



Partenariats et gestion du risque sécurité :

guide d'action conjointe pour
les organisations humanitaires
locales et internationales

Contexte

Ce guide s'appuie sur de précédentes recherches du GISF, et notamment sur le rapport *Partnerships and Security Risk Management: from the local partner's perspective* (Partenariats et gestion du risque sécurité : du point de vue des partenaires locaux). Il repose également sur des entretiens menés avec des experts et sur les résultats d'une phase d'évaluation qui a permis à huit organisations non gouvernementales nationales et locales de tester une version préliminaire de ce guide auprès de leurs organisations partenaires.

L'auteure et GISF tiennent à remercier les personnes et les organisations qui ont pris le temps de partager des ressources et de faire part de leurs observations, ainsi que de mettre à l'épreuve la version préliminaire du guide. Leurs contributions ont joué un rôle fondamental dans l'élaboration de ce document. Vous trouverez ci-après une liste des personnes ayant pris part à cet ouvrage.

Suggestion de citation

GISF. (2021) *Partenariats et gestion du risque sécurité: guide d'action conjointe pour les organisations humanitaires locales et internationales*. Global Interagency Security Forum (GISF).

Clause de non-responsabilité

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

Le contenu de ce document ne doit pas être considéré comme offrant des conseils spécifiques à votre situation sur lesquels vous pouvez entièrement vous fier. Avant d'agir ou de ne pas agir sur la base de ce document, vous devez obtenir des conseils adaptés d'un spécialiste ou professionnel. Bien que GISF se soit efforcé de veiller à l'exactitude des informations figurant dans le présent document, il n'en garantit ni la précision, ni l'exhaustivité. Les informations présentées sont fournies « telles quelles », sans aucune condition, garantie ou autre modalité quelle qu'elle soit, et l'utilisation de tout renseignement ou autre information contenus dans le présent document est entièrement aux risques des lecteurs et lectrices.

Dès lors, dans toute la mesure permise par la législation en vigueur, GISF décline toute responsabilité quant aux représentations, garanties, conditions et autres conditions qui, sans cet avis légal, pourraient être applicables par rapport aux informations contenues dans le présent document. GISF ne saurait être tenu responsable de toute perte ou de tout dommage quels qu'ils soient, causés au lecteur ou à une tierce partie du fait de l'utilisation des informations contenues dans ce document.

© 2021 Global Interagency Security Forum

Remerciements

Responsable du projet : Léa Moutard

Auteure : Adelicia Fairbanks

Experts ayant contribué aux travaux :

Ancien partenaire de CAFOD en Afghanistan

CAFOD : Jamie Monteith, Katy Nembe Katonda

Caritas Goma : Marie Muhemedi

Caritas Ukraine : Maksym Skrypal

Concern Worldwide : Peter Doyle

GISF : Lisa Reilly, Heather Hughes

HAI : Sudhanshu Sekhar Singh

Heizmannconsultancy : Franziska Heizmann

ICRC: Roberto Christensen, Jean-Philippe Kiehl, Hugo Van Den Eertwegh,

Robert WhelanICVA : Eman Ismail, Alon Plato, Jeremy Rempel, Jeremy Wellard

Keen & Care Initiative : Josephine Alabi

Kvinna till Kvinna : Joana Costa

LWF : Susan Muis

MAG : David Adam

Ohaha Family Foundation : John Ede

Oxfam : Jan Bouwman

Partenaire au Myanmar : Tuja

Plan International : Élodie Leroy-LemoigneRICE WN : Jackson Olema, Pax Sakari

Saferworld : Dorcas Akello, Euan Mackenzie, Ramzy Magambo, Wilfred Opobo et Sara Torrelles

SARD : Fares AlsalehTiti Foundation South Sudan : Gloria Modong Morris Soma

Trócaire : Win Naing, Peter Ott, Ashley Proud, Doi San

WACSOF : Komlan Messie

Traduction française : Catherine Dauvergne-Newman avec le soutien d'Emmanuelle Strub et de Léa Moutard.

Navigation

-  principaux points et conseils
 -  témoignages d'experts
 -  renvois
 -  ressources complémentaires
 -  six outils sont inclus ici (à partir de la page 86) et disponibles sous format modifiable sur www.gisf.ngo
- Les **mots en bordaux** sont expliqués dans le glossaire (page 118)

Principales définitions

'Duty of care'¹ : obligation légale et morale d'une organisation de prendre toutes les mesures possibles et raisonnables afin de réduire le risque de préjudice causé à celles et ceux qui travaillent pour elle ou en son nom.

Organisation non gouvernementale internationale (ONGI) : ONG dont les opérations s'étendent au-delà d'un pays ou d'une sous-région.

Organisation non gouvernementale locale/nationale (ONG L/N) : ONG locale ou nationale dont les opérations se déroulent dans son pays d'origine.

Partage du risque : les organisations partagent la responsabilité à l'égard des risques de sécurité qui les affectent.

Partenariat : relation formelle (contractuelle) conclue entre organisations humanitaires. Il s'agit généralement de partenariats entre une organisation internationale et une organisation locale/nationale. Dans le secteur de l'aide, les partenariats peuvent revêtir différentes formes, aussi bien en termes de durée que d'envergure ou de degré de collaboration.

Transfert du risque : apparition ou transformation d'un risque (qu'il diminue ou s'accroît) pour un acteur du fait de la présence ou des actions d'un autre acteur, que cela soit intentionnel ou non.

 Vous trouverez des définitions supplémentaires dans le **glossaire**

¹ Les 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



Table des matières

Introduction	08
À qui s'adresse ce guide ?	09
Guide et outils : mode d'emploi	09
Gestion du risque sécurité : définition	11
1. Poser les bases d'un partenariat équitable en matière de gestion du risque sécurité	13
1.1. De l'importance d'une approche équitable et conjointe à l'égard de la sécurité au sein des partenariats	13
1.2. Comprendre et résoudre la question du transfert du risque sécurité entre partenaires	16
1.3. Adopter les principes du partenariat	20
1.4. Communiquer et instaurer la confiance au sein du partenariat	21
1.5. Explorer les attitudes face au risque sécurité au sein du partenariat	24
2. Réaliser un examen conjoint des processus de gestion du risque sécurité au sein du partenariat	26
2.1. L'examen conjoint de la GRS	26
2.2. Planifier la stratégie	30
2.3. Remplir le questionnaire et évaluer les indicateurs	31
2.3.1. <i>Duty of care</i>	35

2.3.2.	Gouvernance et responsabilité	38
2.3.3.	Politique et principes	41
2.3.4.	Opérations et programmes	44
2.3.5.	Gestion des déplacements et support	48
2.3.6.	Sensibilisation et renforcement des capacités	51
2.3.7.	Suivi des incidents	54
2.3.8.	Gestion de crise	57
2.3.9.	Collaborations et réseaux dans le domaine de la sécurité	60
2.3.10.	Compliance et suivi de l'efficacité	63
2.3.11.	Ressources complémentaires	66
2.4.	Élaborer et mettre en œuvre un plan d'action en vue d'un examen conjoint de la GRS	68
3.	Identifier et répondre ensemble aux besoins, lacunes et défis en matière de GRS	69
3.1.	Identifier et répondre ensemble au risque sécurité	69
3.2.	Financer la gestion du risque sécurité au sein du partenariat	71
3.3.	Renforcer les capacités de gestion du risque sécurité au sein du partenariat	73
4.	Plaidoyer en faveur du changement : améliorer la sécurité dans le secteur de l'aide humanitaire au moyen du partenariat	78
4.1.	Mener un plaidoyer conjoint	78

4.2.	Gestion du risque sécurité et plaidoyer	81
4.2.1	Protéger les travailleurs humanitaires des attaques ciblées	81
4.2.2.	Plaidoyer en faveur de la gestion du risque sécurité et agenda de localisation	82
4.2.3.	Plaidoyer en faveur de la gestion du risque sécurité et financement	82
5.	Outils	86
Outil 1.	Une communication de qualité au sein du partenariat	87
Outil 2.	Attitude face au risque au sein du partenariat	89
Outil 3.	Modèle de questionnaire et de feuille de travail en vue de l'examen conjoint de la GRS	91
Outil 4.	Modèle de plan d'action en vue de l'examen conjoint de la GRS	107
Outil 5.	Modèle d'évaluation et de plan de gestion conjoints du risque sécurité	109
Outil 6.	Modèle de budget dédié à la gestion du risque sécurité au sein du partenariat	114
Glossaire		118
Références		122
Autres publications de GISF		126



Introduction

Ce guide est le troisième volet d'un projet de GISF visant à améliorer la **gestion du risque sécurité (GRS)** dans le cadre des accords de partenariat conclus entre organisations non gouvernementales internationales (ONGI) et organisations non gouvernementales locales et nationales (ONG L/N) du secteur de l'aide.

Qu'entend-on par partenariat ?

Dans ce guide, un **partenariat** désigne toute relation formelle (contractuelle) entre une ONGI et une ONG L/N. Les partenariats du secteur de l'aide peuvent revêtir différentes formes, aussi bien en termes de durée que d'envergure ou de degré de collaboration. Ils peuvent par exemple être stratégiques et de longue durée, ou axés sur un projet unique et de courte durée.

- La première phase de ce projet a consisté à analyser les relations entre les ONG internationales et leurs partenaires locaux. Cette analyse a mis l'accent sur la perspective des ONGI et le renforcement de leurs capacités.

 Voir *Security Management and Capacity Development: International agencies working with local partners* (2012)

- La deuxième phase a été consacrée aux perspectives et expériences du personnel d'ONG L/N. Les recherches ont démontré que le transfert croissant de responsabilité envers la fourniture d'aide humanitaire ou de développement aux acteurs locaux (dans le cadre de l'agenda de **localisation**) n'avait pas donné lieu à des conversations franches et ouvertes sur le transfert des **risques de sécurité**.

 Voir *Partnerships and Security Risk Management: from the local partner's perspective* (2020)

- Ce guide, troisième volet de notre projet, s'appuie sur les résultats de ces précédentes recherches. Il vise à résoudre les difficultés identifiées, à mettre en évidence les opportunités potentielles et à favoriser des partenariats plus équitables, plus durables et plus transparents. Ces partenariats promeuvent un rapport de confiance et l'apport de bénéfices mutuels en matière de gestion du risque sécurité.



Attention : ce guide n'est pas un manuel de formation.

À qui s'adresse ce guide ?

Ce guide s'adresse aux ONGI et aux ONG L/N qui s'appêtent à conclure ou qui ont déjà conclu un partenariat.

- Pour les organisations qui envisagent de conclure un partenariat, ou entament cette démarche : ce guide permettra d'intégrer la gestion du risque sécurité dès la phase préliminaire.
- Pour les organisations qui ont déjà conclu un partenariat : ce guide aidera les différents partenaires à passer en revue les arrangements déjà en place au niveau de la gestion du risque sécurité.



