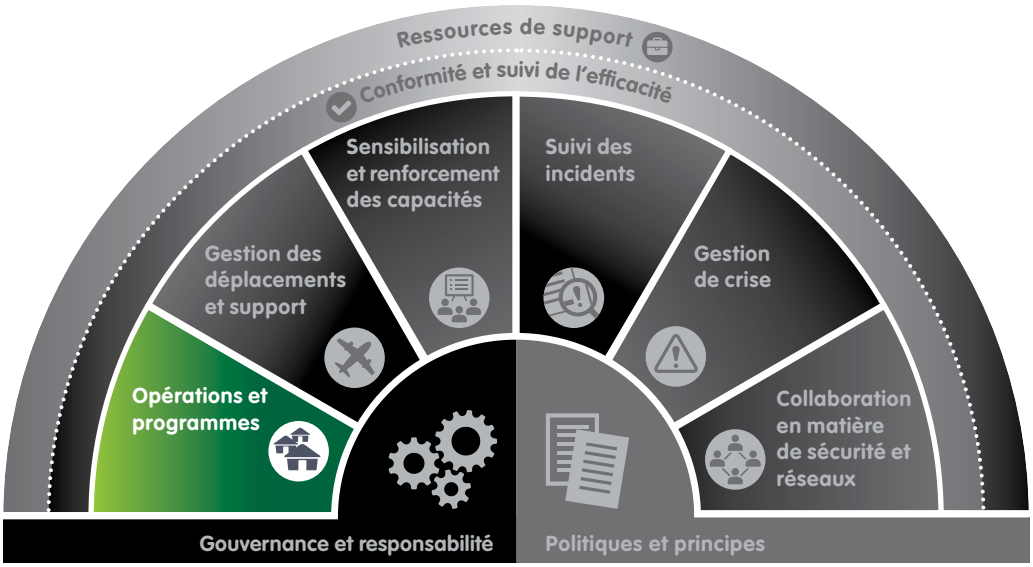
La mise en œuvre de la politique dépendra également selon que votre personnel se rend dans un pays doté d'un bureau pays ou auprès d'une organisation partenaire.

Il est important de noter que les exigences sécurité ne constituent pas à elles seules un système exhaustif de gestion du risque sécurité ; il s'agit du minimum requis, et d'un point de départ à partir duquel élaborer une gestion solide du risque sécurité conforme aux bonnes pratiques et adaptée au niveau de risque auquel votre personnel s'expose.

Complément d'information

« Minimum Operating Security Standards (MOSS) », InterAction

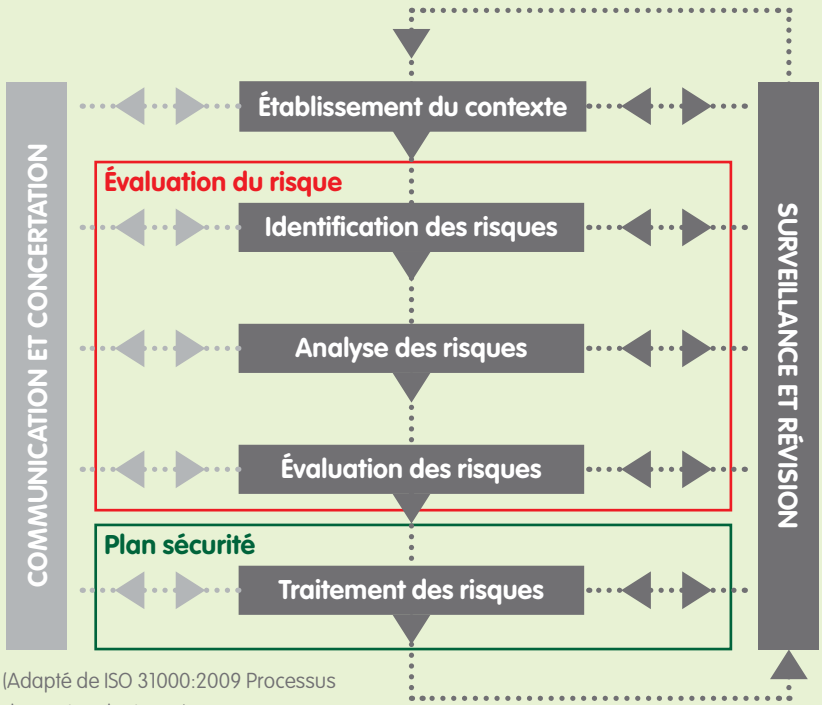
5 Opérations et programmes



Il est primordial de se préparer en se dotant de plans, de procédures et de ressources réalistes pour gérer les risques au sein de vos opérations et programmes. Vous devrez instaurer un processus systématique de gestion du risque sécurité permettant aux managers d'analyser l'environnement opérationnel, d'identifier les risques pour le personnel et les opérations, et de déterminer les stratégies et mesures les mieux adaptées pour gérer les risques dans ce contexte précis.

« Lorsque vous élaborez des plans et procédures pour gérer le risque, il est important de reconnaître que l'objectif est de permettre à votre personnel d'obtenir et de maintenir un accès sécurisé afin de délivrer les programmes, et qu'il ne s'agit pas de gestion de la sécurité pour faire de la gestion de la sécurité à tout prix. S'il n'est pas possible d'instaurer des mesures permettant à votre personnel de travailler dans les limites du seuil de risque convenu par votre organisation, revoyez vos objectifs en tenant compte du contexte. »
Directeur sécurité d'une ONG

Processus de gestion du risque



(Adapté de ISO 31000:2009 Processus de gestion du risque)

Les ONG ont le choix entre différents modèles de processus de gestion du risque.

Par exemple, la norme internationale ISO 31000:2009 a été intégrée par un grand nombre d'ONG. Elle définit le risque comme l'incidence de l'incertitude sur les objectifs, et prévoit les étapes suivantes :

- **Établissement du contexte :** définir les paramètres externes et internes. Une parfaite compréhension de votre environnement opérationnel et des différentes parties prenantes impliquées, et une connaissance détaillée de l'impact de votre ONG sur le contexte de par ses activités, le personnel impliqué et les capacités de votre organisation, vous permettront d'apprécier les éventuels défis sécurité pour votre personnel, vos programmes et votre organisation.
- **Identification des risques :** identifier toutes les menaces envisageables en matière de sécurité pouvant affecter votre personnel, vos programmes ou votre organisation (y compris sa réputation), et comprendre comment, quand et pourquoi chaque menace pourrait se produire.
- **Analyse des risques :** réaliser une évaluation complète pour connaître le risque que les différents membres du personnel soient confrontés aux différentes menaces identifiées. Vous devrez évaluer chaque risque

(menace et exposition à celle-ci) afin d'en déterminer la gravité, en tenant compte de la probabilité qu'il se produise et de son incidence potentielle s'il venait à se produire, étant donné les mesures et procédures actuellement en place.

- **Évaluation des risques :** si vous comprenez bien l'exposition au risque de l'organisation, vous prendrez des décisions éclairées et saurez s'il convient d'accepter certains risques ou de prendre des mesures supplémentaires pour les prévenir ou les minimiser.
- **Traitement des risques :** possibilités s'offrant à votre organisation de prévenir ou de minimiser/atténuer le risque. Il peut s'agir de réduire le risque, de le transférer ou de le partager avec d'autres parties, voire de l'éviter en choisissant de ne pas entreprendre l'activité en question. Réduire le risque sécurité implique de mettre en œuvre différentes stratégies pour minimiser la probabilité d'occurence et/ou l'incidence de certaines menaces. Ces stratégies sont mises en pratique lors du développement des plans sécurité d'un pays ou d'une région.
- **Surveillance et révision :** vous devez continuellement passer en revue chaque composant du processus de gestion du risque pour vous assurer que les stratégies et mesures actuelles restent adaptées à la situation.

Il est crucial de faire preuve d'une communication et d'une concertation efficaces. Aucun individu ne possède toutes les informations nécessaires pour déterminer, analyser et réduire les risques. Il est donc important d'identifier un éventail de parties prenantes, à la fois internes et externes, capables de vous aider dans ce processus.

Le processus de gestion du risque peut également servir à évaluer les organisations partenaires dans lesquelles votre personnel pourrait se rendre ou au sein desquelles il pourrait être intégré.

Complément d'information

Manuel de l'EISF « Security to go: a risk management toolkit for humanitarian aid agencies »

Norme ISO 31000:2009

Manuel ODI « GPR8 - Operational Security Management in Violent Environments »

Document d'information de l'EISF « Security Management and Capacity Development: International agencies working with local partners »

Document d'information de l'EISF « Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management »

Document d'information de l'EISF « Security Risk Management and Religion: Faith and secularism in humanitarian assistance »

À paraître : document d'information de l'EISF « Managing the Security of Staff with Diverse Profiles »

Évaluations du risque sécurité

Les évaluations du risque vous permettent d'identifier les dangers pour votre organisation, vos programmes et, surtout, votre personnel sur un site donné. L'évaluation du risque sécurité est un élément fondamental du processus de gestion du risque, et il fait partie intégrante des évaluations plus générales réalisées avant le lancement d'opérations ou de programmes dans un pays, que leur mise en œuvre se fasse directement ou par le biais de partenaires.

Matrice des risques

		Impact				
		Négligeable	Faible	Modérée	Élevée	Très élevée
Probabilité	Certaine/ imminente					
	Probable					
	Modérée					
	Peu probable					
	Rare					

Risque extrême	Des mesures doivent être prises immédiatement. Le risque est-il acceptable ?
Risque élevé	Mettre en œuvre des mesures de sécurité spécifiques ainsi que des plans d'urgence.
Risque moyen	Faire preuve d'une vigilance accrue et adopter des procédures supplémentaires.
Faible risque	À gérer par le biais des procédures habituelles de sécurité

Il est essentiel de comprendre dans le détail les risques qui existent dans un contexte spécifique pour que votre organisation puisse prendre des décisions sécuritaires plus éclairées.

L'évaluation du risque ne doit pas être un événement ponctuel. Une réévaluation continue de tous les risques possibles vous permettra de disposer à tout moment de mesures de sécurité adaptées.

Le processus d'évaluation du risque consiste dans un premier temps à identifier les différentes menaces sécuritaires dans un contexte donné, et la vulnérabilité potentielle de votre personnel, de vos actifs, des programmes en cours de mise en œuvre ou de votre organisation. Il les analyse ensuite en fonction de leur probabilité d'occurrence et de leurs conséquences afin de déterminer le degré de risque. Enfin, il identifie et évalue les différentes solutions qui pourraient être mises en œuvre pour gérer ces risques. Une fois les mesures d'atténuation du risque identifiées, il est probable qu'il reste encore un certain risque résiduel, qu'il conviendra de comparer au seuil de risque de votre organisation pour savoir s'il est acceptable que le programme se poursuive. Si une évaluation du risque identifie des mesures à prendre, mais que celles-ci ne sont pas mises en œuvre, l'organisation pourrait être considérée comme ayant failli à son « duty of care ».

Le processus d'évaluation du risque sécurité doit être documenté et inclure les principaux résultats et les mesures proposées pour gérer les différents risques. Les évaluations du risque doivent aussi être régulièrement remises à jour. En outre, le personnel devra savoir ce que signifient les différents niveaux de probabilité d'occurrence et d'impact afin d'analyser plus précisément les différentes menaces et de garantir une cohérence à tous les niveaux de l'organisation. Par exemple, « probable » signifie-t-il qu'il s'agit d'un événement hebdomadaire ou quotidien ? Par ailleurs, il faut préciser la mesure dans laquelle la « conséquence » prévue tient compte de l'impact sur les individus, les activités du programme ou l'organisation dans son ensemble, car ceux-ci peuvent être différents. Pour évaluer la vulnérabilité aux menaces, il faut tenir compte à la fois des données spécifiques relatives à l'organisation et à l'individu. Par exemple, le poste, l'âge, le genre, l'ethnicité, la nationalité et l'orientation sexuelle sont autant de facteurs susceptibles d'avoir une incidence.

« Les évaluations du risque sont souvent perçues comme une corvée administrative, comme une case qu'il faut cocher. C'est ainsi que l'on risque de perdre la relation cruciale entre cette analyse et le programme. »
Conseiller sécurité d'une ONG

Il n'existe pas de format officiel pour réaliser une évaluation du risque sécurité, mais vous trouverez un grand nombre de guides sur les bonnes pratiques ainsi que des outils et des modèles.

Il est important de fournir au personnel un modèle standard d'évaluation du risque à employer sur tous les sites, qui soit simple d'utilisation et qui réunisse les informations essentielles.

Les évaluations du risque bien documentées peuvent également servir à justifier des demandes de ressources et de financement en vue de mettre en œuvre les stratégies et mesures de sécurité requises pour appuyer le personnel opérant dans un contexte spécifique.

Complément d'information

« Module 3: Risk assessment tool » dans le manuel de l'EISF « Security to go »

« Security Assessment Tool », ACT Alliance

Plans sécurité

Les plans sécurité sont des documents établis au niveau de chaque pays qui présentent les mesures et procédures de sécurité en vigueur, ainsi que les responsabilités et ressources requises pour les mettre en œuvre. Des plans sécurité doivent être établis pour tous les sites dans lesquels votre organisation dispose d'une présence significative, ainsi que là où elle s'engage régulièrement. Même si votre organisation n'a aucune présence fixe mais que votre personnel se déplace régulièrement vers un lieu, ou si vous avez un représentant unique ou une petite équipe, un document élémentaire présentant les dispositions sécuritaires et la procédure à suivre en cas d'urgence permettra de s'assurer que le personnel comprenne les mesures en vigueur et, surtout, les respecte.

Si l'évaluation du risque met en évidence une menace, le plan sécurité devra permettre au personnel de savoir comment gérer le risque que cette menace présente.

Les plans sécurité doivent être des documents constamment pertinents et accessibles ; ils doivent porter sur les risques spécifiques et propres au lieu en question ; et, le cas échéant, ils doivent préciser à qui s'adressent les mesures et à quel endroit, par exemple à certains groupes ethniques dans des régions spécifiques. Ces plans doivent être actualisés régulièrement, surtout après des incidents ou des changements significatifs intervenus au niveau de l'environnement opérationnel ou des activités de l'organisation. Ils doivent être traduits dans les langues locales si nécessaire.

Plan sécurité du pays

Un plan sécurité établi pour un pays, ou une zone géographique spécifique, doit notamment comporter les éléments suivants :

- **Informations critiques** – résumé d'une page des informations pertinentes accessibles facilement et rapidement à titre de référence, par exemple les éventuelles restrictions telles que les couvre-feux ou les zones interdites, et les interlocuteurs importants.
- **Présentation générale** – objectif et portée du document, qui se charge du plan sécurité, l'attitude de l'organisation face au risque, sa date de publication et sa date de remise à jour, et une synthèse de la stratégie/politique sécurité de l'organisation.
- **Contexte actuel** – synthèse du contexte opérationnel actuel et de la situation sécuritaire globale, principaux risques pour le personnel, les actifs et les programmes (système d'évaluation du risque), menaces présentes dans ce contexte, et évaluation des menaces et évaluation du risque.
- **Procédures opérationnelles standards (POS)** – procédures de sécurité simples et claires que le personnel doit respecter pour empêcher les incidents, et manière d'y répondre en cas de problème. Les POS doivent être liées aux principaux risques identifiés et porter sur des questions telles que le transport de fonds, les communications, le signalement des incidents, la sécurité des véhicules et, lors des déplacements sur le terrain, la sécurité des installations et des sites, le contrôle de l'accès aux bureaux et aux installations, les vols, les accidents de véhicules, la conduite du personnel, la santé et le bien-être du personnel et la sécurité de l'information.
- **Santé et Stress** – protection du personnel face aux dangers d'ordre sanitaire, ainsi qu'aux accidents, au stress en général et au stress post-traumatique.
- **Ressources humaines** – politiques relatives au recrutement, aux vérifications des antécédents, aux contrats, à la confidentialité, aux formations, à l'évaluation des risques associés aux différents rôles, etc.
- **Briefings sécurité** – de quelles informations le nouveau personnel et les visiteurs doivent disposer, et à quel moment cette information doit être fournie.
- **Sécurité administrative et financière** – politiques de prévention du vol, de la fraude et de la corruption, et gestion des espèces et des achats.
- **Niveaux de sécurité** – niveaux/étapes de sécurité de l'organisation, avec des indicateurs situationnels reflétant les risques accrus auxquels s'expose le personnel dans tel contexte et sur tel site, et actions/mesures spécifiques requises pour répondre à la hausse de l'insécurité.