Pour les organisations qui disposent déjà d'un partenariat, il s'agira d'utiliser ce guide et ses outils afin de passer en revue et de modifier les processus existants plutôt que de repartir de zéro.

Ce guide s'adresse aux collaborateurs chargés des opérations, de la sécurité ou des partenariats au sein d'ONGI et d'ONG L/N. Il intéressera aussi les experts non spécialistes de la sécurité. Pour être (la plus) efficace, la gestion du risque sécurité ne saurait fonctionner en vase clos.



Ces différents individus sont invités à consulter des collègues pertinents à tous les niveaux de leur organisation et à collaborer avec eux afin de renforcer la gestion du risque sécurité au sein du partenariat.

Guide et outils : mode d'emploi

Ce document répertorie les mesures que les organisations humanitaires peuvent prendre pour adopter une approche plus équitable en matière de gestion du risque sécurité au sein du partenariat.

Le guide comprend cinq chapitres :

- **Chapitre 1** : Discussions initiales en vue de poser les bases d'un partenariat équitable
- **Chapitre 2** : Étapes d'un « examen conjoint de la gestion du risque sécurité »

- **Chapitre 3** : Besoins, lacunes et défis en matière de gestion du risque sécurité
- **Chapitre 4** : Plaidoyer pour améliorer la gestion du risque sécurité au sein du secteur de l'aide
- **Chapitre** : Outils pour soutenir la gestion du risque sécurité au sein du partenariat.

Le schéma 1 permet de visualiser la structure de ce guide.

Schéma 1. Gestion du risque sécurité au sein du partenariat



Au début d'un partenariat, il est essentiel d'aborder certaines questions et d'adopter des méthodes de travail équitables. Il s'agit notamment de mettre en pratique les principes du partenariat, d'employer une communication de qualité et d'avoir des conversations ouvertes sur le transfert du risque et les attitudes vis-à-vis du risque au sein du partenariat.

C'est sur cette base que le guide présente un **examen conjoint de la gestion du risque sécurité** (« examen conjoint de la GRS »). Cet examen repose sur toute une série de questions et d'indicateurs qui visent à encourager les partenaires à mieux comprendre leur position respective envers la gestion du risque sécurité. Cet examen se termine par l'élaboration et la mise en œuvre d'un **plan d'action en vue de l'examen conjoint de la gestion du risque sécurité** (« plan d'action en vue de l'examen conjoint de la GRS »). Ce plan permet d'assurer un suivi des mesures prises afin de renforcer la gestion du risque sécurité au sein du partenariat.

L'examen conjoint de la gestion du risque sécurité doit faire partie intégrante de l'évaluation plus globale du risque associé au partenariat ; il ne doit pas s'agir d'un processus distinct ou parallèle.

Ce guide propose ensuite des orientations pour aider les partenaires à identifier les besoins, les lacunes et les défis en matière de gestion du risque sécurité. Il suggère comment y répondre à travers une évaluation conjointe du risque sécurité et offre des conseils pour gérer les besoins en matière de financement et de renforcement des capacités. Enfin, il aborde les possibilités de recourir au plaidoyer pour renforcer la gestion du risque sécurité des partenaires.

Les partenariats peuvent être conclus sous différentes formes, selon la nature et la durée de la relation, le type et la taille des ONG impliquées et le contexte. Les conseils présentés dans ce document pourront être adaptés en fonction de la structure du partenariat et du contexte opérationnel de l'organisation.

Gestion du risque sécurité : définition

Il est important que les partenaires comprennent les termes de « risque sécurité » et « gestion du risque sécurité ».

Dans ce guide, le **risque** désigne la manière dont une **menace** peut affecter une organisation, son personnel, ses actifs, sa réputation ou ses

programmes. Une menace peut engendrer un préjudice ou un dommage pour le personnel, ou une perte ou un préjudice pour l'organisation. La **vulnérabilité** désigne la mesure dans laquelle l'organisation, le personnel, les actifs ou les programmes sont exposés à une menace.

Les risques découlant d'événements non intentionnels (par exemple un accident de la route) sont souvent qualifiés de « risques de **sécurité** ».

Les risques résultant d'actions intentionnelles (actes de violence, enlèvements, etc.) sont généralement appelés « risques de **sûreté** ».

Notez que nous employons ici le terme générique de « sécurité » qui comprend la sûreté, et que le « personnel » et les « collaborateurs » désignent également les bénévoles qui travaillent pour une organisation.

La **gestion du risque sécurité** emploie toute une série de stratégies et d'outils pour réduire les risques susceptibles de survenir à l'issue d'un acte intentionnel ou non intentionnel. La GRS est un moyen, et non une fin en soi ; il s'agit d'instaurer des pratiques qui permettent aux organisations d'atteindre leurs objectifs tout en protégeant leurs collaborateurs.



Pour de plus amples renseignements sur la gestion du risque sécurité

Ce guide n'est ni un manuel d'introduction à la gestion du risque sécurité, ni un guide sur le processus d'audit organisationnel en matière de GRS.

Pour de plus amples informations sur la gestion du risque sécurité dans son ensemble, voir :

- *EISF - Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *EISF - La sécurité en pratique*
- *ODI-GPR8 - Operational Security Management in Violent Environments*

Pour obtenir des conseils sur la réalisation d'un audit organisationnel général de la GRS, consulter :

- *EISF - Évaluations de la sécurité*
- *EISF - The Cost of Security Risk Management for NGOs*



Poser les bases d'un partenariat équitable en matière de gestion du risque sécurité

1.1. De l'importance d'une approche équitable et conjointe à l'égard de la sécurité au sein des partenariats



« La gestion du risque sécurité est un outil essentiel de l'action humanitaire et une condition préalable à la conclusion de partenariats équitables. Lorsque les ONG L/N prennent la responsabilité et l'initiative d'apporter une aide humanitaire en partenariat, elles acceptent également les risques de sécurité associés – même si le transfert du risque n'est pas intentionnel. »

GISF – Partnerships and Security Risk Management: from the local partner's perspective

Au sein des partenariats, ce sont souvent les ONG L/N qui font face aux risques de sécurité les plus lourds, notamment lors des opérations quotidiennes menées dans des contextes à haut risque. En matière de gestion du risque sécurité associée plus précisément à leurs accords de partenariat, les ONG rencontrent souvent les difficultés suivantes :

- Disparités dans les discussions et les analyses du **transfert de risque** et des **attitudes face au risque**.
- Difficultés à parvenir à une compréhension commune du contexte et des risques associés.
- Manque de fonds dédiés à la GRS, surtout dans les budgets des ONG L/N, mais aussi des ONGI.
- Trop peu de ressources et de temps consacrés au renforcement des capacités de gestion du risque sécurité des deux partenaires, même quand les lacunes ont été identifiées de manière conjointe.
- Malentendus en raison de la barrière de la langue, d'un engagement physique limité entre partenaires et d'une absence de terminologie commune pour communiquer sur le risque sécurité et la GRS.
- Obstacles à une communication ouverte et franche, notamment

à cause de différences culturelles et de communication, d'un déséquilibre du pouvoir, de pressions pour être compétitifs et d'une crainte de perdre son financement.

- Difficultés à obtenir et partager des informations sécuritaires pertinentes (défi auquel les deux partenaires sont souvent confrontés).

L'une des principales lacunes dont pâtissent les partenariats ONGI-ONG L/N est l'absence d'une discussion équitable et commune permettant d'étudier les défis ci-dessus. Lorsque des conversations ont lieu, il arrive que les ONGI s'en servent simplement afin d'évaluer ce dont dispose l'ONG L/N et déterminer si cela correspond aux normes de l'ONGI.

Si ces discussions peuvent être utiles, elles peuvent aussi donner l'impression à l'ONG L/N d'être « évaluée ». Cette « évaluation descendante » (« top down » en anglais) part du principe que l'approche de l'ONGI en matière de gestion du risque sécurité est meilleure que celle de l'ONG L/N – ce qui n'est pas forcément le cas.

Il est donc important de délaissier les conversations sur la GRS qui visent essentiellement à évaluer de manière descendante la capacité sécuritaire de l'ONG L/N, et d'instaurer à la place un dialogue commun sur les thématiques que sont les risques, les ressources, les besoins, les opportunités de collaboration et le renforcement des capacités.



Pour garantir une approche équitable en matière de GRS au sein des partenariats, il faut cesser de mettre l'accent sur les défis posés par le « transfert du risque », en cherchant plutôt à identifier des moyens de « partager le risque ».

Afin de partager la responsabilité à l'égard du risque sécurité, les organisations doivent adopter une stratégie qui encourage une relation plus équitable entre les partenaires. Il s'agit de :

- Réaliser un examen conjoint de ce dont chaque partenaire dispose déjà en termes de **gestion du risque sécurité**.
- Identifier les lacunes et défis ainsi qu'une stratégie permettant aux partenaires de les résoudre ensemble.
- Veiller à ce que les voix et les expériences des personnels des deux organisations partenaires soient entendues et valorisées de manière égale.
- Étudier les risques de sécurité et les mesures d'atténuation qui s'appuient sur les forces du personnel de l'ONG L/N.
- Reconnaître que les approches sécuritaires les plus efficaces sont

évolutives et contextuelles (les approches sécuritaires conventionnelles des ONGI ne seront donc pas toujours adaptées).

L'action « conjointe » dans la pratique

IL FAUT :

- Mener des discussions ouvertes et franches sur ce qui fonctionne bien et ce qui ne fonctionne pas.
- S'encourager mutuellement à améliorer les méthodes de travail.
- Rechercher des solutions ensemble.
- Partager régulièrement des informations et des pratiques .
- Se consulter afin d'éclairer l'élaboration de nouvelles politiques et pratiques.
- Adapter les ressources existantes aux réalités et aux besoins des deux partenaires.

IL NE FAUT PAS :

- Prendre de décisions de manière isolée qui puissent affecter l'organisation partenaire.
- Ignorer les préoccupations et les idées d'un des partenaires.
- Baisser les bras à la première tentative (l'instauration d'une relation prend du temps).
- Éviter les conversations ou les situations difficiles.

Pour instaurer des bases solides en vue d'un partenariat équitable en matière de GRS, les organisations doivent discuter ouvertement du **transfert du risque**, adopter les principes du partenariat, utiliser un mode de communication de qualité et étudier ensemble l'**attitude face au risque** de chaque partenaire. Ces points fondamentaux sont abordés de manière plus détaillée dans les parties suivantes.



Complément d'information

- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*
- *Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships*

1.2. Comprendre et résoudre la question du transfert du risque sécurité entre partenaires

En concluant un partenariat, les organisations opèrent automatiquement un transfert de risque, qu'elles en aient conscience ou non. Il est important que les partenaires comprennent ce que signifie ce transfert de risque pour les deux organisations et qu'ils trouvent ensemble des moyens de répondre aux difficultés identifiées.

Déséquilibres de pouvoir au sein des partenariats

L'un des partenaires a souvent plus de pouvoir que l'autre – tel est l'un des principaux défis de tout partenariat. Citons notamment les considérations suivantes :

- **Accès aux ressources ou utilisation de celles-ci** : personnels, moyens financiers, équipement, outils de communication.
- **Accès à l'information** : notamment la capacité à contrôler l'information et son mode de diffusion.
- **Relations et réseaux** : relations avec d'autres individus, agences ou groupes dotés d'un certain pouvoir (par exemple les donateurs).
- **Autorité et légitimité** : reconnaissance formelle, ou ancrée dans la réputation de l'organisation, qui permet à celle-ci de prendre des décisions et des mesures largement acceptées.
- **Statut juridique/officiel** : différences au niveau du statut juridique ou officiel – par exemple nationalité/type de passeport, mesures d'évacuation/opportunités de relocalisation, « neutralité » perçue ou implicite.

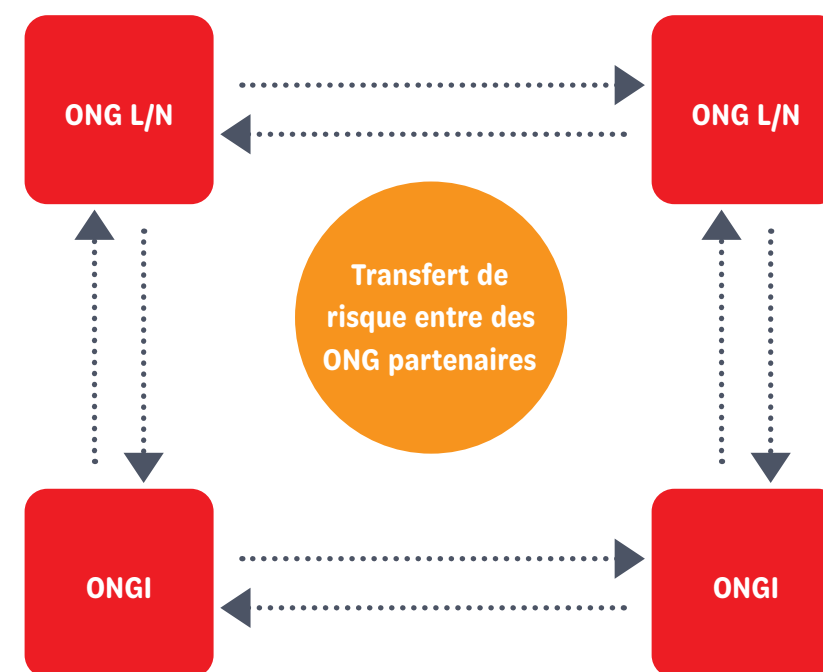
Une organisation qui semble avoir moins de pouvoir risque de se sentir contrainte d'accepter les décisions et les attentes d'un partenaire plus puissant. Par exemple, une organisation locale tributaire du financement qu'elle perçoit à travers son partenariat avec une ONGI pourrait hésiter à faire part de ses préoccupations, de peur de perdre ce financement ou de mettre à mal le partenariat. Il incombe aux organisations plus puissantes de tenir compte des pressions contextuelles qui pèsent sur leurs partenaires et de veiller activement à ce que ceux-ci se sentent capables d'exprimer leur avis et leurs préoccupations sans avoir à redouter des répercussions.

Transfert du risque : définition

Le **transfert du risque** désigne l'apparition ou la transformation d'un risque (qu'il diminue ou s'accroît) pour un acteur du fait de la présence ou des actions d'un autre acteur.

Les risques de sécurité ne sont pas uniquement transférés du niveau global au niveau local. Ils peuvent aussi être transférés de l'ONG L/N à l'ONGI, et entre acteurs opérant au même niveau (voir schéma 2). Par exemple, pour une ONG L/N, le fait de s'associer à une ONGI peut lui faire courir des risques accrus dans ses opérations, car la perception des communautés et des autorités locales à l'égard de cette ONG L/N peut être affectée. Inversement, une ONGI qui noue un partenariat avec des ONG L/N peut voir son niveau de sécurité et d'acceptation affecté dans certains contextes selon la manière dont l'ONG L/N est perçue. Les risques peuvent aussi être transférés au sein-même de l'organisation, par exemple depuis les collaborateurs employés dans la capitale vers le personnel de terrain.

Schéma 2. Différentes directions du transfert de risque



Adapté de GISF – Partnerships and Security Risk Management: from the local partner's perspective

L'identité (réelle ou perçue) d'une organisation peut influencer la manière dont ses partenaires sont perçus. Cela peut impacter le transfert de risque et entraîner un risque sécurité pour le personnel des deux partenaires. L'identité d'une organisation est liée à son mandat, sa mission et ses principales activités de programmation : certaines organisations sont de nature confessionnelle, ou se spécialisent dans des programmes bien particuliers, comme la prestation de services de santé sexuelle et reproductive, par exemple. Les profils individuels des collaborateurs peuvent eux aussi affecter les risques auxquels s'exposent les partenaires (voir encadré ci-dessous).



Il est important d'étudier aussi bien les **menaces internes qu'externes pour évaluer les perceptions et les risques liés à l'identité, et la manière dont elles peuvent apparaître ou se transformer en raison du partenariat.**

Les partenaires doivent comprendre et résoudre ensemble les questions découlant du transfert du risque sécurité au sein du partenariat ; pour cela, il peut être utile que chaque acteur pose des questions pertinentes à son partenaire dès les phases initiales de leur collaboration. Il sera également judicieux d'inclure les risques susceptibles de résulter du partenariat dans un processus d'évaluation du risque sécurité et un plan de gestion de la sécurité.

► Voir section 2.3.2. pour connaître les questions clés permettant d'identifier les risques de sécurité pouvant résulter d'un partenariat



OUTIL 5. Évaluation du risque sécurité et plan de gestion de la sécurité - exemple

Profils personnels et risques connexes

Les collaborateurs présentent différents profils de risque du fait de leurs caractéristiques individuelles, visibles ou non (genre, nationalité, ethnicité, etc.). Ces caractéristiques interagissent entre elles, et se conjuguent au contexte, au rôle et à l'organisation de l'individu, ainsi qu'à l'organisation partenaire.

Les risques sont différents d'une personne à l'autre. Le profil de chaque collaborateur influe sur les menaces auxquelles il peut être confronté et sur sa **vulnérabilité** face à ces menaces. Il est important de tenir compte des différents risques auxquels le personnel fait face pendant toute la durée du partenariat.

En outre, les partenaires ne doivent pas oublier que des menaces peuvent parfois émaner de l'organisation ou du partenariat même. Par exemple, les collaborateurs d'une ONG L/N qui font partie d'un certain groupe ethnique peuvent s'exposer à des menaces internes particulières, qui ne sont pas toujours visibles, ni comprises par le personnel de l'ONGI.

Les profils individuels des collaborateurs d'une organisation peuvent être très différents – de même que leur exposition aux menaces. Il est important que les organisations ne se fient pas aux évaluations du risque sécurité et aux mesures d'atténuation de leurs partenaires, et qu'elles réfléchissent aux risques bien spécifiques auxquels leurs collaborateurs doivent faire face du fait de leur profil individuel.

► Voir 2.3.2. pour des exemples de questions pertinentes afin de traiter les risques formés par les partenariats



Complément d'information

- GISF – Partnerships and Security Risk Management: from the local partner's perspective
- Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships

1.3. Adopter les principes du partenariat

Les partenaires sont encouragés à réfléchir aux principes suivants tout au long du partenariat et à les adopter.

Équité	Transparence et confiance	Bénéfice mutuel	Complémentarité	Approche axée sur les résultats	Responsabilité
Des déséquilibres de pouvoir sont susceptibles d'exister entre les organisations locales et internationales, mais le principe d'équité assure aux deux partenaires qu'ils se trouvent sur un pied d'égalité en termes de droit à se faire entendre et à ce que leurs contributions soient valorisées de la même manière. Cette équité doit s'appuyer sur le « respect » et la « justice ». S'agissant de la gestion du risque sécurité, cela signifie par exemple que les préoccupations d'ordre sécuritaire des deux partenaires sont entendues, comprises et traitées de manière égale.	Une relation de confiance repose d'abord sur des interactions honnêtes et ouvertes, menées sur un pied d'égalité entre les partenaires. Les partenaires doivent mener des conversations ouvertes et honnêtes sur les besoins de sécurité et sur la manière la plus réaliste de les traiter. Il s'agit donc d'écouter et de faire confiance aux acteurs qui sont le plus exposés aux risques, autrement dit, dans un grand nombre de cas, au personnel de l'ONG L/N.	Il ne suffit pas de chercher à remplir les objectifs du partenariat. Il faut aussi adopter une communication de qualité et parfaitement comprendre les intérêts plus généraux de son partenaire, ses motivations et ses buts. Un renforcement actif des capacités du personnel et une prise en compte des besoins sécuritaires à long terme des deux partenaires permettront aux organisations de garantir la sécurité des programmes du partenariat, mais également d'élaborer des stratégies de gestion du risque sécurité durables qui perdureront même une fois le partenariat terminé.	Les partenaires doivent considérer la diversité comme un atout. Les activités des deux partenaires doivent s'appuyer sur le savoir et les compétences de chacun d'eux, en évitant les doublons et en cherchant activement à surmonter les barrières, notamment linguistiques ou culturelles. Les capacités et le savoir local sont des outils fondamentaux pour une gestion efficace du risque sécurité. Les stratégies de GRS d'un partenariat doivent s'appuyer sur les avantages comparatifs des deux partenaires, et les contributions doivent être complémentaires.	Les mesures prises par les partenaires doivent être réalistes et axées sur les résultats. Dans le contexte de la GRS, cela implique une coordination entre partenaires afin d'élaborer et de mettre en œuvre des mesures sécuritaires réalistes. Les activités doivent directement améliorer la sécurité et le résultat des programmes pour les deux partenaires.	Sur le plan déontologique, les partenaires doivent faire leur travail de manière responsable, appropriée et avec intégrité. Les partenaires ne devront s'engager à exécuter une mission que s'ils disposent des compétences, des connaissances, des capacités et des ressources nécessaires. Si un partenaire a le sentiment de ne pas pouvoir assumer la tâche de manière responsable en raison de défis sécuritaires, les deux partenaires devront en discuter ouvertement.