- **Signalement des incidents** – procédures et responsabilités relatives au signalement des incidents sécuritaires, par exemple type d'incidents à signaler, structure du signalement et format.
- **Gestion de crise** – membres de votre équipe de gestion de crise et règles d'activation. Inclure les plans d'urgence prévus en cas de menaces prévisibles ou d'incidents critiques, tels que la nécessité de délocaliser ou d'évacuer le personnel, les catastrophes naturelles et les urgences sanitaires.
- **Annexes** – informations complémentaires, documents et listes permettant d'aider le personnel à suivre les procédures et plans, par exemple listes de contacts, listes de contrôle et formulaire de signalement des incidents.

Assurez-vous de faire participer le personnel affecté par les risques à la préparation des plans sécurité pour améliorer les chances que ceux-ci soient observés, car le personnel comprendra mieux leur raison d'être.

Complément d'information

« Country Security Plan Example », InterAction

« Module 6: Security plan » dans le manuel de l'EISF « Security to go »

Dispositions sécuritaires et support

Il se peut que votre organisation ne dispose pas d'une présence dans un pays donné, mais que votre personnel s'y rende régulièrement ; ou bien que vous ayez sur place un représentant unique ou une petite équipe. Le personnel devra donc compter sur les partenaires locaux ou sur les organisations hôtes, en sachant que chacun d'eux applique des normes de sécurité et un comportement à l'égard du risque différents – pour garantir leur sécurité lors de leurs visites de programmes ou de leurs activités dans le pays.

Même si vous détachez un membre de votre personnel à une autre organisation, vous ne pourrez pas transférer vos responsabilités en matière de duty of care. En tant qu'organisation contractante, il est votre responsabilité de vous assurer que des mesures de sécurité appropriées existent et sont appliquées.

Le niveau et la qualité du support sécurité dont bénéficie votre personnel dépend du soutien que les partenaires locaux ou les organisations hôtes peuvent, ou souhaitent, apporter. Il se peut ainsi que le partenaire/hôte connaisse mal les risques auxquels votre personnel s'expose ou le niveau de soutien dont il aura besoin. Les risques pour le personnel augmentent si le partenaire/l'organisation hôte n'ont que peu voire pas de procédures de sécurité en place, et/ou s'ils n'ont pas d'équipement de communication. Il se peut également qu'ils fournissent un logement mal sécurisé et des véhicules non fiables.

Si le choix d'un partenaire ou d'un hôte est forcément stratégique et tributaire de nombreux facteurs, vous devez aussi évaluer ses capacités et ses dispositions sécuritaires. Si nécessaire, le partenaire/l'organisation hôte devra être soutenu lors de l'élaboration de ses plans et procédures de sécurité et, si possible, il vous faudra l'aider à bénéficier d'une formation sécurité.

Par ailleurs, soyez disposés à coacher ces partenaires et à les aider à vous fournir l'information sécurité dont vous et votre personnel avez besoin. Même si les partenaires locaux n'ont aucune expérience de la réalisation d'évaluations du risque sécurité ou de plans sécurité, ils disposeront certainement d'informations détaillées sur le contexte, qui vous aideront à évaluer les risques et à planifier les dispositions sécuritaires pour votre personnel.

Même dans les situations où il n'existe aucun partenaire ou hôte formel, le personnel devra être encouragé à instaurer des relations avec d'autres ONG de la région ; certaines d'entre elles seront peut-être disposées à fournir des informations, des données sécuritaires actualisées et un soutien en cas d'urgence. Au minimum, ces contacts peuvent veiller sur le personnel et servir d'interlocuteurs lorsque votre personnel se trouvera dans le pays.

Support sécurité des partenaires/organisations hôtes

- **Sélection** – le processus de sélection d'organisations susceptibles d'accueillir votre personnel doit inclure une évaluation des capacités sécuritaires, de l'attitude et des stratégies en matière de risque, des niveaux d'acceptation au plan local et des procédures et plans sécurité déjà en vigueur.
- **Responsabilités et limites** – veillez à ce que tout accord relatif à un support sécurité soit explicite concernant les responsabilités et éventuelles limites des deux parties, en particulier concernant les différentes responsabilités en cas d'incidents de sécurité ou d'urgence médicale affectant votre personnel.
- **Plans et procédures de sécurité** – veillez à ce que vos partenaires/hôtes disposent de plans et de procédures de sécurité appropriés, et qu'ils en fassent part à votre personnel. Si nécessaire, donnez à vos partenaires des exemples ou des conseils pour les aider à élaborer des documents de sécurité.
- **Partage de l'information** – maintenez un dialogue régulier avec les partenaires/hôtes sur la situation sécuritaire afin de vous mettre d'accord sur le niveau de risque et la meilleure manière de gérer la sécurité de votre personnel. Les partenaires/hôtes devront partager les rapports d'incidents pertinents à votre organisation.
- **Élaboration de réseaux** – les partenaires/hôtes devront être encouragés et, si nécessaire, aidés à se rapprocher des réseaux de sécurité et mécanismes de partage de l'information locaux (par exemple, les réseaux coordonnés par des ONGI ou les Nations Unies).
- **Financement de la sécurité** – dans les contextes présentant un plus grand risque, il peut être nécessaire d'octroyer octroyer des fonds supplémentaires aux partenaires/hôtes pour veiller à ce que les ressources sécuritaires essentielles soient en place.

Complément d'information

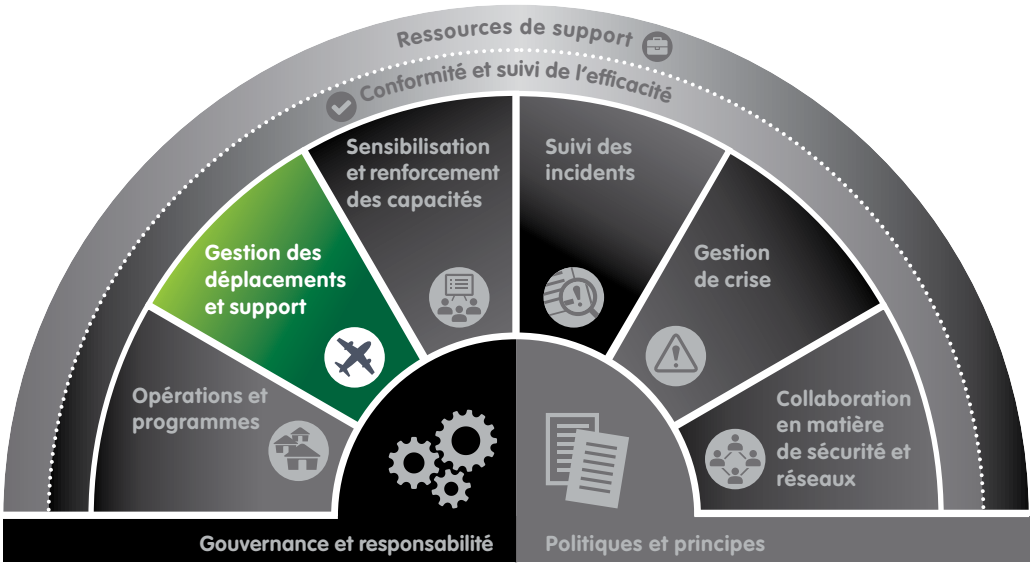
« The Security of Lone Aid Workers », Gonzalo de Palacios

Manuel de l'EISF « Office Opening: A guide for non-governmental organisations »

Document d'information de l'EISF « Security Management and Capacity Development: International agencies working with local partners »

« Humanitarian Safety and Security: Obligations and responsibilities towards local implementing partners », Christopher Finucane

6 Gestion des déplacements et support



Une grande partie du personnel d'ONG est obligée de voyager. Que ce soit pour visiter un programme ou assister à une réunion ou à un quelconque événement, le personnel se rend régulièrement dans des régions du monde qui présentent des risques dont ils n'ont pas forcément conscience, ou des niveaux plus élevés de risque inhérent. Chaque fois que le personnel quitte son cadre de travail habituel, il s'expose souvent à un risque accru en matière de sécurité, ou de santé, et les responsabilités concernant le « duty of care » de leur organisation sont également plus soutenues. Cela veut dire que la gestion du risque sécurité doit être un élément clé de la stratégie globale de chaque organisation relative à la gestion des déplacements.

La gestion efficace des risques de sécurité lors des déplacements est un processus permanent qui démarre avant le départ, se poursuit pendant toute la durée du séjour et même après le retour.

Les risques lors des déplacements peuvent être exacerbés dans les pays où il n'existe guère de présence organisationnelle voire aucune. Le manque de connaissances contextuelles et d'informations actualisées sur les menaces actuelles, associé à l'absence de plans sécurité ou de réseaux, augmentent le risque auquel s'expose le personnel lors de ses déplacements.

Lors de la planification d'un déplacement, il est essentiel que le personnel et les visiteurs aient pleinement conscience des risques auxquels ils pourraient être confrontés et qu'ils aient été correctement informés. Non seulement les mesures de sécurité appropriées devront être en place avant le départ, mais un soutien adapté (y compris des briefings sécurité, un logement sécurisé, un transport sûr, des soins médicaux adaptés, etc.) devra être à leur disposition dès leur arrivée, tant qu'ils se trouvent dans le pays, et à leur retour.

Identifier les risques associés aux déplacements

Bien évidemment, le niveau et le type de risque auxquels s'expose le voyageur varieront selon la destination, la nature du déplacement et son profil personnel. Toutes les destinations et tous les types de déplacements n'exigent pas les mêmes mesures de sécurité. Si le cadre de gestion du risque sécurité de votre organisation n'est pas suffisamment souple pour tenir compte des différents risques associés à différents lieux, les procédures et mesures existantes risquent d'être fastidieuses ou inefficaces, ou de gêner les opérations, et le personnel pourrait ne pas vouloir les respecter.

Accéder à un système actualisé d'évaluation des risques pays permettra à votre organisation, et à chaque membre de votre personnel, de connaître rapidement le niveau de risque global d'un pays ou d'un lieu particulier. Vous pourrez alors préciser quelles mesures de sécurité sont requises avant tout déplacement, et quel niveau d'autorisation est approprié, conformément à la politique sécurité de l'organisation ou à ses procédures de sécurité lors des déplacements.

Si certaines organisations plus importantes sont à même d'effectuer leurs propres évaluations des risques pays, cela exige des capacités significatives, notamment pour obtenir les informations nécessaires afin de rester à jour. Il sera peut-être plus intéressant pour votre organisation de faire appel aux évaluations des risques de prestataires externes, par exemple une entreprise associée à votre agent de voyage ou service de réservation, le cas échéant. Par ailleurs, les sites des ambassades tels que les « Conseils aux voyageurs » ou d'autres prestataires Internet proposent en open source des informations sur les risques lors des déplacements.

▶ *Voir « Informations sécurité et analyse » dans la section ci-après*

Exemple d'évaluation du risque pays

Les évaluations des risques propres à un pays ou à une région s'appuient généralement sur une catégorisation à quatre ou cinq niveaux. Il s'agit là d'évaluer plusieurs types de risques, y compris le risque de conflit, de troubles politiques/civils, de terrorisme, de criminalité, sanitaire et lié aux infrastructures. L'exemple ci-dessous présente certains des grands indicateurs employés.

Faible	Le pays ou la région offre globalement un bon niveau de sécurité et les autorités veillent à garantir une sécurité adéquate. Les taux de criminalité violente sont faibles, et les élections ou d'autres grands événements donnent lieu à un certain niveau de violence politique ou de troubles civils. Les actes terroristes y sont rares. Les risques de catastrophes naturelles sont faibles et les dangers sanitaires sont globalement évitables. Le personnel devra prendre des précautions élémentaires en matière de sécurité, de déplacements et de santé.
Moyen	Ce pays ou cette région connaît périodiquement des troubles politiques ou des manifestations violentes. Des groupes antigouvernementaux, d'insurgés ou extrémistes y sont actifs, et commettent des actes terroristes de manière intermittente. Le personnel risque de faire l'objet d'une criminalité ordinaire et violente. Les modes de transport et de communications ne sont pas fiables et les bilans de sécurité sont mauvais. Ce pays est susceptible de connaître des catastrophes naturelles ou des épidémies. Une vigilance et des procédures de sécurité générales accrues seront requises.
Élevé	Ce pays ou cette région connaît régulièrement des périodes de troubles politiques ou de manifestations violentes, qui peuvent cibler ou perturber les étrangers. Les groupes antigouvernementaux, d'insurgés ou extrémistes sont très actifs et menacent la stabilité politique et/ou économique du pays. Les taux de criminalité violente y sont élevés et il est fréquent que les étrangers soient ciblés. L'infrastructure et les services d'urgence sont de mauvaise qualité et les services de transport et de communications peuvent être régulièrement perturbés. Certaines zones sont inaccessibles ou interdites d'accès aux étrangers. Les agences d'aide peuvent faire l'objet de menaces ou de mesures de harcèlement de la part des autorités, de l'armée ou d'acteurs armés non étatiques. Ce pays ou cette région est en proie à une catastrophe naturelle, ou les épidémies représentent un risque élevé. Le personnel s'y expose à un risque durable, et un niveau élevé de vigilance, ainsi que des précautions sécuritaires efficaces et spécifiques au pays sont requis.
Extrêmement élevé	Ce pays ou cette région est en proie à un conflit actif ou à des troubles civils violents de longue durée. Le risque d'être pris dans un incident violent ou une attaque est élevé. Le gouvernement est susceptible d'avoir perdu le contrôle de zones importantes du pays, et il n'y a plus d'ordre civil. Il est difficile d'établir une distinction entre la criminalité et la violence politique et insurrectionnelle. Il est probable que les étrangers n'aient pas accès à de grandes zones du pays. Le transport et les communications sont en très mauvais état voire inexistants. Ce niveau de violence représente une menace directe pour la sécurité du personnel. Des précautions sécuritaires strictes sont essentielles mais peuvent ne pas suffire à empêcher des incidents graves. Les activités des programmes ou les déplacements peuvent être suspendus, ou le personnel peut devoir se retirer dans des délais extrêmement courts.

Il faut réaliser une évaluation des risques associés aux déplacements pour le personnel se rendant dans des destinations à haut risque, ou si la nature de la visite fait peser des risques sécurité. Faites clairement savoir au personnel qu'une telle évaluation est requise et informez-le des personnes chargées d'approuver l'évaluation et d'autoriser ce déplacement. Le formulaire d'évaluation des risques lors des déplacements devra faire apparaître la destination, l'itinéraire et les coordonnées et expériences du membre du personnel concerné. En outre, il devra évaluer le contexte global et les principaux risques de sécurité sur les différents lieux où le personnel devra se rendre, ainsi que les dispositions spécifiques en place pour gérer ces risques.