Adapté du document *Principles of Partnership* avalisé par The Global Humanitarian Platform et des principes présentés par The Partnering Initiative



Complément d'information

- *Global Humanitarian Platform – Principles of Partnership*
- *Global Mentoring Initiative – Partnerships: Pre-conditions, principles and practices*
- *The Partnering Initiative – The Partnering Cycle and Partnering Principles*

1.4. Communiquer et instaurer la confiance au sein du partenariat

La communication est essentielle à un partenariat équitable. La complexité et la sensibilité du risque sécurité ne doivent pas être prétexte à communiquer de manière vague ou en s'appuyant sur de simples hypothèses.

Les partenaires doivent être encouragés à s'interroger les uns les autres et se sentir en mesure de demander des informations pour améliorer leur compréhension mutuelle. À cette fin, et pour instaurer la confiance, les personnels en contact avec les partenaires devront :

1. **Faire preuve d'une véritable attention** : en remettant en question leurs éventuels préjugés et partis pris avant d'entamer toute conversation.
2. **Écouter pour mieux comprendre et non pour mieux répondre.**
3. **Rechercher des points communs afin de construire la relation** : identifier les objectifs et les intérêts communs qui serviront de base.
4. **Accepter les différences tant que l'existence de points communs n'a pas été démontrée** : ne pas supposer que les deux partenaires interprètent tout de la même manière. Chacun doit tenir compte de la culture et des traditions de l'autre pour renforcer la cohérence du message.
5. **Faire preuve d'empathie** : dire la vérité avec compassion et prendre en compte les circonstances du partenaire susceptibles d'affecter sa relation avec vous (p. ex. circonstances personnelles, contexte, besoins).
6. **Faire preuve de transparence et établir des attentes justes** : présenter honnêtement les contraintes et les limites avec lesquelles le partenaire doit œuvrer, sans promesses excessives.
7. **Être positif et respectueux** : insister sur les objectifs communs pour instaurer une cohésion entre vous et votre partenaire.
8. **Distinguer les personnes du problème** : parler des problèmes avec votre partenaire, sans rejeter la responsabilité sur lui.
9. **Choisir le bon moment, le bon endroit et la bonne méthode pour communiquer** : tenir compte de la culture du partenaire (p. ex. traditions orales/traditions écrites) et rendre accessibles les informations importantes. Veiller à ce que le mode de communication soit sécurisé et que les deux partenaires se sentent à l'aise pour l'employer.
10. **Dire ce que l'on veut faire, faire ce que l'on dit** : assumer ses actes

et ses paroles, ce qui sous-entend de reconnaître ses erreurs et les malentendus.

11. **Demander et recevoir un retour pour favoriser une plus grande autonomie** : aussi bien de manière anonyme que directe pour montrer au personnel qu'il peut s'exprimer sans crainte.
12. **Communiquer de manière claire et spécifique** : expliquer clairement ce qui est attendu du partenaire en termes de communication.
13. **Communiquer régulièrement**, notamment en période d'incertitude.

Les organisations doivent toujours adapter leur stratégie de communication au contexte et aux individus concernés.



« Dans certains contextes, on ne peut pas employer le terme 'sécurité' car il est associé aux services de renseignements et pourrait exposer le partenaire local à un risque supplémentaire vis-à-vis des autorités de l'État. »

Un collaborateur d'une ONG L/N



Pour mener à bien ces conversations, les partenaires devront disposer d'un interlocuteur qui comprend non seulement les langues parlées par les deux partenaires, mais également leur culture, et qui pourra servir d'interprète.

Veillez à impliquer les bons individus dans la conversation. Demandez-vous aussi à quel niveau cette conversation doit se dérouler : faut-il uniquement impliquer du personnel du siège de l'organisation et de son principal bureau pays, ou également des collaborateurs du bureau local et/ou de terrain ?



« Au siège, nous prévoyons toute une série de mesures pour améliorer les accords de partenariat, mais sur le terrain, tout cela risque de capoter si des membres du personnel national communiquent mal avec les partenaires locaux et perpétuent une structure du pouvoir descendante. »

Un collaborateur d'une ONGI



Les organisations doivent veiller à ce que les techniques de communication fassent partie de la formation du personnel ou constituent un aspect de l'évaluation de la performance des employés.



OUTIL 1. Une communication de qualité au sein du partenariat

Les accords de partenariat et les méthodes de communication doivent aussi tenir compte du fait que des formes de discriminations et préjugés inconscients ou non, sont courantes entre partenaires, et au sein du secteur de l'aide d'une manière générale. Ici, les préjugés désigne la tendance d'un groupe particulier à avoir un avis ou des inclinaisons en faveur (ou à l'encontre) d'un autre groupe, sur la base de la race, de l'ethnicité et d'autres aspects identitaires, comme la nationalité.

► *Voir le glossaire pour de plus amples renseignements sur les différents partis pris*

Un partenaire qui agit de manière biaisée peut gravement impacter les relations et la communication au sein du partenariat, surtout lorsqu'il existe déjà un déséquilibre des pouvoirs et un manque de confiance. Les deux partenaires doivent s'interroger sur l'éventuelle présence de préjugés, conscients ou inconscients.

Exemple de partialité

Dans le secteur de l'aide, on peut voir une certaine partialité dans la manière dont les normes sécuritaires s'appliquent à différents groupes de personnel. Dans un exemple tiré de précédents travaux de GISF, les collaborateurs d'une ONG L/N percevaient moins d'argent que leurs collègues d'une ONGI pour leurs déplacements. Le personnel de l'ONG L/N devait donc faire des compromis sur son logement, contrairement aux partenaires de l'ONGI.

Complément d'information

- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*
- *The Partnering Initiative – Talking the Walk: A Communication Manual for Partnership Practitioners*
- *Global Mentoring Initiatives Resources*
- *Aid Reimagined*
- *Race Forward*

1.5. Explorer les attitudes face au risque sécurité au sein du partenariat

Le risque peut être atténué (réduit) de différentes manières. Par exemple, on peut réduire le risque d'accidents de la route en entretenant les véhicules et en formant les conducteurs, notamment aux procédures d'urgence. Le risque d'accidents de la route diminuera, certes, mais il restera présent. C'est ce que l'on appelle le **risque résiduel**. L'attitude d'une organisation face au risque désigne le risque résiduel qu'elle est prête à accepter (on parle ici d'« acceptation du risque » ou de « seuil de risque atteint »).



La décision d'accepter les risques de sécurité n'est pas toujours prise sur un pied d'égalité selon qu'il s'agit d'une ONGI ou d'une ONG L/N.

Acceptation du risque, attitude face au risque et seuil de risque

L'**acceptation du risque**, l'**attitude face au risque** et le **seuil de risque** sont des termes qui désignent le niveau de risque qu'une organisation est disposée (ou obligée) à accepter pour remplir ses objectifs.

Il est impératif que les partenaires comprennent, étudient et communiquent sur la question de l'attitude face au risque des deux organisations. Ce point est essentiel pour assurer l'équité du partenariat. Les partenaires doivent respecter les préoccupations de chacun ; ils doivent aussi savoir qu'une **accoutumance au risque** peut s'instaurer et que les organisations peuvent se sentir contraintes de dépasser leur seuil de risque pour continuer d'opérer.

Les principes déontologiques suivants aideront les organisations partenaires à évaluer leur propre attitude face au risque :

1. **Criticité** : à quel point le programme joue-t-il un rôle critique ?
2. **Ne pas nuire** : quels préjudices un incident de sécurité pourrait-il causer ?
3. **Autonomie** : les collaborateurs des deux partenaires (surtout ceux qui présentent le risque le plus élevé) ont-ils donné leur accord de manière libre et éclairée pour assumer les risques de sécurité, ou le partenariat a-t-il joué un rôle dans cette décision ?
4. **Bonne utilisation des ressources** : l'organisation se sert-elle des ressources de manière responsable ?



5. **Équité** : les partenaires se traitent-ils mutuellement de manière équitable ?
6. **Fidélité** : les partenaires sont-ils fidèles à leur vision et leurs rôles institutionnels et professionnels respectifs ?

L'**attitude face au risque** de chaque partenaire doit être abordée dès le début du partenariat – puis revisitée régulièrement.

OUTIL 2. Attitude face au risque au sein du partenariat

Complément d'information

- GISF – *Partnerships and Security Risk Management: from the local partner's perspective*
- EISF – *Security Risk Management and Capacity Development: International agencies working with local partners (en particulier, « Figure 3: Framework for ethical decision-making »)*
- EISF – *Risk Thresholds in Humanitarian Assistance*

2

Réaliser un examen conjoint des processus de gestion du risque sécurité au sein du partenariat

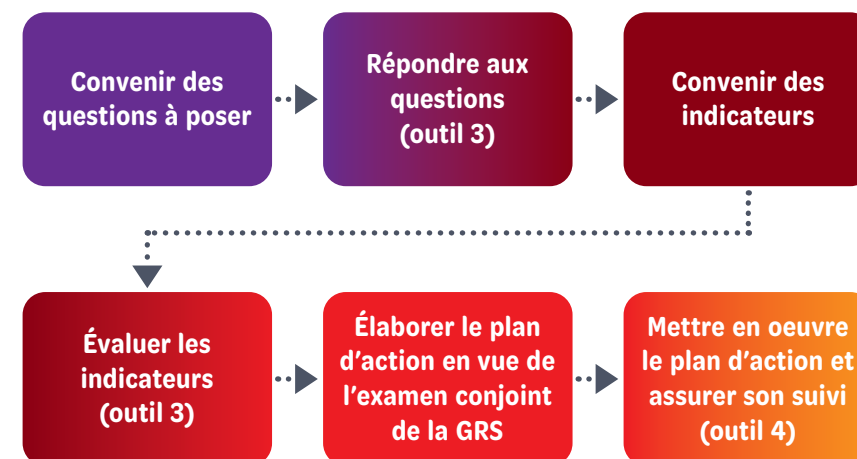
2.1. L'examen conjoint de la GRS

Pour un partage équitable des responsabilités sécuritaires, les partenaires doivent s'aider mutuellement à gérer les risques de sécurité. Dans un premier temps, il s'agit de mener des discussions ouvertes, honnêtes et constructives sur la manière dont chaque partenaire conçoit et gère ses risques de sécurité, et appuie la stratégie de l'autre en matière de gestion du risque sécurité. Ce guide décrit l'examen conjoint de la gestion du risque sécurité qu'il faudra réaliser pour appuyer ces conversations. L'**examen conjoint de la GRS** est un processus qui comporte deux grandes étapes :

1. Étudier la manière dont chaque organisation comprend et appréhende la gestion du risque sécurité et identifie les lacunes et défis ;
2. Prendre des mesures conjointes pour combler les lacunes et surmonter les défis auxquels chaque partenaire est confronté dans sa gestion de la sécurité ; il s'agira ici d'élaborer et de mettre en œuvre un **plan d'action en vue de l'examen conjoint de la GRS**.

L'examen conjoint de la GRS commence par un questionnaire. Les réponses permettront de choisir les principaux indicateurs. Les partenaires doivent ensuite évaluer ces indicateurs pour savoir quels éléments existent déjà, et lesquels sont encore absents. Cette évaluation servira de point de départ pour élaborer un plan d'action assorti d'une liste d'actions propres à améliorer la coordination des deux partenaires en matière de GRS. Les deux partenaires devront ensuite veiller au suivi régulier de ce plan d'action. (Voir le schéma 3 pour connaître les différents éléments du processus d'examen conjoint de la GRS.) Ce guide propose également des outils pour faciliter les différentes étapes du processus, mises en évidence dans le schéma 3.

Schéma 3. Étapes de l'examen conjoint de la GRS



Le **cadre de gestion du risque sécurité** ci-dessous présente les différents éléments de l'examen conjoint de la GRS (voir schéma 4). Les partenaires sont vivement encouragés à s'y référer lors de leurs discussions.

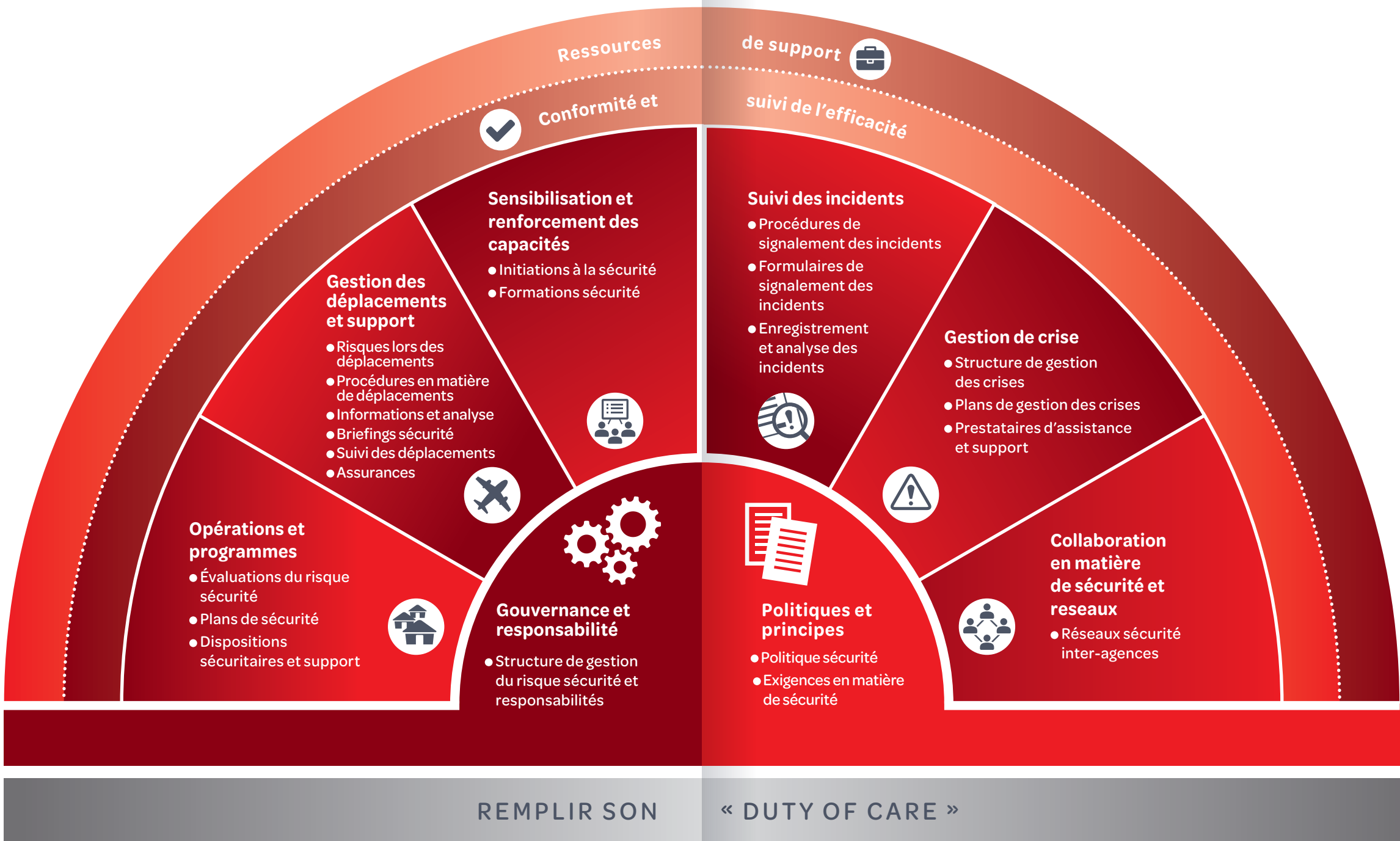
Gérer les véritables risques de sécurité

L'examen conjoint de la GRS permet de réfléchir aux stratégies de gestion du risque sécurité au sein du partenariat. Il s'agit donc d'un « outil de gestion du partenariat » et non d'un « outil de gestion du risque sécurité ».

À l'issue de l'examen conjoint de la GRS, les partenaires étudieront les véritables risques de sécurité auxquels leur personnel, leur organisation et le partenariat sont exposés, tels que les accidents de la route ou les attaques visant des collaborateurs. Il est possible pour cela de réaliser une **évaluation conjointe du risque sécurité** et de développer un **plan conjoint de gestion du risque sécurité**. Ces « outils de gestion du risque sécurité » sont abordés de manière plus détaillée dans la troisième partie de ce guide.

► Voir 3.1, Identifier et répondre ensemble au risque sécurité

Schéma 4. Cadre de gestion du risque sécurité



Source: EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG

2.2. Planifier la stratégie

Les partenaires doivent commencer par planifier leur stratégie, et ainsi :

- Convenir du fait que l'amélioration de la GRS est l'objectif de cet examen.
- Convenir des dates/horaires auxquels les partenaires pourront mener leurs discussions.
- Convenir du mode de déroulement de l'examen.

L'examen conjoint de la GRS devra être adapté en fonction des circonstances des organisations partenaires et de différents facteurs – par exemple, la relation de chaque partenaire avec les communautés et les autres acteurs avec lesquels il travaille, son attitude face au risque et sa capacité à répondre aux défis en matière de risque sécurité, le type d'activités, etc.

Pour un partenariat de longue durée, un examen conjoint de la GRS doit dans l'idéal être réalisé tous les deux ans, voire plus souvent si le contexte est fragile. Les partenaires pourront également en effectuer un en cas de changement significatif de contexte opérationnel susceptible d'affecter la mise en œuvre des programmes, ou en cas de changement au niveau de la relation entre les partenaires (p. ex. en cas d'élargissement des opérations). Les éléments déclencheurs de ces discussions devront être identifiés par les partenaires.

Dans l'idéal, la majorité des discussions relatives à la gestion du risque sécurité doivent avoir lieu avant la conclusion du partenariat. Si cela n'est pas possible, les organisations devront mener ces discussions dès que possible et tout au long du partenariat.

Il est également important de tenir compte des autres évaluations susceptibles de se dérouler en même temps au sein du partenariat. Les organisations locales ont souvent à gérer une multitude d'attentes de la part de leurs différents partenaires d'ONGI et départements d'une même ONGI, non seulement dans le domaine de la sécurité, mais également dans celui de la gestion du risque d'une manière plus générale, notamment du risque financier.



En raison des susceptibilités autour des questions de sécurité, le personnel d'ONG L/N préférera peut-être parler de ses défis et préoccupations en face à face plutôt que par écrit.

Les partenaires doivent s'interroger sur les meilleurs individus à impliquer. Il peut par exemple s'agir de membres de la direction, de collaborateurs

chargés de la sécurité ou de points focaux du partenariat. À noter toutefois que d'autres personnels peuvent aussi apporter un éclairage intéressant, par exemple les collaborateurs en charge de programmes à haut risque, et les employés assumant des responsabilités dans les domaines de la finance et/ou du plaidoyer.

► *Voir la quatrième partie pour en savoir davantage sur le rôle du plaidoyer*

Adapter la stratégie en fonction des facteurs externes

Les organisations partenaires doivent adapter la stratégie présentée dans ce guide afin de répondre aux opportunités et aux limites résultant de la nature même du partenariat, et en fonction du contexte et d'autres circonstances telles que les défis environnementaux (p. ex. épidémie et insécurité). Ces adaptations peuvent revêtir différentes formes :

- Organiser des ateliers à distance par téléphone ou en ligne, en veillant à ce que toutes les parties prenantes aient accès au mode de communication ou à la plateforme employée.
- Faire preuve de souplesse en réagissant rapidement face aux changements ayant trait à l'environnement, à la **sûreté** et à la **sécurité**.
- Veiller à ce que toutes les parties prenantes aient conscience des risques susceptibles d'impacter l'application de cette stratégie et soient prêtes à y répondre et/ou à s'adapter en fonction de la **vulnérabilité** des individus impliqués.
- Veiller à assurer une communication régulière et pertinente avec toutes les parties prenantes, et tenir ouvertes toutes les voies de communication afin de promouvoir la souplesse et la capacité d'adaptation.

L'une des mesures proactives peut consister à explorer les besoins des deux partenaires à long terme et à instaurer des structures de partenariat solides et une relation de confiance pour encourager la résilience face aux futurs incidents et crises.

2.3. Remplir le questionnaire et évaluer les indicateurs

Les partenaires doivent d'abord se mettre d'accord sur les questions clés à poser afin de mieux comprendre ce qu'implique la gestion du risque sécurité pour chaque organisation et pour le partenariat dans son ensemble.

Les réponses à ces questions serviront à élaborer des indicateurs clés pour le partenariat, ou pour chaque organisation partenaire. Ces indicateurs peuvent être « présents », « partiellement présents » ou « absents ». Les partenaires devront convenir d'une définition pour chaque « catégorie d'évaluation ». Par exemple, « présent » signifie-t-il que l'indicateur a été documenté, que le responsable confirme qu'il est bel et bien en place, ou que plusieurs collaborateurs confirment son existence ?

Vous trouverez ci-après des exemples de questions et d'indicateurs classés en fonction des différents éléments du **cadre de gestion du risque sécurité** présenté au point 2.1. Ils ne sont donnés qu'à titre indicatif, et devront être modifiés selon les circonstances de chaque partenariat.



OUTIL 3. Modèle de questionnaire et de feuille de travail en vue de l'examen conjoint de la GRS, pour répondre aux questions et évaluer les indicateurs. Cet outil peut également être téléchargé sous format modifiable sur www.gisf.ngo

Le chapitre suivant présente point par point le questionnaire dédié à l'examen conjoint de la GRS, avec des explications et des questions supplémentaires que certaines organisations souhaiteront éventuellement aborder.