Complément d'information

Exemple de formulaire d'évaluation des risques lors des déplacements

Procédures de sécurité lors des déplacements

Un grand nombre de petites ONG ne disposent pas de bureaux pays permanents, mais leur personnel se déplace beaucoup. Pour ces organisations, les procédures de sécurité lors des déplacements doivent être une priorité. Ces procédures présentent la stratégie de votre organisation en matière de gestion des risques pour le personnel (et d'autres entités) lors d'un déplacement effectué pour le compte de l'organisation. Tandis que les plans sécurité mettent essentiellement l'accent sur les lieux où votre organisation est présente ou souvent active, les procédures de sécurité lors des déplacements doivent couvrir tous les lieux vers lesquels votre personnel se rend, y compris les endroits où votre organisation n'a qu'une présence limitée voire inexistante, et y compris les zones dans lesquelles vous collaborez avec, ou êtes accueillis par, une organisation partenaire locale. Ces procédures doivent aussi inclure les mesures prévues pour tenir un registre dans les pays à moindre risque des lieux où se trouve le personnel et où des événements susceptibles de faire de nombreuses victimes risquent de se produire, tels que les capitales européennes.

Le personnel est plus susceptible de respecter les procédures relatives aux déplacements s'il a lui-même participé à leur élaboration et s'il comprend leur raison d'être.

Il se peut que des procédures de sécurité lors des déplacements existent déjà dans le cadre de la politique plus générale de votre organisation régissant les déplacements. Si ce n'est pas le cas, ces procédures devront être clairement présentées dans un document dédié ; il faudra y aborder les

différents types de déplacements du personnel et d'autres parties prenantes, et fournir des détails sur les mesures de sécurité et les obligations des voyageurs avant, pendant et après leur déplacement. Il est possible que les gouvernements aident à évacuer leurs ressortissants en cas de troubles politiques ou sécuritaires, mais cela n'est pas garanti et peut changer d'un pays à un autre. Tout dépendra de la nationalité de l'individu et non du pays où se trouve le siège de l'organisation. Avant qu'un incident ne se produise, veillez à vérifier la manière dont les gouvernements de votre personnel répondraient en cas de crise.

Procédures de sécurité lors des déplacements

Ce document doit comprendre les éléments suivants :

- **Introduction** – présente les personnes visées par ces procédures. Souligner les éventuelles différences en matière d'exigences ou de soutien fourni au personnel, aux consultants, aux partenaires et aux visiteurs officiels.
- **Échelle des déplacements à risques** – présente le système d'évaluation des risques pays ou de déplacement employé, la manière dont le personnel peut accéder à l'information, les différents indicateurs et catégories employés et leurs implications.
- **Rôles et responsabilités** – présente les responsabilités des voyageurs, leurs supérieurs hiérarchiques ou points de contact, et le membre de la direction générale chargé de ces risques, ainsi que les différences lorsqu'il s'agit d'une destination à plus haut risque.
- **Autorisation de déplacement** – précise qui dans l'organisation autorise le déplacement, les différentes mesures de conformité requises, et les différences lorsqu'il s'agit d'une destination à plus haut risque.
- **Évaluation des risques lors des déplacements** – présente les cas de figure où une évaluation doit être faite, le modèle à employer et la personne chargée d'approuver l'évaluation une fois celle-ci complétée.
- **Informations et consignes avant le déplacement** – présente l'information qui doit être fournie à tous les voyageurs avant leur départ, le type de consignes à leur donner et par qui, et la façon dont ces exigences évoluent lorsque le risque augmente.
- **Formation sécurité** – détermine si une formation sécurité est requise avant un déplacement et quel cursus suivre. Cela dépendra du niveau de risque du pays. Inclure des informations sur un éventuel système de dérogation à une formation, et le nom de la personne qui peut délivrer cette dérogation. Il est toutefois important de noter qu'au titre du « duty of care », toute dérogation devra être justifiée.
- **Formulaires de profil du personnel/du voyageur** – le personnel, et toutes les personnes qui voyagent pour le compte de l'organisation,

doivent compléter un formulaire de profil faisant apparaître des détails personnels (nom, nationalité, religion, langues parlées, signes distinctifs, etc.), les personnes à contacter en cas d'urgence (parents proches ou toute autre personne), des données médicales (problèmes de santé préexistants, traitements réguliers, groupe sanguin, coordonnées du médecin traitant, etc.), des informations sur la présence de cette personne sur les réseaux sociaux (principales plateformes utilisées, en cas d'incident critique) et les questions servant de preuve de vie (s'il existe un risque d'enlèvement ou de kidnapping). Les formulaires de profil doivent être faciles d'accès en dehors des heures ouvrées.

- **Protocole de suivi** – indique la personne avec laquelle le voyageur doit rester en contact lors de son déplacement et à quelle fréquence, ainsi que le processus de remontée si le contact est perdu. La fréquence de ces contrôles dépendra du risque que présente la destination.
- **Procédures d'urgence** – présente les procédures d'urgence de l'organisation en cas d'urgences sécuritaires et médicales, y compris qui contacter et comment.

Les procédures de sécurité lors des déplacements doivent aussi indiquer ce qui doit se produire lorsqu'un membre du personnel ajoute un déplacement à titre personnel à son déplacement professionnel – assurance, nécessité de confirmer sa présence, temps de déplacement réels, etc.

« Les informations clés sur le personnel en déplacement, telles que la compagnie d'assurance médicale, doivent aussi être fournies, si possible, à l'organisation hôte dans le pays. En effet, en cas d'urgence, le fait de ne pas pouvoir accéder rapidement à cette information si elle se trouve dans les dossiers du siège pourrait avoir un impact considérable sur les conséquences de l'incident. »

Directeur sécurité d'une ONG

Informations sécurité et analyse

L'ensemble du personnel et des personnes en déplacement pour le compte de l'organisation doit avoir accès à des informations et conseils détaillés et actualisés sur les risques sanitaires et de sécurité associés à la destination, et ce, avant leur départ. Pour les ONG qui n'ont qu'une faible présence dans le pays, voire aucune, des informations sont disponibles sur les différents sites de conseils aux voyageurs gouvernementaux et des sources d'actualités

en open source et autres sites de voyages ; cependant, une bonne analyse exigera des ressources importantes en termes de temps et d'efforts. Même une fois cette démarche accomplie, les informations disponibles ne refléteront pas toujours les événements actuels ou la situation sur le terrain, et les conseils s'adressent souvent aux individus qui se rendent dans ces pays pour y faire des affaires ou du tourisme, et non dans le cadre d'une ONG.

De nombreuses organisations font appel à des services externes d'informations sécurité/voyages, soit par le biais de leur assurance voyage (service gratuit ou payant), soit directement auprès de prestataires spécifiques. La plupart des prestataires externes proposent des informations détaillées sur les pays et les villes ainsi que des rapports sur des plateformes en ligne interactives, et comprennent des informations et conseils sur les événements importants qui ont des répercussions sur la sécurité personnelle ou pourraient entraîner des perturbations dans les transports. Cependant, la qualité et l'exhaustivité des informations fournies par les différents prestataires peuvent varier de façon significative, et, pour avoir une analyse plus approfondie, il faut souvent s'adresser à des services premium. Si votre organisation cherche à faire appel à des services externes d'information sur la sécurité, nous vous conseillons de tester plusieurs plateformes en ligne et différents services avant d'en choisir un et de décider d'acheter des services payants. Envisagez d'adhérer à des initiatives sans but lucratif telles que la base de données Aid Worker Security Database gérée par Humanitarian Outcomes ou le projet Aid in Danger d'Insecurity Insight, dont l'objectif est de recueillir et diffuser l'information sur les incidents de sécurité subis par les organisations d'aide. Les organes de coordination de la sécurité des ONG (p. ex. EISF, INSO, etc.) peuvent aussi aider les organisations à accéder à des informations spécifiques aux ONG.

Sélectionner un prestataire d'informations externe

Si vous envisagez de faire appel à des services externes d'information sur la sécurité, prenez garde aux points suivants :

- **Assurance** – identifiez les services d'information et de support sécurité dont votre personnel peut déjà bénéficier par le biais de la police d'assurance actuelle de votre organisation.
- **Services** – déterminez quels services d'information et de support sécurité sont proposés par chaque prestataire et demandez-vous s'ils répondent à votre profil de risque et à vos besoins.
- **Réputation et expérience** – entretenez-vous avec d'autres organisations pour savoir si ces prestataires ont effectivement l'expérience et la crédibilité dont vous avez besoin en matière d'analyse et d'informations/conseils fournis.

- **Coûts** – recherchez un prestataire offrant le meilleur rapport qualité/prix en termes de gamme et de qualité de services.
- **Prestataires multiples** – déterminez s'il vaut mieux centraliser les services auprès d'un prestataire unique, utiliser les services existants en plus d'en acheter d'autres, ou opter pour des services spécifiques localisés dans le pays. Cependant, le fait d'utiliser de multiples prestataires pour accéder à différentes informations peut être complexe et entraîner une sous-utilisation de certains services.
- **Plateformes en ligne et applications** – vérifiez l'accessibilité de ces services, le personnel étant davantage susceptible d'utiliser un service facilement accessible depuis une application ou un site Internet déjà utilisé par les voyageurs, par exemple des sites de réservation de voyages en ligne.

Les voyageurs et le personnel doivent être informés le plus rapidement possible des incidents et événements qui se produisent dans le pays et peuvent avoir une incidence sur leur sécurité. La plupart des prestataires d'informations sur la sécurité/les voyages ont un service d'alerte par courriel ou SMS et de conseils en cas de problème. Certains de ces services d'alerte sont compris dans le forfait standard, mais d'autres sont facturés en plus. Pour recevoir ces alertes directement, le personnel doit s'être inscrit et avoir choisi de recevoir des alertes sur un ou plusieurs pays, ou veiller à ce que ses projets de déplacement soient liés au service par le biais d'un agent de voyage.

Certains prestataires ont mis au point des applications pour faciliter l'accès à leurs services d'information et envoyer des alertes de sécurité sur le téléphone des voyageurs. Pour certains prestataires, ce service est compris dans le forfait standard, et pour d'autres, il est facturé en sus. Il est important de noter que ces services ne s'adressent pas forcément au personnel d'ONG. Les avis et conseils fournis par ces prestataires devront être validés par l'organisation et, si nécessaire, des conseils supplémentaires devront être communiqués au personnel.

Briefings sécurité

Les membres du personnel et les visiteurs qui s'apprêtent à partir en déplacement doivent recevoir des briefings sécurité spécifiques au pays ou à la région avant leur départ, ainsi qu'à leur arrivée ; ces consignes leur seront communiquées soit par l'organisation elle-même si elle dispose d'une présence dans le pays, soit par une organisation partenaire.

Il peut être irréaliste de s'attendre à ce que votre organisation fournisse à l'ensemble du personnel et des visiteurs en déplacement un briefing sécurité en face à face. Il est donc important de lier les exigences en matière de briefing à un système d'évaluation du risque de déplacement/pays afin de s'assurer que les individus qui se rendent dans des endroits à plus haut risque reçoivent toujours des consignes détaillées. Néanmoins, tous les voyageurs doivent au moins recevoir des informations sur les principaux dangers ainsi que sur les précautions à prendre pour les éviter.

Aide-mémoire – briefings sécurité

- **Situation actuelle** – présenter la situation sécuritaire actuelle, y compris les principaux acteurs et groupes, les causes des troubles/conflits, l'état de l'ordre public, les niveaux de criminalité et les zones concernées.
- **Risques de sécurité** – mettre en évidence les principales menaces sécuritaires susceptibles d'affecter le personnel, les incidents récents et ce que le personnel doit faire pour y répondre. Par ailleurs, mettre en évidence les préoccupations ou risques relatifs à la sécurité de membres du personnel du fait de leur nationalité, de leur ethnicité, de leur identité de genre, de leur orientation sexuelle ou de leur handicap.
- **Santé et climat** – mettre en évidence les principaux risques naturels et sanitaires dans le pays ou certaines régions, les précautions de base que le personnel doit prendre et la réponse à apporter en cas de préoccupations sanitaires ou d'urgences médicales.
- **Comportement personnel** – mettre en évidence toutes les législations locales importantes, les normes et coutumes culturelles et le type de comportement attendu de la part du personnel.
- **Voyages et déplacements** – expliquer quels papiers d'identité et autres documents de voyage sont nécessaires pour pouvoir se déplacer dans le pays ou dans certaines régions, le processus d'autorisation et les éventuelles restrictions (par exemple couvre-feux, zones interdites).
- **Communications** – présenter les systèmes utilisés pour garder le contact avec le personnel et ce qui se passe si la personne ne se met pas en contact comme convenu, ainsi que les éventuelles préoccupations ou restrictions relatives aux communications.
- **Logement** – présenter le logement et les principales mesures de sécurité en vigueur.
- **Principaux interlocuteurs** – fournir au personnel les coordonnées essentielles, et s'assurer qu'il comprenne comment et à qui signaler des incidents ou des problèmes.

Les personnes qui se déplacent souvent n'ont pas besoin de ces consignes ; à noter toutefois que malgré leur expérience, elles sont susceptibles de s'exposer à un plus grand risque car elles pourraient ne pas remarquer immédiatement des changements.

Les consignes de sécurité contextuelles devraient servir à fournir au personnel en déplacement des informations et des conseils actualisés sur les risques sanitaires et de sécurité, pour qu'il comprenne suffisamment bien la situation locale afin d'y opérer de manière aussi sécurisée que possible.

Complément d'information

Document d'information de l'EISF « Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management »

Suivi des déplacements

Vous devez être en mesure de rester en contact avec le personnel et toute personne en déplacement pour le compte de votre organisation, et suivre leurs mouvements. La fréquence des prises de contact dépendra du niveau de risque du lieu en question. Dans la plupart des cas, il s'agira tout simplement d'un rapide coup de téléphone ou d'un texto envoyé à un interlocuteur prédéfini. Convenez d'un calendrier simple indiquant les moments où le personnel devra se mettre en contact, et auprès de qui, même s'il n'a rien à signaler. Il faut au minimum que l'organisation sache : que l'individu est bien arrivé ; si son itinéraire a été modifié ; quand il doit partir ; et qu'il est bien rentré.

Le personnel doit être conscient des conséquences qui découleront d'une prise de contact manquée, autrement dit du processus de remontée. Cette remontée doit être menée de manière cohérente à travers l'organisation, faute de quoi le système de suivi n'aurait plus de sens.

Si un incident de sécurité ou un événement majeur se produit dans le pays où se trouvent des membres du personnel, votre organisation doit être capable de localiser rapidement tout le personnel et de savoir s'il risque d'être impacté. Il existe aujourd'hui des solutions high-tech de suivi des déplacements, de nombreux systèmes étant capables de localiser précisément les individus grâce à leur téléphone satellitaire/portable/GPS. Certains employés peuvent se montrer réticents à l'idée d'être suivis d'aussi près et ces solutions high-tech ne sont généralement envisagées que dans des contextes de risque extrême. Il existe une solution de suivi des déplacements plus généralisée, qui conviendrait aux petites ONG, et qui

consiste à suivre la localisation générale des voyageurs d'après leur billet d'avion. De nombreuses agences de voyage et prestataires d'assistance sécurité offrent des services de suivi des déplacements ; les services de base peuvent être gratuits, mais les solutions les plus complètes auront un coût.

« Si vous donnez un numéro d'urgence à un employé, il faut être sûr de pouvoir y répondre rapidement 24 heures sur 24 et 365 jours par an. Il est inacceptable de rappeler au bout de deux heures en disant : 'Désolé, mais aujourd'hui c'est samedi.' »

Travailleur humanitaire d'une ONG

Assurance

Selon l'ONG, la gestion des polices d'assurance incombe à différents rôles et elle pourrait ne pas être considérée aussi importante qu'elle l'est. Les choix sont innombrables. Il serait dangereux de choisir une police uniquement pour son prix. Par exemple, les polices bon marché limitent souvent leur couverture et peuvent exclure les conflits, les troubles et les actes de terrorisme, et/ou certaines destinations. Elles limitent souvent les lieux en fonction des « Conseils aux voyageurs » établis par le gouvernement d'origine. Il vous faudra donc contracter des extensions spécifiques pour vous assurer que le personnel est entièrement couvert.

Lors de l'achat d'une police d'assurance, veillez à ce qu'elle soit adaptée à votre profil de risque et de déplacement, à ce que les pays et régions dans lesquels votre personnel pourrait se rendre ne soient pas exclus, et à ce que le personnel et toute personne se déplaçant pour le compte de votre organisation dispose au moins d'une assistance médicale. Traiter et rapatrier un employé, un consultant ou un visiteur gravement blessé et non assuré est extrêmement onéreux. De nombreuses compagnies d'assurance offrent aussi des formations ou un accès à d'autres services de gestion du risque susceptibles de réduire vos risques organisationnels ; demandez donc à votre assureur quels services et support il peut vous proposer.

Certes, une police d'assurance est coûteuse, mais ce coût porte essentiellement sur des éléments non négociables pour le type de travail entrepris par les ONG.

Par conséquent, le fait d'ajouter des services facultatifs, tels que des services et alertes relatifs aux transports, un soutien en cas d'évacuation sécuritaire ou de crise, pourrait ne pas coûter bien plus à l'organisation, mais conférer des avantages substantiels en termes de gestion des risques de sécurité, surtout pour les petites ONG dont les capacités et les ressources dans le pays sont limitées.

Les détails de la police d'assurance des personnes en déplacement doivent dans la mesure du possible être communiqués à l'organisation hôte dans le pays, y compris lors de visites dans vos propres bureaux, l'assurance voyage pouvant avoir été contractée auprès d'un assureur différent de celui du personnel basé dans le pays.

Types d'assurance

- **Déplacements internationaux et accident/maladie** – assurance pour professionnels couvrant, lors des déplacements, les accidents et la maladie, y compris l'évacuation sanitaire et le rapatriement, pour les individus assurés (personnel et parties associées) en déplacement pour le compte de l'organisation. A moins que la police n'inclue une couverture « Risque de guerre », de nombreux produits excluent certaines menaces et destinations à haut risque (en s'appuyant sur les conseils aux voyageurs du gouvernement ou sur une liste publiée par l'assureur), par conséquent le fait de couvrir ces lieux et risques nécessitera de contracter des produits d'assurance supplémentaires.
- **Assurance santé internationale** – assurance santé et évacuation sanitaire/rapatriement pour le personnel international (et les personnes à charge) basé à l'étranger. Lorsque le personnel se rend en dehors du pays dans lequel il est basé, il est normalement couvert par l'assurance voyage de l'organisation.
- **Plans nationaux d'assurance santé** – plans d'assistance santé locaux/régionaux. Les produits proposés et leur portée peuvent varier, mais la plupart fournissent un remboursement des frais médicaux encourus par le personnel recruté dans le pays. Si l'évacuation sanitaire est incluse, elle tend à se limiter à une évacuation à l'intérieur même du pays.
- **Réponse d'urgence et assurance évacuation** – soutien et évacuation non sanitaires du fait de troubles politiques, d'un conflit ou d'une catastrophe naturelle. Cette couverture peut être incluse dans votre assurance voyage ou achetée en plus.
- **Assurance risques spéciaux** – couverture enlèvement, rançon et extorsion (ou couverture gestion de crise), qui rembourse les frais encourus par une organisation suite à un incident spécifique. Cette assurance comprend également l'accès à des consultants spécialisés dans le type d'intervention en question et qui sauront conseiller et soutenir l'organisation.

Complément d'information

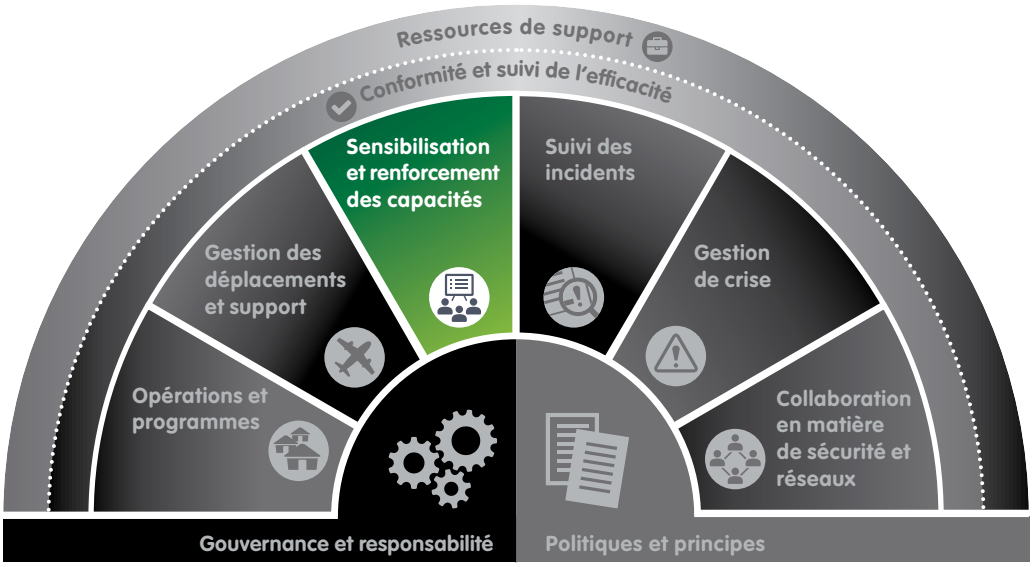
« Guide to selecting appropriate Crisis Management Insurance », Harry Linnell

« Module 11: Medical support and evacuation », dans le manuel de l'EISF « Security to go »

« Annex 5: Insurance », guide ODI « GPR 8 - Operational Security Management in Violent Environments »

Document d'information de l'EISF « Engaging Private Security Providers: A Guideline for Non- Governmental Organisations »

7 Sensibilisation et renforcement des capacités



La mise à disposition d'une formation sécurité adaptée à votre personnel, et pertinente au vu de son rôle et de son environnement de travail, ainsi que de conseils et d'un soutien permanents, fait partie intégrante du travail de sensibilisation de votre personnel à la sécurité et d'amélioration de la culture de sécurité de votre organisation.

L'ensemble du personnel doit disposer des connaissances et compétences nécessaires en matière de sécurité pour pouvoir gérer sa propre sécurité ainsi que celle de ses collègues..

Initiations à la sécurité

Votre personnel doit être correctement informé des politiques et stratégies de votre organisation en matière de sécurité, et être préparé aux risques et défis auxquels il pourrait faire face dans le cadre de son travail.

Pour cela, il est primordial que tous les nouveaux membres du personnel reçoivent une initiation, ou formation de base, à la sécurité peu après leur arrivée au sein de votre organisation. Dans l'idéal, cette formation sera incluse dans le processus d'orientation plus général prévu par le service RH, et elle leur donnera une idée de la culture, des politiques et des stratégies sécurité de l'organisation ; il s'agira aussi de présenter leurs rôles et responsabilités spécifiques dans ce domaine.

Aide-mémoire – initiation à la sécurité

- **Stratégie sécurité** – expliquez l'approche adoptée par l'organisation à l'égard de la sécurité, son profil de risque et son attitude globale face au risque.
- **Politique** – présentez la politique sécurité, les principes clés et les exigences minimales de sécurité de l'organisation, et la manière dont ceux-ci s'appliquent à différentes situations.
- **Structure de gestion du risque sécurité** – expliquez les rôles et responsabilités à l'égard de la sécurité au sein de l'organisation.
- **Responsabilité individuelle** – soulignez le fait que chaque individu est responsable de sa propre sécurité et de celle de ses collègues, et expliquez l'importance du consentement éclairé et de son droit à dire « non » s'il estime qu'une situation pourrait être dangereuse.
- **Sécurité lors des déplacements** – abordez les dispositions sécuritaires en vigueur pour le personnel en déplacement. Présentez les procédures de sécurité lors des déplacements et expliquez les exigences en vigueur en matière d'autorisation, d'informations, de formation et de suivi des déplacements.
- **Procédures d'urgence** – expliquez les procédures d'urgence de l'organisation. Informez le personnel du prestataire d'assistance médicale qui leur est attribué et de la manière de le contacter.
- **Signalement des incidents** – expliquez quels incidents de sécurité doivent être signalés et quelles procédures s'appliquent.
- **Ressources supplémentaires** – familiarisez le personnel aux ressources sécurité supplémentaires, tels que les manuels, les guides et les documents de formation.

Formations sécurité

La formation est essentielle pour améliorer la sensibilisation et les capacités de gestion du personnel. De nombreuses ONG comprennent l'importance d'une formation sécurité ; cependant, les coûts et la disponibilité sont des obstacles significatifs. Les petites ONG, en particulier, peuvent avoir du mal à

trouver les ressources nécessaires ou à justifier une telle dépense. Toutefois, grâce au développement des outils de sécurité et d'apprentissage en ligne, les organisations ont désormais le choix entre différentes options pour améliorer la sensibilisation à la sécurité et les capacités de leur personnel.

Les dépenses associées à la formation sécurité devront être prises en compte lors de l'élaboration des propositions et budgets destinés à vos projets. Ces coûts peuvent varier considérablement selon le prestataire, le lieu et le type de formation requis.

Types de formation sécurité

Il existe quatre grandes catégories de formations sécurité :

- **Sensibilisation à la sécurité du personnel** – s'adresse aux individus qui travaillent dans un environnement au risque modéré ou qui y effectuent des déplacements pour le travail. Il s'agit de sensibiliser l'employé à un niveau individuel quant aux risques de sécurité et à la démarche à suivre pour les réduire et y répondre.
- **Formation préparatoire à une mission en milieu hostile** – s'adresse aux individus qui se rendent dans un environnement à haut risque ou y sont basés. Il s'agit d'une formation sécurité personnelle axée spécifiquement sur les dangers, qui comprend des exercices de simulation.
- **Gestion du risque sécurité** – s'adresse aux individus ayant des responsabilités en matière de gestion du risque sécurité (points focaux sécurité, responsables de programmes et membres de l'équipe de direction). Il s'agit de présenter les principaux concepts de la gestion du risque sécurité et de contribuer à développer des compétences en évaluation du risque sécurité, en gestion du risque de sécurité opérationnel et en gestion des incidents critiques.
- **Gestion de crise** – s'adresse aux membres des équipes de direction ou de gestion de crise (au niveau du siège et du pays). Il s'agit de faire connaître les principes et actions entrant en jeu lors d'un incident critique ou d'une situation de crise, sous la forme d'exercices en direct et sur ordinateur et/ou d'ateliers.

Avant d'entreprendre une formation sécurité, décidez de ce dont votre personnel a besoin, en fonction du lieu où il réside et de l'endroit où il doit se rendre, de ses rôles et responsabilités, du profil de risque et du travail qu'effectue votre organisation. Par exemple, il ne servirait à rien de faire suivre une formation coûteuse de quatre jours sur les missions en milieu hostile à des employés qui se rendent essentiellement dans des pays à risque modéré pour de courtes durées, qui sont principalement basés dans les capitales, et qui passent la majeure partie de leur temps dans des réunions ou dans un hôtel.

Pour réaliser une analyse basique des besoins en formation, tenez compte des points suivants :

- Des compétences et connaissances requises en matière de sécurité pour certains rôles et activités spécifiques au sein de votre organisation ;
- Du niveau d'expérience en la matière ainsi que des formations que le personnel existant a déjà suivies ;
- Du nombre d'employés ayant besoin d'un type de formation sécurité spécifique ;
- De la répartition géographique du personnel, et des lieux où la formation sécurité devra être dispensée pour attendre un maximum d'employés au moindre coût ;
- Du budget disponible et du coût des différentes options de formation.

Lorsque vous avez identifié et priorisé les exigences de formation de votre organisation, cherchez à les rapprocher des ressources et des options disponibles, lesquelles varieront d'un pays à un autre. Parmi les ressources potentielles, citons les suivantes :

- **Formations en ligne.** Plusieurs organisations proposent des formations sécurité en ligne gratuites qui confèrent des ressources utiles et rentables en matière de sécurité. Si les formations en ligne n'offrent pas les mêmes avantages que les formations en face à face, elles constituent une introduction complète à la sécurité et sont faciles à déployer en tant que formation obligatoire pour votre personnel.

Formations sécurité en ligne

Voici quelques-unes des formations en ligne gratuites disponibles (chacune nécessite une inscription individuelle) :

• **DisasterReady.org** – plateforme de formation en ligne gratuite s'adressant aux travailleurs humanitaires et proposant plusieurs formations sécurité (dont les formations sécurité Save the Children et RedR).

• **Kayaconnect.org** – plateforme de formation de la Humanitarian Leadership Academy, qui propose plusieurs formations sécurité en ligne gratuites (y compris les formations sécurité du HCR et de Save the Children).

• **Plateforme d'apprentissage de la FICR** – donne accès aux formations en ligne de la FICR *Stay Safe - Personal Security* et *Stay Safe - Security Management* (cours en ligne).

• **Formation UNDSS** – donne accès aux formations en ligne de l'ONU *Basic Security in the Field* et *Advanced Security in the Field* (cours en ligne).

- **Formations ouvertes.** Plusieurs prestataires de formations externes organisent régulièrement des formations ouvertes en Europe et dans des plateformes régionales, qui tendent à être moins coûteuses que les formations sur mesure (mais votre personnel devra se rendre sur le lieu de formation). Pour les organisations aux ressources limitées, les formations ouvertes peuvent être une option intéressante, étant donné que le développement et la pérennisation d'une formation sécurité interne exige des capacités significatives.
- **Formations sur mesure.** De plus en plus de prestataires externes et de formateurs individuels offrent un large éventail de formations et de services sur mesure axés sur la sécurité. Un grand nombre d'entre eux sont en mesure d'organiser une formation à votre siège ou dans le bureau pays. Si ces formations sur mesure tendent à être plus coûteuses, il est probable qu'elles conviendront mieux à la stratégie sécurité spécifique de l'organisation et aux risques auxquels votre personnel doit faire face.
- **Formations inter-agences.** Dans certains pays, les organes de coordination inter-agences ou le Département de la sûreté et de la sécurité de l'ONU (UNDSS) – dans le cadre de l'initiative Saving Lives Together (SLT) – proposent au personnel d'ONG une formation sécurité. Si votre organisation compte du personnel basé dans différents pays, celui-ci pourra profiter de ces formations locales à un tarif réduit voire, dans certains cas, gratuitement.