Questions préliminaires relatives à la gestion du risque sécurité pour les partenaires

Les partenaires qui ne sont pas en mesure de compléter l'examen dans son intégralité, par exemple parce qu'ils n'en sont encore qu'à un stade précoce du partenariat, peuvent commencer par réfléchir aux questions préliminaires suivantes :

Questions préliminaires à l'attention des partenaires concernant la gestion du risque sécurité	
Duty of care	• Quelles sont les obligations légales et morales (duty of care) respectives de chaque partenaire ?
Gouvernance et responsabilité	• Les deux partenaires ont-ils contribué aux principales prises de décisions (p. ex. réunions) concernant le programme, le projet, le partenariat et/ou la sécurité ? • Les deux partenaires disposent-ils de structures de gestion du risque sécurité (y compris rôles et responsabilités) adaptées aux objectifs du partenariat ? • L'accord de partenariat traite-t-il des risques de sécurité et de leur gestion ?

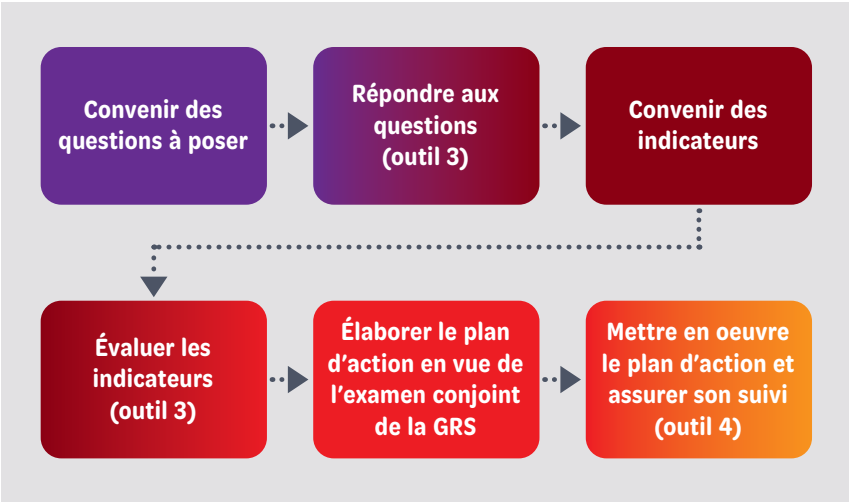
Questions préliminaires à l'attention des partenaires concernant la gestion du risque sécurité suite	
Transfert du risque	• Comment les partenaires sont-ils perçus par les parties prenantes avec lesquelles ils entretiennent des relations et dont ils dépendent pour leur bon fonctionnement ? • Dans quelle mesure le partenariat modifie-t-il le degré de vulnérabilité de chaque organisation et de son personnel face aux menaces existantes ? L'identité perçue d'une organisation joue-t-elle un rôle à cet égard ? • Le partenariat fait-il apparaître de nouvelles menaces ? • Le partenariat modifie-t-il la probabilité qu'une menace particulière se produise, ou son impact ? Si oui, est-ce une bonne ou une mauvaise chose ?
Politiques et principes	• Les deux partenaires comprennent-ils parfaitement le mandat, la mission, les valeurs et les principes de chaque organisation, et se sentent-ils à l'aise avec le travail de l'autre et son approche des opérations et de la sécurité (p. ex. les deux partenaires sont-ils d'accord avec leurs positions respectives concernant le plus strict respect des principes humanitaires) ?
Opérations et programmes	• Quels sont les besoins et attentes de chaque partenaire en matière de sécurité ? • Les partenaires se sont-ils mis d'accord sur un système permettant d'identifier et d'évaluer les risques de sécurité auxquels leurs personnels sont confrontés ? • Les partenaires se sont-ils mis d'accord sur les individus à qui confier la gestion des risques identifiés, et sur la manière dont ces individus doivent être supervisés et financés ? • Existe-t-il un système permettant d'alerter les deux partenaires en cas de risques de sécurité et de changements dans le contexte ? • Chaque partenaire dispose-t-il de ressources suffisantes (humaines, temporelles et financières) pour gérer les risques de sécurité ?
Approches inclusives de la gestion du risque sécurité	• L'approche de gestion du risque sécurité des deux organisations tient-elle compte de la manière dont l'identité des collaborateurs peut affecter leur vulnérabilité face aux menaces ? • Comment les partenaires doivent-ils aborder les sujets identitaires sensibles, par exemple les menaces internes et externes basées sur l'orientation sexuelle ou le genre ? Quel est le niveau de « confort » des partenaires à cet égard (en tenant compte des sensibilités culturelles) ? • Comment les partenaires peuvent-ils s'aider à sortir de leur zone de confort pour assurer une gestion efficace du risque sécurité pour l'ensemble du personnel ?
Menaces internes et mesures de sauvegarde ²	• De quelle manière les partenaires comptent-ils gérer les menaces de sécurité susceptibles d'émaner des organisations partenaires (p. ex. de leur personnel) ? • Comment la question de la sauvegarde est-elle envisagée au sein du partenariat ? Existe-t-il des mécanismes de signalement appropriés pour le personnel de chaque partenaire, les bénéficiaires du programme et les membres de la communauté ?

2. Les mesures de 'sauvegarde' réfèrent au terme anglais de 'safeguarding'.

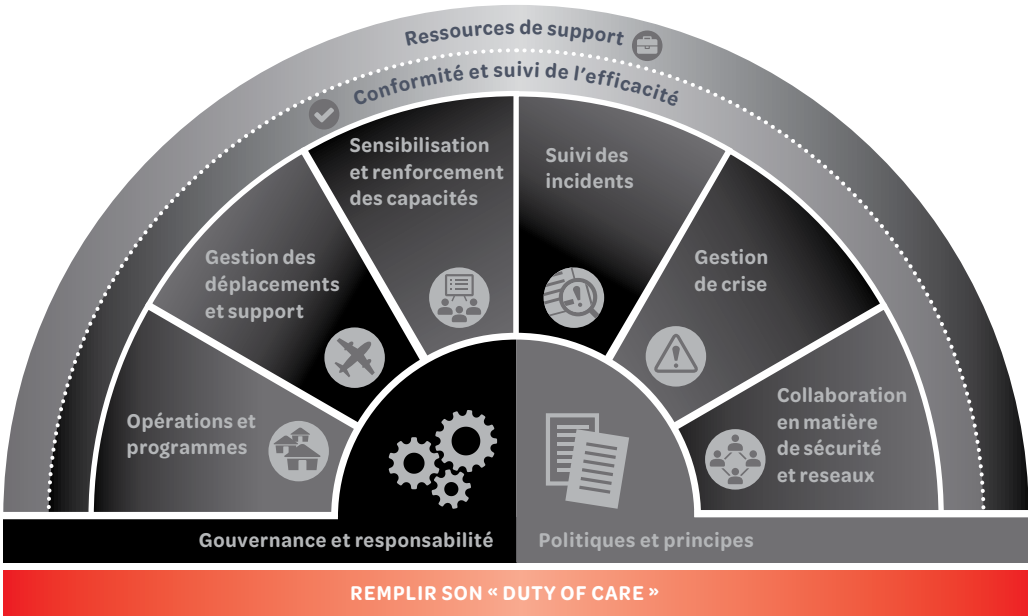
Questions préliminaires à l'attention des partenaires concernant la gestion du risque sécurité <i>suite</i>	
Déplacements	• Comment prendre en charge les risques de sécurité résultant des déplacements effectués pour les besoins du partenariat ?
Sensibilisation et renforcement des capacités	• Comment les partenaires comptent-ils identifier les besoins en matière de sensibilisation et de renforcement des capacités et travailler ensemble (tant pour la gestion de la sécurité générale que de la sécurité personnelle) ?
Suivi des incidents	• Les partenaires doivent-ils transmettre l'information sur les incidents à l'autre partie et, si oui, de quelle manière ?
Gestion de crise	• De quelle manière les partenaires comptent-ils collaborer/coordonner leurs actions en cas de crise ou d'incident critique affectant l'une ou l'autre organisation là où le partenariat est actif ?
Collaborations et réseaux dans le domaine de la sécurité	• Existe-t-il des plateformes dans le contexte particulier du partenariat qui permettent d'aborder les questions sécuritaires ? • Si oui, les deux partenaires ont-ils accès de manière égale à ces plateformes et réseaux de coordination dans leurs zones opérationnelles, y compris aux plateformes de partage de l'information sécuritaire ?
Conformité et suivi de l'efficacité	• Comment les partenaires comptent-ils régulièrement passer en revue la gestion du risque sécurité au sein du partenariat ?
Ressources	• Chaque partenaire permet-il à l'autre partie d'accéder à ses ressources dédiées à la gestion du risque sécurité ?
Fin du partenariat	La fin du partenariat conformément au contrat (et aux échéances financières) a-t-elle des implications sur la sécurité de chaque partenaire ? Si oui, comment y répondre ?



Rappel: Suivez l'organigramme ci-après pour effectuer l'examen.



2.3.1. Duty of care



Les obligations de sécurité communément appelées **duty of care** dans le secteur humanitaire sont essentielles pour bien comprendre les obligations et les attentes de chaque partenaire envers son personnel. Il est également important de vérifier que les partenaires ont la même conception du duty of care, d'autant plus qu'ils ne connaîtront pas forcément tous ce terme.

Le duty of care pour l'organisation

Le **duty of care** est un terme anglais utilisé aussi bien dans des contextes anglophones que francophones pour désigner l'obligation légale et morale d'une organisation de prendre toutes les mesures possibles et raisonnables afin de réduire le risque de préjudice causé à ceux qui travaillent pour elle ou en son nom. Il s'applique aussi bien dans les contextes à haut risque qu'à faible risque. Bien que, généralement, le **duty of care** porte surtout sur les obligations légales, les partenaires se devront aussi d'envisager leurs obligations morales à l'égard de leur personnel. Cela concerne toute action (ou inaction) allant au-delà des obligations légales de l'organisation pour assurer le bien-être de tout individu affecté par les activités de l'organisation.

suite à la page suivante

Le *duty of care* pour l'organisation *suite*

Fondamentalement, le *duty of care* implique généralement de :

- Connaître les risques auxquels s'exposent les individus dont l'organisation a la responsabilité.
- Instaurer des mesures d'atténuation du risque pour gérer les risques identifiés.
- Élaborer des plans d'urgence.
- Veiller à ce que le personnel comprenne les risques auxquels il peut être confronté et les mesures en place pour les appréhender.
- Veiller à ce que les collaborateurs prennent des décisions éclairées sur les risques associés à leur rôle.
- Apporter un soutien approprié en cas d'incident sécuritaire.