▶ *Pour de plus amples renseignements sur Saving Lives Together, voir la section 10 : Collaboration en matière de sécurité et réseaux*

Assurez-vous que la formation externe que vous envisagez de faire suivre à vos employés est adaptée aux ONG. En effet, de nombreux prestataires s'adressent principalement à des voyageurs d'affaires, des journalistes ou des étudiants, et n'abordent donc pas les enjeux de sécurité spécifiques auxquels le personnel d'ONG doit faire face et les stratégies requises pour gérer ces risques.

Il est conseillé d'utiliser les mécanismes de coordination de la sécurité pour savoir quelles formations externes les autres ONG emploient. Le site Internet de l'EISF donne une liste de formations sécurité, qui n'apparaissent sur cette liste qu'une fois que le prestataire a reçu deux références positives et distinctes de la part d'organisations membres de l'EISF.

Sélectionner des prestataires de formation externes

Pour sélectionner un formateur externe, tenez compte des points suivants :

- **Profil** – ses valeurs, sa motivation, sa déontologie et sa culture correspondent-elles à celles de votre organisation et de votre personnel ?
- **Réputation et expérience** – peut-il vous fournir des références et des témoignages fiables ? Qui sont ses clients, actuels ou passés ? Dispose-t-il des capacités et de l'expérience requises pour délivrer des formations adaptées ?
- **Contenu** – quel est le contenu de la formation, son approche et sa méthodologie ? Cela correspond-il à votre profil de risque et à votre approche en matière de sécurité ? Cette formation implique-t-elle des exercices de simulation ? Quel type d'incidents et quel niveau d'agression seront employés lors de ces exercices ?
- **Coût** – Le coût comprend-il la préparation, le transport, la prestation et le travail effectué avant et après la formation ? Ce coût est-il raisonnable et comparable à celui d'autres prestataires au vu de la formation demandée ?
- **Formateurs** – Quelles compétences, connaissances et expérience les formateurs affichent-ils ? Quel est le degré de mixité des formateurs ? Pouvez-vous demander à avoir des formateurs spécifiques ?
- **Lieu et langue** – Où se déroulera la formation ? Votre personnel pourra-t-il s'y rendre sans gros problème ? Y a-t-il d'autres frais de transport à prévoir ? Dans quelle langue la formation sera-t-elle dispensée ? Le prestataire a-t-il des formateurs qui peuvent assurer la formation dans les langues dont votre organisation a besoin ?

Complément d'information

« NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs », EISF et InterAction

Document d'information de l'EISF « Engaging Private Security Providers: A Guideline for Non- Governmental Organisations »

Page du site de l'EISF consacrée aux formations et aux événements

8 Suivi des incidents

Il est primordial de signaler les incidents le plus vite possible afin de protéger les membres de votre personnel. Celui-ci pourra ainsi recevoir rapidement une aide, et l'incident et ses répercussions seront gérés de manière optimale. Un système de suivi des incidents de bonne qualité aidera leurs collègues à éviter des incidents similaires et à faire face aux changements qui s'opéreront dans l'environnement opérationnel. Il permettra également de mieux comprendre le contexte et appuiera le processus décisionnel relatif à la gestion des incidents.

Le fait de signaler et de suivre régulièrement les incidents permet aux organisations de savoir où et comment la situation sécuritaire évolue, les raisons de ce changement et les implications pour la sécurité du personnel.

Pour la plupart des petites ONG, il n'est guère rentable d'investir dans de vastes systèmes et logiciels de suivi des incidents car elles n'auront sans doute qu'un petit nombre d'incidents à gérer. Cependant, l'instauration

d'un système basique de signalement et d'enregistrement des incidents de sécurité est cruciale pour toutes les organisations, quelle qu'en soit la taille. Ce système devra se composer de deux grands éléments :

1. D'un processus permettant de signaler l'incident ou la situation ;
2. D'un système de gestion de l'information signalée.

Processus de signalement des incidents

Les processus de signalement des incidents doivent fournir des directives claires sur le type d'incidents à signaler, à qui, et selon quel mécanisme.

L'instauration d'un système de signalement des incidents dans une organisation n'est pas une tâche simple – il faut du temps et de la persévérance pour l'intégrer pleinement et pour que tous les incidents soient bien signalés. Le sous-signalement des incidents de sécurité étant un problème dans toutes les organisations, vous devrez communiquer clairement à votre personnel l'objectif, la raison d'être et les avantages à retirer de ces signalements. Pour instaurer un système de signalement efficace, il est essentiel que le personnel soit sensibilisé à la nécessité d'effectuer ces signalements, que la manière dont l'organisation gère l'information soit fiable, qu'un retour soit adressé au personnel lorsqu'il a signalé un incident, et que le mécanisme soit simple d'utilisation.

Quels événements signaler

Pour de nombreuses organisations, un incident de sécurité est : **une situation ou un événement qui porte ou pourrait porter atteinte aux membres du personnel, à des membres du personnel associés ou à des tiers, qui perturbe ou pourrait perturber grandement les programmes et les activités, ou provoquer des dommages substantiels ou des pertes importantes pour les biens de l'organisation ou sa réputation**.

Les « accidents évités de justesse » doivent eux aussi être signalés car ils pourraient éviter à d'autres d'être impliqués dans un incident et aider le personnel à savoir si le contexte sécuritaire évolue et de quelle manière.

S'il convient d'encourager le personnel à signaler tous les incidents, vous devrez clairement faire savoir ce qui constitue un incident à signaler. Les perceptions en la matière varient selon l'employé et le lieu, les normes étant différentes d'un contexte à un autre. Il ne fait pratiquement aucun doute que les incidents majeurs seront signalés, mais des incidents qui semblent isolés ou insignifiants risquent d'être ignorés ou négligés alors que, pris ensemble, ils peuvent signaler une évolution de la situation sécuritaire.

Les accidents évités de justesse doivent eux aussi être signalés. Il s'agit des

cas où un incident grave a été évité, par le pur fait du hasard ou parce qu'une réponse appropriée y a été apportée.

Tous les incidents graves doivent être pleinement examinés afin de comprendre les événements avant, pendant et après l'incident. Une enquête post-incident, si possible menée par un individu sans lien avec l'incident, devra tenir compte des causes et des motivations, des mesures et du comportement adoptés par le personnel et des réponses apportées à l'incident. Les enquêtes devront permettre d'identifier des recommandations clés ou des actions de suivi, voire des procédures disciplinaires, afin d'améliorer la gestion du risque sécurité de manière permanente.

Rapports d'incident

Au minimum, les rapports devront répondre à cinq questions : qui a fait quoi à qui, où et quand.

Il existe essentiellement trois types de rapports d'incidents :

- **Les rapports d'incidents immédiats** – envoyés dès que l'incident se produit ou le plus tôt possible (dès qu'il peut être signalé sans que cela présente un danger), normalement de manière verbale au téléphone ou par radio, en donnant un bref résumé de ce qui s'est passé et des actions/du support requis.
- **Les mises à jour** - envoyées aussi souvent que nécessaire afin de compléter l'information sur l'incident ou la situation.
- **Les rapports post-incident** – envoyés une fois que l' incident s'est stabilisé ou est terminé, en fournissant un rapport écrit de l'incident et des diverses mesures qui ont été prises.

Formulaires de rapports d'incidents

Un formulaire standard et simple d'emploi peut apporter de la clarté et de la cohérence au processus de signalement des incidents de votre organisation. Tous les incidents de sécurité impliquant directement votre personnel ou d'autres personnes qui travaillent pour le compte de votre organisation devront faire l'objet d'un rapport post-incident formel. Un rapport devra aussi être complété après un incident ayant entraîné des pertes ou des dommages considérables à un bien, ou des blessures ou des torts à un tiers.

Le rapport d'incident de sécurité devra donner un compte-rendu complet de l'incident et des différentes mesures qui ont été prises. Un modèle type devra être créé pour tous les rapports post-incident.

Certaines informations devront être traitées de manière confidentielle, telles que les états de santé, les agressions sexuelles, les noms des victimes, etc. Le personnel devra être informé de la démarche à suivre pour traiter les

informations sensibles afin de préserver la confidentialité. Il devra par exemple savoir qui est autorisé à accéder aux rapports d'incident, et à quels moments et de quelle manière l'accès aux rapports devra être limité.

Formulaire de rapport d'incident

Il doit faire apparaître les informations suivantes :

- **Type d'incident** – par exemple s'il s'agit d'un vol, d'un cambriolage ou d'un vol à main armée.
- **Lieu** – où l'incident s'est produit, en indiquant le lieu précis.
- **Date, jour et heure** – quand l'incident s'est produit, avec autant de précisions que possible.
- **Qui est impliqué** – qui a été affecté par l'incident, y compris poste, type of programme, nationalité, genre, etc., afin de mieux comprendre les vulnérabilités spécifiques.
- **Description de l'incident** –description détaillée de la nature des événements, de l'impact qu'ils ont eu sur les personnes affectées, détails de toute perte matérielle, etc.
- **Analyse de l'incident** – évaluation initiale de la personne qui aurait pu perpétrer l'incident, de ce qui aurait pu le provoquer, chercher à déterminer si l'organisation ou des membres du personnel étaient spécifiquement ciblés, et implications éventuelles pour la sécurité future du personnel.
- **Décisions immédiates et mesures prises** – informations sur les décisions et mesures prises, et par qui, immédiatement après l'incident.
- **Qui a été informé** – liste indiquant dans le détail les personnes auprès desquelles l'incident a été signalé au niveau local, par exemple autorités, autres agences humanitaires, bailleurs de fonds ou autres parties prenantes.
- **Mesures supplémentaires restant à prendre** – indiquer dans le détail les décisions et mesures qui doivent être prises en réponse à l'incident. Donner d'éventuelles recommandations afin d'améliorer la sécurité du personnel.

Complément d'information

Exemple de modèle de rapport d'incident

« Chapter 5: Incident reporting and critical incident management », dans le manuel d'ODI « GPR8 - Operational Security Management in Violent Environments »

« Guidance Tool F: Good practice in gender-sensitive incident reporting » dans le document d'information de l'EISF « Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management »

Enregistrement et analyse des incidents

Les enregistrements de tous les incidents de sécurité doivent être centralisés et analysés périodiquement. En plus de constituer un registre institutionnel de l'incident et de la réponse apportée par l'organisation en cas de litige ou de demandes de renseignements externes, le fait d'analyser cette information permettra à votre organisation de mieux comprendre les questions de sécurité affectant votre personnel. Une analyse régulière des rapports d'incidents de votre organisation peut servir à :

- Sensibiliser le personnel à la question de la sécurité et ainsi renforcer la culture de sécurité de l'organisation ;
- Sensibiliser les membres de la direction et du conseil d'administration au profil de risque de l'organisation, aux principaux dangers affectant le personnel et aux lacunes au niveau des procédures, du support et de la formation ;
- Fournir une analyse afin d'améliorer le processus décisionnel axé sur la conception et la mise en œuvre de programmes ;
- Négocier avec les assureurs. Ceux-ci s'appuient souvent sur des « statistiques globales » pour fixer leurs tarifs, mais si vous pouvez démontrer les risques spécifiques auxquels votre organisation s'expose et les mesures dont vous disposez pour les gérer, peut-être pourrez-vous les convaincre de réduire leurs tarifs, ou du moins de ne pas les augmenter.

Il existe plusieurs progiciels standard et outils logiciels en open source qui servent à enregistrer et analyser les données d'incidents, et de nombreuses organisations ont établi leur propre base de données exhaustive de signalement des incidents. Cependant, pour certaines ONG, cela peut sembler soit trop onéreux, soit trop compliqué à instaurer et à maintenir. De simples tableurs Excel, dans lesquels vous enregistrerez les principales informations tirées de différents rapports d'incidents, pourraient amplement suffire à votre organisation.

Il est conseillé de diffuser l'information entre différentes agences, si possible, afin que votre organisation comprenne mieux le contexte – par exemple, en accédant et en contribuant au projet Aid in Danger d'Insecurity Insight et à la base de données Aid Worker Security de Humanitarian Outcomes.

Complément d'information

« Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study », Gonzalo de Palacios, dans le document d'information de l'EISF « Communications Technology and Humanitarian Delivery »

Document d'information de l'EISF « Incident Statistics in Aid Worker Safety and Security Management »

« Managing security information - Simson software », Centre for Safety and Development

Projet Aid in Danger d'Insecurity Insight

Base de données Aid Worker Security de Humanitarian Outcomes

Incident Dashboard d'INSO

9 Gestion de crise

La mort, l'arrestation ou l'enlèvement d'un membre du personnel sont des épreuves extrêmement difficiles pour toute organisation. Non seulement celle-ci devra faire face à l'incident, gérer les relations avec les autorités et soutenir la famille et les collègues de la victime, mais il lui faudra aussi continuer à gérer ses activités et son personnel sur d'autres sites.

La résolution et la bonne gestion d'une situation de crise dépendent de la capacité de votre organisation à prendre des décisions rapidement, ce qui exige une préparation, une bonne circulation des informations et des voies de communication claires que l'ensemble du personnel comprend parfaitement.

La préparation est cruciale pour bien gérer un incident, surtout lorsqu'il faut apporter une réponse coordonnée, efficace et impliquant plusieurs lieux géographiques et différentes parties prenantes.

Instaurer une structure de gestion de crise

La majorité des incidents de sécurité sont traités dans le cadre de la hiérarchie normale de votre organisation. Cependant, dans certains cas exceptionnels, du fait de la nature et de la gravité de l'incident, ou de ses répercussions globales, votre organisation devra instaurer une structure dédiée pour y répondre. Ces cas sont généralement qualifiés de « crises ».

L'une des étapes essentielles pour planifier cette structure consiste à constituer une équipe pour coordonner et gérer la réponse de l'organisation. L'équipe de gestion de crise (EGC) instaurée au niveau d'une région ou du siège est un élément clé, même si la terminologie et la composition employées par différentes organisations, et ses responsabilités, varient énormément. Dans de nombreux cas, l'équipe se composera de membres clés de l'équipe dirigeante. Cependant, l'attribution des rôles au sein de l'EGC sera fonction de l'expérience, des capacités et des compétences de chaque individu, plutôt que du poste occupé.

Il est plus facile de démobiliser une EGC lorsqu'il devient évident que l'incident n'est pas aussi grave qu'on aurait pu le croire, que d'en mobiliser une lorsque l'incident a déjà progressé.

Veillez à instaurer une équipe de gestion de crise et une structure globale adaptées à votre organisation. Cependant, l'expérience a montré qu'il valait mieux disposer d'une EGC de petite taille basée au siège et d'une équipe de gestion de l'incident (EGI) basée le plus près possible du lieu où s'est produit l'incident, tout en restant en sécurité. L'autorité décisionnelle stratégique (ADS) se situe au sommet de la hiérarchie et en dehors de l'EGC. Envisagez d'inclure dans la structure de réponse à la gestion de crise le personnel auxiliaire, tel que les soutiens familiaux, un porte-parole pour les médias et des membres du personnel de la logistique, mais pas dans l'EGC. Il est bon d'identifier des individus alternatifs pour chacun des principaux rôles afin d'assurer une prise en charge adéquate lors d'un incident prolongé, ou si un membre de l'équipe est malade, en congé ou en déplacement. Il se peut toutefois, vu la petite taille de votre ONG, que cela soit difficile ; il vous faudra donc identifier une équipe adaptée tout en tenant compte des capacités, des compétences et de l'expérience dont vous disposez.

Équipe de gestion de crise (EGC)

Il s'agit d'une petite équipe chargée de gérer tous les aspects d'un incident et de se mettre en relation avec l'ensemble des parties prenantes.

La composition et les responsabilités d'une EGC dépendent du type d'incident, du lieu où il survient et du niveau de soutien requis.

Principales fonctions de l'EGC	
Coordinateur de crise	Chargé de la coordination et de la gestion de l'EGC ; principal décideur au sein de l'équipe. Le coordinateur de crise relève normalement du directeur exécutif/PDG, lequel est chargé des décisions exécutives.
Ressources humaines	Fournit des conseils en matière de politiques RH et coordonne l'ensemble du support dédié au personnel et aux familles, ainsi que les questions d'assurance liées à la réponse apportée à l'incident.
Programmes et opérations	Fournit des conseils sur le contexte pays, les activités du programme et les parties prenantes pertinentes dans le pays ; coordonne l'ensemble des communications avec l'équipe pays.
Communications et médias	Fournit des conseils sur les questions relatives aux médias et coordonne l'ensemble des activités avec les médias et toutes les communications internes.
Gestion de l'information et support	Appuie l'EGC et maintient des dossiers d'information pendant la durée de la réponse apportée à l'incident.

Un membre de l'EGC peut avoir plusieurs fonctions. Selon la nature de l'incident, et les capacités disponibles au sein de l'organisation, des rôles de support supplémentaires seront requis, notamment dans les domaines de la sécurité, des finances, de l'assurance, des conseils juridiques, des communications internes et de l'informatique.

L'EGI a des fonctions internes similaires à celles de l'EGC, mais l'accent porte davantage sur une gestion localisée de l'incident. Il est essentiel d'avoir instauré une communication spécifique et gérée entre l'EGC et l'EGI pour bien pouvoir répondre à la crise. Dans les pays où l'ONG ne compte pas de personnel permanent et où un incident se produit, des dispositions devront être prises dans le plan de gestion de crise afin d'apporter une réponse localisée.

Quand peut-on parler de crise ?

Le moment où un incident ou une situation devient critique, ou se transforme en « crise », dépend principalement de sa gravité mais aussi des capacités de votre organisation, du degré de préparation et de l'expérience dont votre organisation dispose dans la gestion de ce type d'incidents.

Pour certaines ONG, même les incidents ou situations les moins graves peuvent être jugés critiques faute de capacités, d'expérience et de ressources. On parle généralement de « crise » lorsque les structures de gestion normales ne sont plus considérées comme étant suffisantes pour faire face à l'incident, d'où la nécessité de déclencher une intervention en cas de crise.

Tout incident de sécurité qui affecte votre personnel et vos programmes doit être rapidement évalué au plus haut niveau de la hiérarchie afin de déterminer ses répercussions potentielles et de clarifier le niveau d'engagement et de soutien nécessaire pour gérer la situation. Veillez à bien identifier les facteurs à partir desquels déclencher votre mécanisme de gestion de crise et à savoir qui dans l'organisation est chargé de prendre cette décision. Parmi les incidents critiques susceptibles de mobiliser votre équipe de gestion de crise, citons notamment les suivants :

- Si un membre du personnel décède ou est gravement blessé ;
- Si un tiers décède ou est gravement blessé du fait d'actes perpétrés par des membres du personnel ou d'activités de l'organisation ;
- Si une grave détérioration de la sécurité ou une menace spécifique affecte directement la sécurité du personnel ;
- En cas d'incident faisant de nombreuses victimes (par exemple catastrophe naturelle, bombardement ou attentat) et affectant le personnel ;
- En cas d'agression physique ou de violence sexuelle à l'encontre d'un membre du personnel ;
- En cas d'enlèvement, de kidnapping, d'arrestation ou de mise en détention d'un membre du personnel ;
- Si l'incident de sécurité risque de donner une mauvaise image de l'organisation dans les médias.

Principes de la gestion de crise

Lors d'un incident critique impliquant des membres du personnel, les principes clés suivants doivent être mis en œuvre :

- Minimiser tout autre dommage et veiller à la sécurité et au bien-être de la ou des victime(s) et des autres membres du personnel affectés par l'incident.
- Assurer aux familles et aux autres membres du personnel que l'organisation fait face à la situation de manière appropriée, et offrir un soutien aux parents affectés.
- Minimiser les éventuels préjudices ou pertes causés aux biens et aux ressources ; réduire tout impact négatif sur la réputation de l'organisation et la continuité des programmes/activités existants, pourvu que cela ne risque pas d'affecter la sécurité et le bien-être du personnel.
- Maintenir des communications efficaces avec l'ensemble des parties prenantes internes et externes afin de leur permettre de coopérer, en insistant sur l'importance de la confidentialité.

Plans de gestion de crise

Chaque incident est unique et, par conséquent, il est difficile de s'y préparer complètement. Il existe toutefois des mécanismes et dispositions clés qui peuvent être planifiés à l'avance.
Bien que le plan de gestion de crise soit un document établi au niveau du siège pour aider la direction à mobiliser et focaliser des ressources pour faire face aux incidents critiques ou aux situations de crise, il doit aussi exister un plan au niveau du pays à l'attention de l'EGI locale. Définissez clairement les rôles et les responsabilités, et établissez des points d'action clés, des listes de contrôle et des outils dans le cadre du plan de gestion de crise – votre personnel pourra alors réagir plus rapidement et de manière plus adaptée. Il faudra tenir un registre des décisions et des mesures prises dès l'activation du mécanisme.

Le personnel est en proie à un stress considérable en cas de crise, par conséquent les plans de gestion de crise devront être simples d'emploi, assortis de listes de contrôle facilement accessibles.

Plans de gestion de crise

Parmi les principaux éléments d'un plan de gestion de crise, citons les suivants :

- **Introduction** – indiquez à qui s'adresse ce document, qui est couvert par le plan, les définitions clés, quand le document devra être passé en revue et par qui.
- **Activation et facteurs déclencheurs** – indiquez de quelle manière le mécanisme sera activé et désactivé, qui en prend la décision et selon quels critères.
- **Gestion et processus décisionnel** – présentez la structure en place pour gérer les incidents critiques, les parties prenantes, les principes de gestion de crise de l'organisation et les questions de confidentialité. Incluez un organigramme des décisions pour expliquer les communications et le processus décisionnel.
- **Rôles et responsabilités** – présentez les rôles et responsabilités spécifiques pour les différentes fonctions de la structure de réponse à la crise, y compris pour les membres de l'EGC, de l'EGI et le personnel auxiliaire. Des cahiers des charges devront préciser les responsabilités de chaque fonction avant, pendant et après l'incident.
- **Protocoles d'incident** – présentez les procédures et directives relatives aux éventuelles interventions immédiates, les questions liées à la gestion des parties prenantes et les besoins en matière de soutien post-incident pour des scénarios spécifiques, par exemple urgences médicales, violence sexuelle, catastrophes naturelles, évacuations de sécurité, enlèvements et kidnappings, et mort de membres du personnel.
- **Ressources et outils** – incluez des listes de contrôle, des formulaires et des outils pour appuyer l'intervention de l'organisation, y compris des modèles pour enregistrer les communications et les décisions, des listes des interlocuteurs clés, etc.

Prestataires d'assistance et support

Les spécialistes de l'assistance externe peuvent considérablement aider votre organisation lors d'une crise en lui donnant des informations et des conseils précieux. Dans certains cas, selon la nationalité des individus impliqués, une assistance spécialisée peut aussi être fournie par leur gouvernement.

Même les organisations de plus grande taille qui disposent d'équipes dédiées internes et d'importantes capacités de sécurité font appel à des prestataires d'assistance externe lors de crises. Pour les ONG de plus

petite taille, qui n'ont peut-être pas l'expérience de ce type d'incidents ou la capacité de prendre en charge les différents rôles d'une EGC, il est important de prévoir un accès à une assistance externe avant qu'un incident ne survienne afin d'améliorer la capacité de l'organisation à faire face à une crise.

Les organisations peuvent bénéficier d'une assistance d'urgence complète et d'un soutien à la gestion de crise fournis par des prestataires commerciaux et des consultants par le biais de leur assurance ou en faisant directement appel à eux. Assurez-vous que l'expert auquel vous faites appel est adapté aux besoins de votre organisation et affiche le niveau de connaissances requis. Il existe un large éventail de services, notamment l'assistance médicale, le soutien aux évacuations sanitaires, l'évacuation du personnel suite à une détérioration de la situation sécuritaire ou à une catastrophe naturelle, l'accès à des consultants spécialisés dans la résolution des cas d'enlèvements et de kidnappings, et le soutien et la formation axés sur la gestion de crise. Si vous envisagez de demander un soutien supplémentaire, vérifiez le type de services déjà inclus dans votre police d'assurance et réfléchissez aux sociétés capables de fournir ces services.

Votre organisation ne saurait déléguer la gestion des incidents critiques ou sa responsabilité décisionnelle à un prestataire externe ou à d'autres parties prenantes. Elle doit rester activement engagée et s'assurer de l'adéquation de toutes les réponses et interventions. Tout mécanisme de soutien externe devra venir en complément de la réponse que votre propre organisation apporte à un incident critique.

Certains pays peuvent aider au rapatriement de leurs ressortissants en cas d'évacuation résultant d'un incident de sécurité (par exemple après un coup d'État), mais cela dépendra à la fois du pays du ressortissant et du pays dans lequel il se trouve. Cette aide ne saurait être garantie.

L'ONU ne garantit pas d'évacuer les travailleurs humanitaires qui ne font pas partie de ses employés. Même si elle organise une évacuation, il est probable qu'elle fasse payer la totalité du coût de cette assistance.

Complément d'information

Exemple de plan de gestion de crise

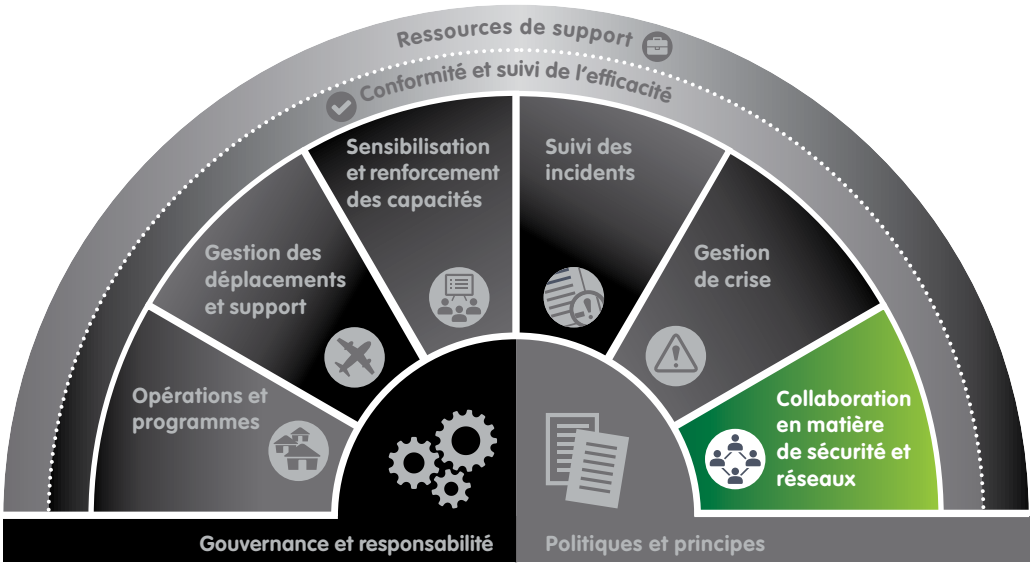
Manuel de l'EISF « Managing the message: Communication and media management in a security crisis »

Manuel de l'EISF « Family First: Liaison and support during a crisis »

Document d'information de l'EISF « Crisis Management of Critical Incidents »

Document d'information de l'EISF « Engaging Private Security Providers: A Guideline for Non-Governmental Organisations »

10 Collaboration en matière de sécurité et réseaux



De plus en plus soucieuses pour la sécurité de leur personnel, les ONG accordent désormais une grande importance à la collaboration et au partage d'informations sur la sécurité avec d'autres organisations. L'accès à des informations, à une analyse et à des conseils fiables permet de mieux prendre conscience de la situation, de prendre des décisions plus éclairées et, en fin de compte, de renforcer les stratégies de sécurité, quelle que soit la taille de l'organisation. Cependant, pour être efficace, la collaboration en matière de sécurité exige du temps et un investissement de la part du personnel. La qualité des mécanismes de collaboration est directement tributaire de la qualité de la participation des organisations impliquées.

Le partage actif de l'information sur la sécurité et la collaboration avec d'autres organisations sont des facteurs propices à la sécurité collective.

Réseaux sécurité inter-agences

Ces dernières années, les ONG ont formé différents réseaux et plateformes inter-agences dédiés à la sécurité, au niveau des pays, des régions et des sièges. Ces formes de collaboration facilitent l'échange des informations sécuritaires, sensibilisent les personnels grâce à des formations et des ateliers sur la sécurité, et encouragent l'adoption de meilleures pratiques. Il existe un large éventail de mécanismes plus ou moins formels. Citons notamment : les réunions informelles entre un petit groupe d'ONG pour aborder les défis associés à la sécurité, les bureaux dédiés à la sécurité chargés de fournir des informations et d'appuyer la communauté des ONG dans un contexte particulier, et les réseaux au niveau des sièges dédiés aux points focaux de la sécurité de différentes ONG (tels que l'EISF et InterAction).

Parmi les services proposés par ces initiatives figurent :

- L'organisation de réunions/briefings sur la sécurité ;
- La publication d'alertes sécurité/d'avertissements et d'avis ;
- La fourniture de rapports réguliers sur la sécurité ;
- La préparation de rapports analytiques sur les tendances des incidents ou des défis sécuritaires spécifiques ;
- L'instauration de liens avec l'UNDSS et d'autres acteurs de la sécurité (forces de sécurité nationales, y compris la police et l'armée, forces militaires internationales, etc.) ;
- La facilitation d'un accès aux formations et ateliers sur la sécurité ;
- La fourniture d'une assistance et d'un soutien lors des situations et incidents critiques.

Au niveau des sièges et des régions, ces services incluent généralement :

- L'organisation de réunions pour débattre des questions sécuritaires ;
- La facilitation d'un partage d'informations sur les bonnes pratiques en matière de gestion du risque sécurité ;
- L'appui à des organisations afin d'élaborer des stratégies et des politiques adaptées en vue d'une gestion efficace du risque sécurité ;
- L'instauration de liens avec les acteurs de la sécurité, tels que l'ONU, au niveau stratégique/d'un siège ;
- La promotion d'une sensibilisation accrue et d'améliorations en matière de sécurité des travailleurs humanitaires dans le secteur humanitaire en général.

Global Interagency Security Forum (GISF)
(anciennement European Interagency Security Forum, EISF)

GISF est un réseau de points focaux de sécurité qui représente plus de 100 organisations humanitaires opérant à l'international.

L'adjectif 'humanitaire' est ici entendu au sens large et désigne les activités non lucratives visant à contribuer au bien de l'humanité et à réduire ses souffrances.

GISF s'engage à améliorer la sécurité des opérations et du personnel, en soutenant la gestion humanitaire du risque sécurité.

A travers son réseau, il facilite les échanges entre ses membres et autres acteurs tels que l'ONU, les bailleurs de fonds, les universités et instituts de recherche, le secteur privé et autres ONGI.

GISF produit également des papiers de recherches et guides pratiques, ainsi qu'organise divers ateliers, événements et formations.