Exemples de questions

- 1.1. Quelles sont les obligations légales et morales (*duty of care*) respectives de chaque partenaire ?
- 1.2. Quelles sont les obligations légales et morales (*duty of care*) de chaque partenaire à l'égard de son personnel, de ses bénéficiaires et des communautés affectées ?
- 1.3. Les besoins psychosociaux de l'ensemble du personnel sont-ils pris en compte, et quelles mesures chaque partenaire peut-il prendre pour améliorer le *duty of care* dont bénéficie le collaborateur (p. ex. assurance, bien-être psychosocial) ?
- 1.4. Les deux partenaires comprennent-ils ce en quoi consiste le *duty of care* – en termes d'obligations aussi bien légales que morales – et en ont-ils la même conception ?
- 1.5. Le fait de mettre un terme au partenariat conformément au contrat (et à l'échéancier financier) aura-t-il des implications sur la sécurité de chaque partenaire ? Si oui, comment y remédier ?

Exemples d'indicateurs

- 1.1. Les deux partenaires comprennent et remplissent leurs obligations légales au titre du *duty of care*.
- 1.2. Les deux partenaires se sont mis d'accord sur les obligations morales au titre du *duty of care*.



Duty of care : étapes suivantes et complément d'information

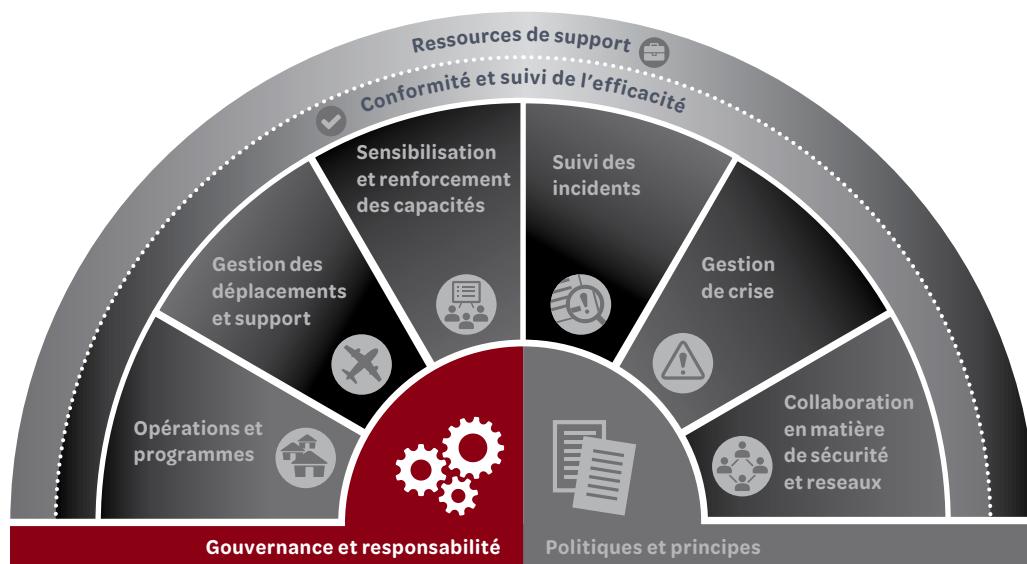
Les partenaires pourront aussi :

- Faire part de leurs politiques de *duty of care* à l'autre partenaire et y ajouter un paragraphe couvrant le *duty of care* dans le cadre du partenariat (s'ils disposent d'une telle politique).
- Dresser ensemble une liste des prestataires proposant un soutien psychosocial approprié sur les plans culturel et linguistique, qui sera ensuite diffusée auprès du personnel des deux organisations.

Complément d'information :

- *cinfo – Duty of Care Maturity Model Tool*
- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *EISF – Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*
- *EISF et cinfo – Duty of care under Swiss law and Duty of Care Maturity Model*
- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*

2.3.2. Gouvernance et responsabilité



Les structures dédiées à la bonne gouvernance et à la responsabilité sont essentielles pour une gestion efficace du risque sécurité. Il est important que les deux partenaires disposent de structures axées sur la gestion du risque sécurité, tout en tenant compte des différences en matière de pratiques et de capacités des deux organisations.

Pour partir sur de bonnes bases, les organisations auront intérêt à déterminer la **propriété du risque** à un stade précoce du partenariat ainsi que les responsabilités de chaque partenaire. Le partage des responsabilités relatives au risque sécurité peut se faire de manière stratégique et nécessite une évaluation des profils de risque des partenaires ainsi que de leur complémentarité.



Les accords relatifs à la gestion du risque sécurité devront être adaptés en fonction du type de partenariat.

Exemples de questions

2.1. Les deux partenaires disposent-ils de structures adéquates pour gérer le risque sécurité qui permettent d'atteindre les objectifs du partenariat ?

2.2. Les deux partenaires comprennent-ils parfaitement les rôles et responsabilités associés à la gestion du risque sécurité au sein du partenariat et à la mise en œuvre des programmes ? Par exemple, les deux organisations ont-elles un responsable de sécurité pouvant servir de référent principal des partenaires en cas de questions relatives à la sécurité ?

2.3. De quelle manière chaque partenaire conçoit-il le **transfert du risque** au sein du partenariat (le cas échéant) ? Quelles mesures chaque partenaire estime-t-il pouvoir prendre pour passer du transfert du risque au **partage du risque** ? (Voir encadré ci-après pour découvrir des questions spécifiques sur le transfert du risque.)

2.4. A-t-il été convenu d'une procédure de signalement des préoccupations qui tient responsable chaque partenaire si les besoins en matière de GRS au sein du partenariat ne sont pas remplis ?

2.5. Que peuvent faire les deux partenaires pour encourager une **culture de la sécurité** parmi leurs employés, notamment par des discussions et des sessions de sensibilisation à la sécurité ?

2.6. Les rapports entre les risques de sécurité et les autres risques (financiers, juridiques, administratifs) sont-ils bien compris ? Les collègues qui travaillent sur ces autres catégories de risque ont-ils connaissance des stratégies de gestion du risque sécurité mises en œuvre par les partenaires ?

2.7. Les deux partenaires ont-ils contribué aux principales prises de décisions (p. ex. réunions) concernant le programme, le projet, le partenariat et/ou la sécurité ?

2.8. L'accord de partenariat fait-il mention des risques de sécurité et de leur gestion ?

Questions clés pour comprendre les risques de sécurité pouvant découler d'un partenariat

Pour identifier les risques susceptibles de découler d'un partenariat, les organisations doivent s'interroger en interne et mutuellement sur les points suivants :

- Comment les partenaires sont-ils perçus par les parties prenantes avec lesquelles chacun d'eux entretient des relations et dont il dépend pour son bon fonctionnement ?
- Certains aspects identitaires de l'organisation ont-ils un impact sur celle-ci et sur la vulnérabilité de son personnel face aux menaces ?
- Le partenariat provoque-t-il de nouvelles menaces ?
- Le partenariat modifie-t-il la probabilité qu'une menace particulière se produise, ou son impact ? Si oui, est-ce une bonne ou une mauvaise chose ?
- Lorsqu'elle étudie les mesures d'atténuation et les stratégies de sécurité, une organisation peut-elle prendre des mesures particulières pour réduire le risque auquel son partenaire est confronté ?

► Voir 1.2, Comprendre et résoudre la question du transfert du risque sécurité entre partenaires

Exemples d'indicateurs

- 2.1. Il existe une déclaration de responsabilité et de gouvernance relative à la gestion du risque sécurité au sein du partenariat.
- 2.2. Il existe un processus de signalement et de responsabilité (dont le contenu et la fréquence ont été définis) pour informer chaque partenaire en cas de problème lié au risque sécurité. Les responsabilités des deux partenaires à l'égard de la gestion de la sécurité au sein du partenariat y sont clairement définies.
- 2.3. Les deux partenaires disposent d'un point focal explicitement désigné, qui est chargé de la gouvernance du risque sécurité pour l'organisation et le partenariat.

Gouvernance et responsabilité – étapes suivantes et complément d'information

Les partenaires pourront aussi :

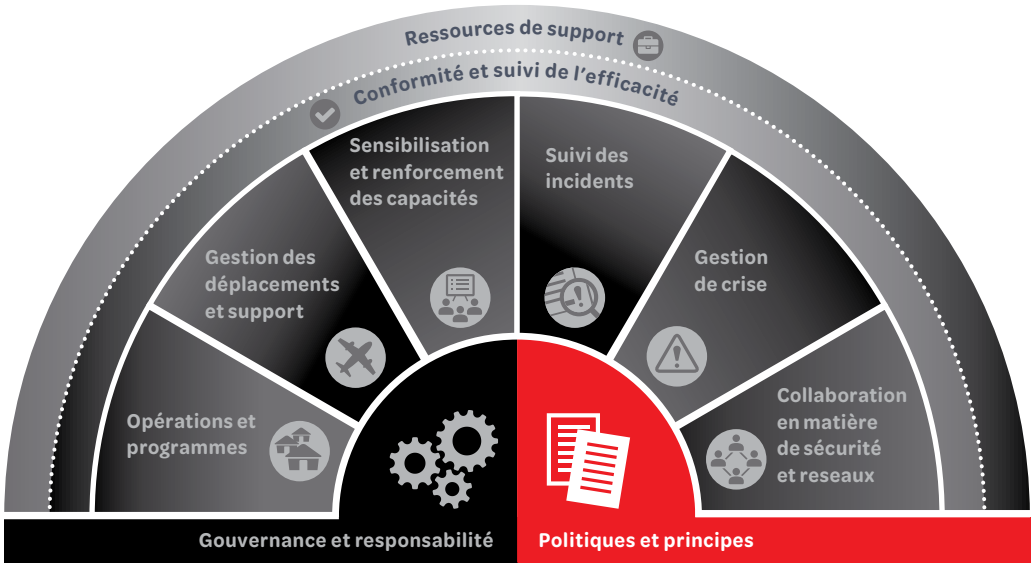
- Créer un organigramme (indiquant les noms/coordonnées/responsabilités) du personnel chargé des questions sécuritaires au sein du partenariat.
- Encourager une culture positive de la sécurité parmi le personnel (voir par exemple « 11 mesures pour instaurer une culture positive de la sécurité » dans EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG (p. 12)).
- Prévoir une réunion récurrente avec le personnel des deux organisations travaillant sur différents risques afin de répertorier régulièrement les intersections et les répercussions des différents risques pour les deux organisations.

Complément d'information :

- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *GISF – La sécurité en pratique*
- *Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships*



2.3.3. Politique et principes



La stratégie de GRS des deux partenaires doit s'appuyer sur une politique de sécurité organisationnelle. Cette politique sert à renseigner le personnel sur les principes et approches de l'organisation en matière de gestion du risque sécurité et indique les responsabilités du personnel dans ce domaine. Les partenaires devront comparer entre eux leurs principes et approches de GRS. Il est particulièrement important que les partenaires parlent ensemble de leur **attitude face au risque**, de leur **accoutumance au risque** et de leur approche globale en matière de sécurité, y compris de leurs principes humanitaires.