Pour en savoir plus visiter www.gisf.ngo

La sécurité de votre personnel devrait grandement bénéficier de l'accès à des informations, des conseils et du soutien sécuritaires rapides et fiables que procurent ces mécanismes. Cependant, l'information et les conseils ainsi fournis étant génériques et non pas adaptés à une organisation spécifique, vous devrez vous demander s'ils sont pertinents pour votre ONG étant donné son profil et ses capacités. Les membres du personnel chargés de la question sécurité au niveau d'un pays, d'une région ou du siège doivent être encouragés à identifier et instaurer des relations avec les différents réseaux sécurité inter-agences.

« Même si une organisation décide de ne pas participer à un mécanisme de coordination formel, elle doit chercher à partager l'information et à discuter des questions de sécurité sur le terrain. En tant qu'ONG, nous ne travaillons pas de façon isolée, par conséquent la sécurité de notre personnel dépend beaucoup de l'information et du soutien émanant d'autres organisations. »

Point focal sécurité d'une ONG

Saving Lives Together Framework

Le cadre Saving Lives Together est une série de recommandations formulées pour améliorer la collaboration en matière de sécurité entre le système de gestion de la sécurité de l'ONU et les ONG/organisations internationales. Il s'agit notamment :

- D'instaurer des arrangements et forums dédiés à la coordination de la sécurité ;
- De partager les informations sécuritaires pertinentes ;
- De coopérer en matière de formation à la sécurité ;
- De coopérer sur les arrangements opérationnels et logistiques, chaque fois que cela est possible ;
- D'identifier les besoins en ressources pour améliorer la coordination de la sécurité entre l'ONU, les ONG internationales et les organisations internationales, et de solliciter un financement ;
- De fournir des conseils sur les règles fondamentales communes de l'action humanitaire.

Complément d'information

« Saving Lives Together - A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field », IASC

« Guidelines for the Implementation of the "Saving Lives Together" Framework », Saving Lives Together

European Interagency Security Forum (EISF)

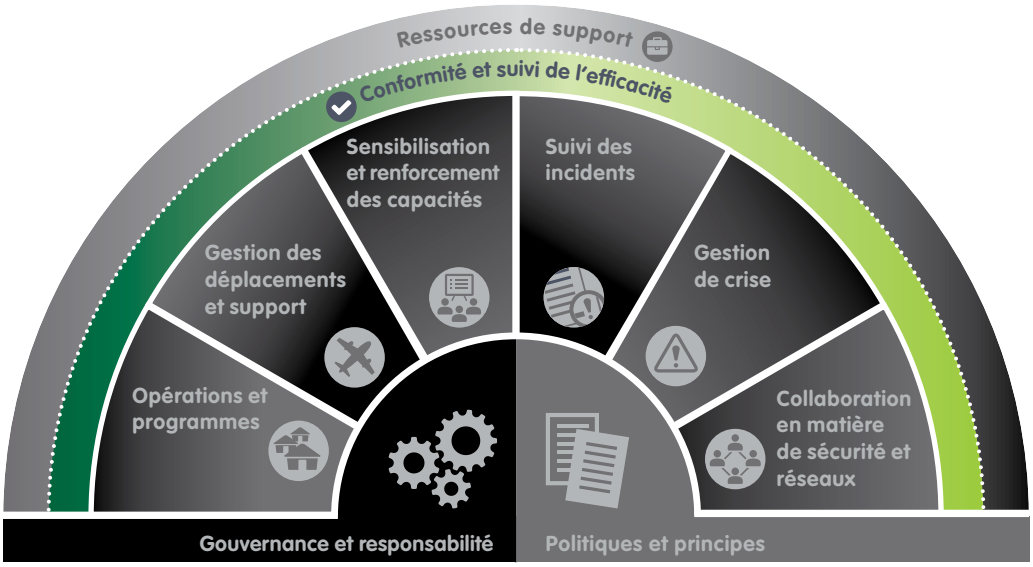
Strategic Security Coordination Mechanisms (page thématique sur le site de l'EISF)

The International Safety Organisation (INSO)

International NGO Safety and Security Association (INSSA)

InterAction

11 Contrôle de la conformité et de l'efficacité



Toute initiative visant à améliorer la sécurité au sein de votre organisation risque de connaître une certaine perte de vitesse après son lancement. Les risques auxquels est confronté votre personnel évoluant en permanence, votre gestion du risque sécurité doit être constamment révisée et améliorée.

La gestion du risque sécurité doit être réactive au changement, tant dans l'environnement externe qu'au sein de l'organisation. Les ONG doivent régulièrement contrôler et réviser leur cadre de gestion du risque sécurité pour s'assurer de sa pertinence.

Il est impératif que votre organisation contrôle sa conformité et entreprenne des examens et audits périodiques de sa gestion de la sécurité afin de déterminer si ses politiques et procédures restent efficaces et sont suivies, et si les risques de sécurité sont bien gérés à travers l'organisation afin de garantir l'accès aux populations affectées et une bonne mise en œuvre des programmes.

Contrôle de la conformité

Que faut-il contrôler ? Il s'agit de vérifier que votre personnel respecte les politiques et procédures de sécurité et que celles-ci fonctionnent comme prévu. Un contrôle routinier, à la fois de la conformité et du nombre d'incidents qui surviennent, sera propice à la bonne gestion des risques, conformément au cadre de sécurité, aux politiques et aux procédures de votre organisation. Il vous permettra aussi d'évaluer l'efficacité (par exemple l'accès, l'impact, les bénéfices et les coûts) de votre stratégie sécurité globale. Le contrôle de la conformité peut revêtir différentes formes :

- **Listes de contrôle de conformité** – les listes de contrôle aideront les managers/représentants pays à évaluer la conformité aux politiques sécurité et exigences minimales. Bien que ces listes ne se substituent pas à un audit ou à un examen complet, elles peuvent être utiles lorsqu'une organisation lance un cadre de gestion du risque sécurité et qu'elle cherche à savoir quels progrès ont été accomplis et quels ont été les obstacles.

  Voir « Tool 3 - Document review checklist », manuel de l'EISF « Security Audits »

- **Indicateurs de performance clés (KPI - Key Performance Indicators)** – l'instauration de KPI liés à la sécurité permet de vérifier que différents éléments du cadre de gestion du risque sécurité sont mis en œuvre et servent effectivement à minimiser les risques auxquels le personnel s'expose. Parmi les KPI à contrôler, citons les suivants : les plans sécurité sont à jour (% complets) ; le personnel qui se rend dans des destinations à haut risque a été briefé sur la sécurité (% réussite) ; le personnel a été formé (nombre total) ; et des incidents ont été signalés (nombre total).

  Pour d'autres exemples d'indicateurs, voir « Tool 6 - SMS Audit worksheet template », manuel de l'EISF « Security Audits »

- **Analyse des incidents** – le suivi et l'examen des incidents affectant le personnel permettront d'améliorer la manière dont votre organisation évalue son profil de risque. En comprenant quel type d'incidents implique le personnel, à quelle fréquence, et pourquoi, vous pourrez identifier les éventuels problèmes de conformité ou lacunes dans les procédures, dans la structure de support et dans la formation.

  Voir section 8 : Suivi des incidents

Si la conformité est faible, vous devrez faire preuve d'une plus grande rigueur à l'égard des personnes qui en sont responsables. Notez toutefois qu'une mauvaise conformité peut indiquer que le personnel peine à mettre en œuvre votre cadre de gestion du risque sécurité et les procédures en place. Il faudra donc les examiner et les adapter dans le cadre de l'amélioration continue du cadre de gestion du risque sécurité de votre organisation.

Audits et examens de sécurité

Si le contrôle de conformité repose sur des vérifications de routine, il vous faudra à un moment donné réaliser un audit ou un examen de la sécurité plus détaillé. Un audit de la gestion du risque sécurité est un examen interne ou externe, fondé sur des preuves, du cadre de gestion du risque sécurité d'une organisation et de sa mise en œuvre. Il permet de savoir si l'organisation remplit ses obligations de sécurité à l'égard de son personnel.

Il existe deux types d'audits de la gestion du risque sécurité :

- Les **audits organisationnels** passent en revue les dispositions prises au niveau de toute l'organisation concernant la gestion du risque sécurité ;
- Les **audits relatifs à un pays/un** site particulier étudient la gestion du risque sécurité et les systèmes dans un pays ou une région spécifique, souvent suite à une insécurité croissante ou à des changements au niveau de l'environnement opérationnel. Ces audits doivent être menés conformément aux politiques en vigueur au niveau de l'organisation, et non pas de manière isolée.

L'objectif de l'audit ou de l'examen doit être d'étudier l'efficacité de l'approche de votre organisation à l'égard de la gestion du risque sécurité afin que les objectifs des programmes soient réalisés et qu'un plan d'action soit élaboré pour améliorer la sécurité de l'ensemble du personnel. Appuyez-vous sur un large éventail d'employés (en particulier sur les « propriétaires des risques », autrement dit les personnes chargées de prendre des décisions en matière de gestion du risque sécurité), non seulement pour savoir si votre personnel comprend les systèmes en vigueur, mais aussi pour lui permettre de mettre en évidence les risques sécurité et défis auxquels il est confronté dans le cadre de son travail.

Pour vous faire une idée impartiale de votre organisation et la comparer à d'autres ONG, ou si vos capacités sont limitées, il peut être utile de faire appel à un consultant externe pour effectuer cet audit/examen sécurité.

Un audit externe étant onéreux, il sera important d'en tirer le meilleur profit.

Au lieu de recourir à un consultant, vous pourriez envisager de collaborer avec une autre ONG et d'effectuer un processus d'examen par les pairs.

Veillez à transmettre les conclusions et recommandations à tous ceux qui ont participé à l'exercice, ainsi qu'au personnel en général. Cela favorisera votre transparence, et montrera combien la gestion du risque sécurité est importante au sein de votre organisation.

De nombreuses organisations ont utilisé avec succès la boîte à outils « Security Audits » de l'EISF pour réaliser des audits internes et externes ; elle peut aussi servir de référence, et contribuer à identifier les domaines auxquels votre organisation devrait affecter ses ressources.

Examens externes de la sécurité

Un examen externe de la sécurité nécessite entre le consultant et le client une collaboration étroite et une vision claire des attentes et responsabilités, et ce, dès le début. Lorsque vous faites réaliser un examen externe de la sécurité, veillez aux points suivants :

- Assurez-vous d'avoir bel et bien besoin d'une aide externe ou d'un point de vue indépendant ;
- Rédigez un cahier des charges clair et concis. Soyez clairs quant à la portée de l'examen, aux résultats attendus et aux échéances ;
- Soyez réalistes quant au calendrier, au nombre de journées nécessaires et au budget requis ;
- Identifiez les consultants potentiels par un processus de sélection adapté à l'ampleur de l'examen recherché ;
- Soyez prêts à aborder vos priorités et exigences avec le consultant. Confirmez par écrit toutes les modifications apportées au cahier des charges ;
- Identifiez un point de contact unique au sein de l'organisation auquel le consultant présentera ses résultats et qu'il tiendra informé des progrès réalisés ;
- Veillez à ce que le consultant ait accès à l'information. Parmi les principaux documents requis, citons les politiques sécurité, les directives en matière de gestion du risque sécurité, les procédures lors des déplacements, les plans sécurité pays, les documents relatifs à la gestion de crise et les informations sur de précédents incidents ;
- Demandez à vos collègues de consacrer une partie de leur temps et de fournir des documents pour appuyer la réalisation de cet examen. Désignez la personne qui sera chargée d'organiser les entretiens avec les parties prenantes et adressez un courriel à l'ensemble du personnel pour leur demander de se tenir à disposition ;
- Gérez les attentes de vos collègues par rapport à l'examen, diffusez le cahier des charges et instaurez une méthode pratique pour solliciter un retour sur les conclusions et recommandations du rapport ;
- Donnez au consultant un retour sur les réactions suscitées par son rapport et ses recommandations, ainsi que sur son service en général.

Complément d'information

Manuel de l'EISF « Security Audits »

12 Ressources complémentaires

Pour renforcer la gestion du risque sécurité de votre organisation, tous les managers et membres du personnel doivent avoir accès à des conseils, outils et modèles relatifs à la sécurité qui soient pertinents. Il est essentiel de créer une bibliothèque ou référentiel de ressources utiles portant sur la question de la sécurité. Tirez parti des conseils relatifs à la sécurité personnelle et des ressources relatives à la gestion de la sécurité des ONG qui existent déjà, au lieu de partir de zéro.

En 2020, EISF est devenu GISF (Global Interagency Security Forum). Vous pouvez trouver toutes les ressources mentionnées dans ce rapport sur notre nouveau site internet : www.gisf.ngo

Sites Internet

www.gisf.ngo

www.ngosafety.org

www.ngosafety.org/keydata-dashboard

http://ingossa.org/

www.interaction.org/work/security

www.insecurityinsight.org/aidindanger

https://aidworkersecurity.org/incidents

www.disasterready.org/

https://kayaconnect.org

https://ifrc.csod.com/

https://training.dss.un.org/

Directives relatives à la sécurité personnelle

Stay Safe: The International Federations' Guide to Safer Missions, FIRC (2009).

Safety First: A Safety and Security Handbook for Aid Workers, Shaun Bickley, Save the Children (2014).

Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas, David Lloyd Roberts, ICRC (2005).

Safety Guide for Journalists, Reporters Without Borders et UNESCO (2015).

Directives en matière de gestion du risque sécurité

Security to go: a risk management toolkit for humanitarian aid agencies, 2nd edition by James Davis et al, EISF (2017).

GPR8 – Operational Security Management in Violent Environments, Revised Edition, Koenraad van Brabant, Overseas Development Institute (ODI) (2010).

ISO 31000:2009: Risk Management – Principles and guidelines, International Organization for Standardization (ISO) (2009).

Security Audits, Christopher Finucane, EISF (2013).

Mainstreaming the Organisational Management of Safety and Security (HPG Report 9), Koenraad van Brabant, Overseas Development Institute (ODI) (2001).

Glossaire

Acceptation : Instaurer un environnement opérationnel sécurisé grâce au consentement, à l'accord et à la coopération des différents individus, des communautés et des autorités locales.

Attitude face au risque : Démarche employée par l'organisation pour évaluer puis gérer, atténuer ou éviter le risque.

Audit sécurité : Examen interne ou externe, reposant sur des preuves, du cadre de gestion du risque sécurité d'une organisation et de sa mise en œuvre. Consiste à évaluer l'efficacité du cadre de gestion du risque sécurité en permettant à l'organisation d'atteindre ses objectifs, et à savoir si l'organisation remplit ses obligations de sécurité à l'égard de son personnel.

Cadre de gestion du risque sécurité : Série de politiques, de protocoles, de plans, de mécanismes et de responsabilités propres à réduire les risques de sécurité pour le personnel.

Crise : Un événement qui perturbe considérablement les opérations normales, qui a provoqué ou est susceptible de provoquer une grande souffrance, ou qui a des répercussions graves sur des individus, des membres du personnel ou l'organisation, et requiert des mesures extraordinaires pour que l'ordre normal soit rétabli, d'où la nécessité pour la direction de prendre immédiatement des initiatives.

Culture de sécurité : La « culture » d'une organisation peut tout simplement se définir comme « la manière de faire les choses ici ». Chaque organisation a sa propre culture en matière de sécurité et de gestion des risques en général.

Dissuasion : Réduire le risque en prenant des mesures pour le contrer (par exemple, protection armée, pressions diplomatiques/politiques, suspension provisoire).

« Duty of care », ou obligations de sécurité : Obligation légale et morale d'une organisation de prendre toutes les mesures possibles et raisonnables afin de réduire le risque de préjudices causés aux personnes qui travaillent pour l'organisation ou pour son compte.

Équipe de gestion de crise (EGC) : Une équipe chargée de gérer une situation de crise (incident critique) au siège de l'organisation ou au niveau régional.

Évaluation du risque : Processus par lequel l'organisation identifie les différentes menaces susceptibles d'affecter son personnel, ses actifs

et ses programmes, et analyse les risques en fonction de leur probabilité d'occurence et de leur impact afin d'identifier le degré de risque.

Gestion du risque : Activités coordonnées qui servent à guider et contrôler l'organisation face aux risques.

Incident critique : Événement ou série d'événements qui menace gravement le bien-être du personnel et pourrait entraîner la mort, des blessures mortelles ou des maladies, et qui peut pousser l'organisation à déclencher son protocole de gestion de crise. Un incident critique peut aussi être un événement qui a un impact grave sur les programmes, les actifs de l'organisation ou sa réputation.

Incident de sécurité : Une situation ou un événement qui a causé, ou pourrait causer, un préjudice au personnel, au personnel associé ou à un tiers, des perturbations significatives au niveau des programmes et activités, ou des dommages ou une perte substantiels pour les biens de l'organisation ou sa réputation.

Menace : Une difficulté pour l'organisation, son personnel, ses actifs, sa réputation ou ses programmes, liée à la sécurité ou à d'autres facteurs, présente dans le contexte opérationnel de l'organisation.

Plan sécurité : Document établi au niveau du pays qui présente les mesures et procédures de sécurité en vigueur, et les responsabilités et ressources nécessaires pour les mettre en œuvre.

Politique sécurité : Document exhaustif présentant clairement la stratégie de l'organisation à l'égard des risques de sécurité, les principes clés sous-jacents, et les rôles et responsabilités que doivent assumer tous les membres du personnel pour gérer ces risques.

Protection : Réduire la vulnérabilité de l'organisation à une menace éventuelle, par exemple en érigeant des murs ou en embauchant des gardiens.

Risque : Manière dont une menace pourrait affecter l'organisation, son personnel, ses actifs, sa réputation ou ses programmes, en tenant compte des vulnérabilités spécifiques.

Sécurité : Absence de risque ou de préjudices résultant d'actes de violence, d'agressions et/ou d'actes criminels volontairement perpétrés à l'encontre de membres du personnel, d'actifs ou de biens de l'organisation ; ou résultant d'actes, d'événements ou de dangers involontaires ou accidentels.

Stratégie de sécurité : Stratégie globale de l'organisation en matière de gestion du risque sécurité, qu'il s'agisse d'une stratégie d'acceptation, de protection et/ou de dissuasion.

Vulnérabilité : Exposition de l'organisation à une menace. Varie selon la nature de l'organisation, les particularités de son personnel, et sa capacité à gérer les risques.

Références

ACT Alliance. (2011). *Security Assessment Tool*. EISF. https://gisf.ngo/resource/security-assessment-tool/

Behn, O. et Kingston, M. (2010). « Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management », *Humanitarian Exchange Magazine, Issue 47*. Juin 2010. https://odihpn.org/magazine/whose-risk-is-it-anyway-linking-operational-risk-thresholds-and-organisational-risk-management/

Behn, O. et Kingston, M. (2010). *Risk Thresholds in Humanitarian Assistance*. EISF.

Buth, P. (2010). *Crisis Management of Critical Incidents*. EISF.

Centre for Safety and Development (non daté). « Managing security information – Simson software », *Centre for Safety and Development*. https://centreforsafety.org/duty-of-care/

Centre for Safety and Development. (2011). *Open NGO Security Policy*. EISF. https://gisf.ngo/resource/open-ngo-security-policy/

Davidson, S. (2013). *Family First: Liaison and support during a crisis*. EISF.

Davidson, S. (2013). *Managing the message: Communication and media management in a security crisis*. EISF.

Davis, J. et al. (2017). *Security to go: a risk management toolkit for humanitarian aid agencies*, 2nd edition. EISF.

De Palacios, G. (2014). « Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study », dans *Communications Technology and Humanitarian Delivery*. EISF. https://gisf.ngo/resource/communications-technology-and-security-risk-management/

De Palacios, G. (2016). « The Security of Lone Aid Workers », EISF. https://gisf.ngo/blogs/the-security-of-lone-aid-workers/

Finucane, C. (2011). *Humanitarian Safety and Security: Obligations and responsibilities towards local implementing partners*. Church World Service. https://gisf.ngo/resource/humanitarian-safety-and-securiy-obligations-and-responsibilities-towards-local-implementing-partners/

Finucane, C. (2013). *Security Audits*. EISF.

Finucane, C. (2013). *The Cost of Security Risk Management for NGOs*. EISF.

Garrett, C. (2005). *Developing a Security-Awareness Culture - Improving Security Decision Making*. SANS Institute.

Glaser, M. (2011). *Engaging Private Security Providers: A Guideline for Non-Governmental Organisations*. EISF.

Hodgson, L. et al. (2014). *Security Risk Management and Religion: Faith and secularism in humanitarian assistance*. EISF.

InterAction. (2015). *Minimum Operating Security Standards (MOSS)*. InterAction.

InterAction. (2017). *Security Plan Example*. EISF.

Inter-Agency Standing Committee (IASC). (2015). « Saving Lives Together – A Framework for Improving Security Arrangements Among IGOS, NGOs and UN in the Field, (October 2015) », IASC.
https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0

International Organization for Standardization (ISO). (2009). *ISO 31000:2009: Risk Management – Principles and guidelines*.

Kemp, E. et Merkelbach, M. (2011). « Can you get sued? Legal liability of international humanitarian aid organisations towards their staff », *Security Management Initiative*.
https://gisf.ngo/resource/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

Kemp, E. et Merkelbach, M. (2016). « Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications », *EISF*.
https://gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/

Linnell, H. (2017). « Guide to selecting appropriate Crisis Management Insurance », EISF.
https://gisf.ngo/resource/guide-to-selecting-appropriate-crisis-management-insurance/

Merkelbach, M. (2017). *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel*. Département fédéral suisse des Affaires étrangères (DFAE), Stabilisation Unit (SU) et Center for International Peace Operations (ZIF).

Persaud, C. (2012). *Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management*. EISF.

Persaud, C. (2014). *NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs*. EISF et InterAction.

Saving Lives Together. (2016). « Guidelines for the Implementation of the "Saving Lives Together" Framework », *Saving Lives Together*. Juillet 2016. https://gisf.ngo/resource/guidelines-for-the-implementation-of-the-saving-lives-together-framework/

Singh, I. (2012). *Security Management and Capacity Development: International agencies working with local partners*. EISF.

Source 8. (2015). *Office Opening: A guide for non-governmental organisations*. EISF.

van Brabant, K. (2010). *GPR8 – Operational Security Management in Violent Environments, Revised Edition*. Overseas Development Institute (ODI).

van Brabant, K. (2012). *Incident Statistics in Aid Worker Safety and Security Management*. EISF. https://gisf.ngo/resource/incident-statistics-in-aid-worker-safety-and-security-management/

Les références ci-dessus, ont été vérifiées en décembre 2020.

Annexe. **Cadre de gestion du risque sécurité – aide-mémoire**

Gouvernance et responsabilité

- Convenez d'une structure de gestion du risque sécurité adaptée à l'organisation afin qu'elle remplisse ses objectifs et veillez à ce que les rôles et responsabilités soient bien compris.
- Identifiez un Point focal sécurité (PFS) pour appuyer l'élaboration et la mise en œuvre du cadre de gestion du risque sécurité.
- Instaurez un groupe de travail/comité regroupant les différents départements de l'organisation et dédié à la sécurité afin de superviser l'instauration et la mise en œuvre du cadre de gestion du risque sécurité.
- Veillez à ce que tous les descriptifs de poste/cahiers des charges pertinents présentent les rôles et responsabilités en matière de gestion du risque sécurité qui sont associés à ce poste ou à cette tâche.

Politiques et principes

- Élaborez une politique sécurité qui reflète les principes et l'approche de l'organisation à l'égard de la sécurité.
- Veillez à ce que cette politique présente clairement l'attitude de l'organisation par rapport au risque, la structure de gestion du risque sécurité et les responsabilités des différents membres du personnel en matière de sécurité ainsi que ceux qui doivent assumer des rôles spécifiques dans le domaine de la sécurité.
- Fixez des exigences de sécurité minimales réalistes et adaptées à déployer sur chaque site et pour chaque activité, conformément au système d'évaluation du risque pays.

Opérations et programmes

- Instaurez un processus d'évaluation du risque sécurité identifiant les principaux risques dans un pays ou sur un lieu donné et présentant les mesures de contrôle en place pour gérer ces risques.
- Veillez à ce que tous les programmes pays réalisent régulièrement des évaluations du risque sécurité, avec documents à l'appui.
- Veillez à ce que des plans sécurité présentant les mesures et procédures de sécurité en place pour gérer les risques identifiés soient instaurés sur tous les sites où l'organisation dispose d'une présence significative ou bien où elle s'implique régulièrement.
- Évaluez la capacité et le soutien sécurité dont votre personnel peut disposer auprès de partenaires locaux ou d'organisations hôtes. Veillez à ce que tout arrangement ou accord relatif à un soutien sécurité présente clairement les responsabilités des deux parties.

Gestion des déplacements et support

- Trouvez un système basique d'évaluation du risque pays/déplacements pour que les membres du personnel sachent quels risques sont associés à leur travail ou leur déplacement dans ces pays. Instaurez des exigences minimales en matière de mesures, mécanismes et formation sécurité s'appliquant à chaque niveau d'évaluation.
- Assurez-vous que des évaluations de risques lors des déplacements soient faites et approuvées chaque fois que du personnel se rend dans une destination à haut risque, ou si la nature de cette visite soulève des préoccupations d'ordre sécuritaire.
- Élaborez des procédures de sécurité spécifiques aux déplacements internationaux s'adressant au personnel, aux consultants et aux visiteurs. Il s'agira ainsi de fournir des informations sur les rôles et responsabilités, les formations et briefings, le suivi des déplacements, les autorisations et les procédures d'urgence.
- Assurez-vous que le personnel dispose d'informations et conseils détaillés et à jour sur les risques sanitaires et de sécurité dans leur destination avant leur départ.
- Vérifiez que l'ensemble du personnel, des consultants et des visiteurs qui se rendent dans un lieu à haut risque reçoive des informations sécuritaires spécifiques au pays ou à la zone concernée, avant leur départ, et à leur arrivée si l'organisation dispose d'un bureau pays.
- Instaurez des procédures pour vérifier la présence d'un membre du personnel lors d'un déplacement afin de contrôler ses mouvements, et s'assurer de pouvoir le localiser d'après son billet d'avion.
- Veillez à ce que l'ensemble du personnel, y compris les consultants, dispose d'une couverture d'assurance adéquate lors de ses déplacements et activités professionnelles sur le terrain, et à ce qu'il soit pleinement informé des dispositions liées à cette police d'assurance.

Sensibilisation et renforcement des capacités

- Veillez à ce que tous les nouveaux membres du personnel soient initiés à la question de la sécurité grâce à une formation de base couvrant la politique et l'approche sécurité de l'organisation, ainsi que les différentes responsabilités au sein de l'organisation.
- Identifiez des ressources de formation à la sécurité disponibles en ligne et que l'ensemble du personnel devra suivre dans le cadre de son orientation.
- Étudiez les différentes options en matière de formation sécurité pour les différentes catégories de personnel en fonction de l'environnement risque là où il travaille et se déplace et de ses responsabilités à l'égard de la sécurité .

Suivi des incidents

- Instaurez des procédures de signalement des incidents et des rapports types. Faîtes comprendre au personnel l'importance d'un signalement des incidents, ce qu'il faut signaler et de quelle manière.
- Instaurez un système d'enregistrement centralisé des incidents pour sauvegarder les informations clés sur tous les incidents sécurité affectant le personnel.
- Passez périodiquement en revue tous les incidents affectant le personnel afin d'identifier d'éventuelles tendances et préoccupations en matière de sécurité.

Gestion de crise

- Identifiez une structure de gestion de crise adaptée afin de coordonner et gérer la réponse de l'organisation aux incidents critiques.
- Développez un plan de gestion de crise indiquant les rôles et fonctions de l'EGC et de l'EGI, présentant l'autorité décisionnelle et décrivant les principales procédures à suivre pour répondre aux situations de crise.
- Envisager d'inclure un accès à des services de soutien en cas d'urgence et de gestion de crise (sanitaire et autre) dans la couverture d'assurance de l'organisation.

Collaboration en matière de sécurité et réseaux

- Veillez à ce que le personnel participe régulièrement à des forums et réunions inter-agences axés sur la sécurité afin de renforcer le partage de l'information et la collaboration dans ce domaine.

Contrôle de la conformité et de l'efficacité

- Procurez aux managers/représentants pays une liste de contrôle relative à la gestion du risque sécurité afin qu'ils puissent voir si les politiques sécurité et les exigences minimales sont respectées.
- Veillez à ce que des audits sécurité pays/programmes soient régulièrement réalisés, surtout si les activités se déroulent dans des pays à haut risque.
- Réalisez un examen périodique de l'approche et du cadre de gestion du risque sécurité de l'organisation, et élaborez un plan d'action pour promouvoir la sécurité de tout le personnel.
- Instaurer et faîtes respecter une forte culture disciplinaire à l'égard du non-respect des politiques sécurité et des exigences minimales.

Ressources complémentaires

- Mettez à disposition différents documents, outils et modèles dans le cadre d'un référentiel sécurité destiné à aider les managers et le personnel à gérer les risques sécurité.

Autres publications de l'EISF

Pour contribuer à de prochains projets de recherche ou suggérer des thématiques pour de futurs travaux, veuillez contacter **gisf-research@gisf.ngo**.

En 2020, EISF est devenu GISF (Global Interagency Security Forum). Vous pouvez trouver toutes les ressources mentionnées dans ce rapport sur notre nouveau site internet : www.gisf.ngo.

Documents d'information et rapports

Partnerships and Security Risk Management: from the local partner's perspective
Septembre 2020
Moutard, L. – GISF

Duty of Care under Swiss law: how to improve your safety and security risk management processes
Octobre 2018
Fairbanks, A. – cinfo et EISF

Managing the Security of Aid Workers with Diverse Profiles
Septembre 2018
Jones, E. *et al.* – EISF

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
March 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 espagnole et française 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 française 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 Formation de l'EISF

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

Articles

Managing security-related information: a closer look at incident reporting systems and software
Décembre 2018
de Palacios, G.

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 Council Ruling and its Implications
Septembre 2016
Kemp, E. et Merkelbach, M. Edité 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*, numéro 47)
Behn, O. et Kingston, M.

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

Guides

Managing Sexual Violence against Aid Workers: prevention, preparedness, response and aftercare
Mars 2019
EISF

Abduction and Kidnap Risk Management
Novembre 2017
EISF

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

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

Office Opening
Mars 2015 – *Version française disponible*
Source8

Security Audits
Septembre 2013 – *Versions espagnole et française disponibles* Finucane C. Édité par French, E. et Vazquez Llorente, R.
(Es. et Fr.) – Secrétariat de l'EISF

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

Family First: Liaison and Support During a Crisis
Février 2013 – *Version française 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