► Voir 1.5, Réfléchir aux attitudes face au risque sécurité au sein du partenariat



OUTIL 2. Attitude face au risque au sein du partenariat

Exemples de questions

3.1. Les deux partenaires comprennent-ils parfaitement le mandat, la mission, les valeurs et les principes de chaque organisation, et se sentent-ils à l'aise avec le travail de l'autre partenaire et son approche à l'égard des opérations et de la sécurité (p. ex. les partenaires sont-ils d'accord avec leur position respective concernant le plus strict respect des principes humanitaires) ?

3.2. Les partenaires sont-ils d'accord sur les exigences sécuritaires minimales concrètes devant être en place sur chaque site ou pour chaque activité ? (Bien que ces exigences s'appliquent aux deux partenaires, elles doivent aussi être réalistes et adaptées aux capacités de chaque organisation.)

3.3. De quelle manière les partenaires définissent-ils et appréhendent-ils l'attitude face au risque, et sont-ils d'accord sur ce qui constitue un **seuil de risque** acceptable pour le partenariat et les programmes connexes ?

3.4. Comment les partenaires perçoivent-ils l'accoutumance au risque, et les partenaires peuvent-ils s'entraider sur ce point ?

3.5. Quels sont les rapports entre l'attitude face au risque, la criticité du programme et les capacités de gestion du risque sécurité au sein du partenariat ?

3.6. Les principes et objectifs sur lesquels s'appuie le partenariat sont-ils acceptés et compris par les partenaires ?

Exemples d'indicateurs

3.1. Les politiques de gestion du risque sécurité et leur mise en œuvre (au moyen de plans, de procédures et/ou de directives) sont adaptées au contexte local et aux circonstances du partenariat, et tout le personnel peut y accéder (p. ex. elles sont disponibles dans des langues et sous un format pertinent).

3.2. L'accord de partenariat comprend une déclaration commune relative au seuil de risque régissant les activités du partenariat.

3.3. L'accord de partenariat est conforme aux politiques de sécurité des deux partenaires, voire les renforce (p. ex. dispositions relatives à l'emploi d'escortes armées).



Politique et principes – étapes suivantes et complément d'information

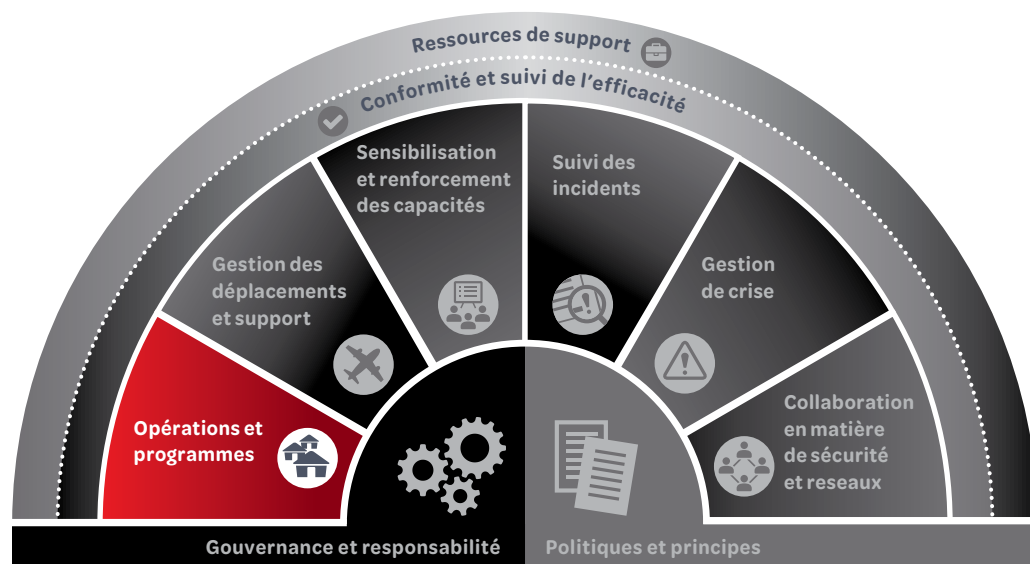
Les partenaires pourront aussi :

- Partager le mandat, la mission, les valeurs, les principes et les politiques de sécurité de chaque organisation et débattre ensemble de leurs points communs et différences (sont-ils comparables ou existe-t-il des tensions importantes ?).
- Dresser une liste des signaux d'alerte en termes de risques de sécurité et des mesures d'atténuation à aborder avant leur mise en œuvre, surtout si ceux-ci concernent les principes et les politiques (par exemple, l'emploi d'escortes armées).
- Discuter de leur attitude face au risque et décider d'une méthode de signalement des préoccupations lorsque le seuil d'un partenaire est atteint.
- Organiser des actions de sensibilisation pour que tout le personnel comprenne les concepts d'**accoutumance au risque** et d'**acceptation du risque**, et puisse faire part de ses éventuelles préoccupations.

Complément d'information :

- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *EISF – Risk Thresholds in Humanitarian Assistance*

2.3.4. Opérations et programmes



Il est essentiel que les programmes soient mis en œuvre de manière efficace. Les partenaires devront se mettre d'accord sur le meilleur moyen de gérer les risques de sécurité découlant de leurs activités. Des plans réalistes, des procédures et des ressources devront être déployés pour contribuer à l'analyse de l'environnement opérationnel et à l'identification du risque sécurité pour le personnel et les opérations.

Cela permettra de déterminer les stratégies et mesures les plus efficaces pour gérer les risques de sécurité dans le contexte opérationnel.



Si possible, effectuez une *évaluation conjointe du risque sécurité* pour chaque contexte opérationnel.

► Voir 3.1, *Identifier et répondre ensemble au risque sécurité*



OUTIL 5. Modèle d'évaluation et de plan de gestion conjoints du risque sécurité

Une bonne gestion du risque sécurité repose sur la collaboration d'un large éventail de collègues. Les membres des services Programmes et Finances doivent être impliqués, si nécessaire, dans les discussions sur

l'identification et l'atténuation des risques, et pour veiller à ce que la gestion du risque sécurité soit incluse dans les budgets du partenariat et du projet.

► Voir 3.2, *Financer la gestion du risque sécurité au sein du partenariat*



OUTIL 6. Modèle de budget dédié à la gestion du risque sécurité au sein du partenariat

Exemples de questions

- 4.1. Quels sont les besoins et attentes de chaque partenaire en matière de sécurité ?
- 4.2. Les partenaires se sont-ils mis d'accord sur un système permettant d'identifier et de contrôler les risques de sécurité auxquels le personnel est exposé ? (Constate-t-on une cohérence entre les **évaluations du risque sécurité** et les plans de sécurité des deux organisations sur les sites où opère le partenaire d'exécution ? Quelles sont les divergences, et pourquoi ?)
- 4.3. Les partenaires se sont-ils mis d'accord sur les individus à qui confier la gestion des risques identifiés, et sur la manière dont ces individus doivent être supervisés et financés ?
- 4.4. Existe-t-il un système permettant d'alerter les deux partenaires en cas de risques de sécurité et de changements dans l'environnement de risque ?
- 4.5. Chaque partenaire dispose-t-il de ressources suffisantes (humaines, financières et le temps) pour gérer les risques de sécurité ?
- 4.6. Le budget du partenariat/projet inclut-il des postes budgétaires liés à la sécurité, et suffit-il pour répondre aux besoins de sécurité des deux partenaires ? Ce financement est-il suffisamment souple pour couvrir les frais généraux, pour s'adapter si le contexte et les risques de sécurité évoluent, ou pour mener des activités de renforcement des capacités ?
- 4.7. Qui est chargé de contrôler ce qui est inclus dans le(s) budget(s) du partenariat ? Cette responsabilité peut-elle être transférée et partagée de manière égale entre les deux partenaires ?
- 4.8. De quelle manière les questions de sauvegarde sont-elles prises en compte au sein du partenariat ? Existe-t-il des mécanismes de signalement de la sauvegarde³ au sein du partenariat ? Existe-t-il des

³ Les mesures de 'sauvegarde' réfèrent au terme anglais de 'safeguarding'.

mécanismes de signalement de la sauvegarde pour le personnel de chaque partenaire, les bénéficiaires du programme et les membres de la communauté ?

4.9. De quelle manière les partenaires comptent-ils gérer les menaces de sécurité pouvant apparaître au sein-même des organisations partenaires (p. ex. personnel) ?

Questions clés pour une gestion inclusive du risque sécurité

Pour limiter les risques qui peuvent émerger du partenariat, les organisations partenaires doivent se demander :

- La stratégie de gestion du risque sécurité des deux organisations tient-elle compte de la façon dont l'identité des collaborateurs peut affecter leur vulnérabilité face aux menaces ?
- Comment les partenaires doivent-ils aborder les sujets identitaires sensibles, par exemple les menaces internes et externes basées sur l'orientation sexuelle ou le genre ? Quel est le niveau de « confort » des partenaires à cet égard (en tenant compte des sensibilités culturelles) ?
- Comment les partenaires peuvent-ils s'aider à sortir de leur zone de confort pour assurer une gestion efficace du risque sécurité pour l'ensemble du personnel ?

Exemples d'indicateurs

4.1. Une **évaluation conjointe du risque sécurité** liée aux opérations, ainsi que des risques associés et de l'impact pour chaque partenaire a été réalisée, et un processus clair est en place pour l'actualiser régulièrement. L'évaluation comprend une analyse des risques internes et des risques pouvant résulter du partenariat à proprement parler.

4.2. Il existe dans le budget du partenariat des lignes budgétaires explicites pour répondre aux besoins sécuritaires, y compris pour des activités de renforcement des capacités, et ces lignes budgétaires sont jugées suffisantes pour répondre à tous les besoins de ressources des deux partenaires.

4.3. Les partenaires se sont mis d'accord sur des stratégies ou des approches sécuritaires spécifiques au contexte, qui ont été communiquées à l'ensemble des services pertinents de chaque organisation.

4.4. Les responsables promeuvent et appuient activement la gestion du risque sécurité à tous les niveaux de l'organisation, ce qui se manifeste



par des communiqués et des rapports, des ateliers et/ou d'autres initiatives.

4.5. Les partenaires sont d'accord sur la manière de prévenir, de se préparer et de répondre aux incidents d'exploitation, d'abus et de harcèlement sexuels affectant leur personnel et les bénéficiaires au sein de leur organisation et du partenariat.

Opérations et programmes – étapes suivantes et complément d'information

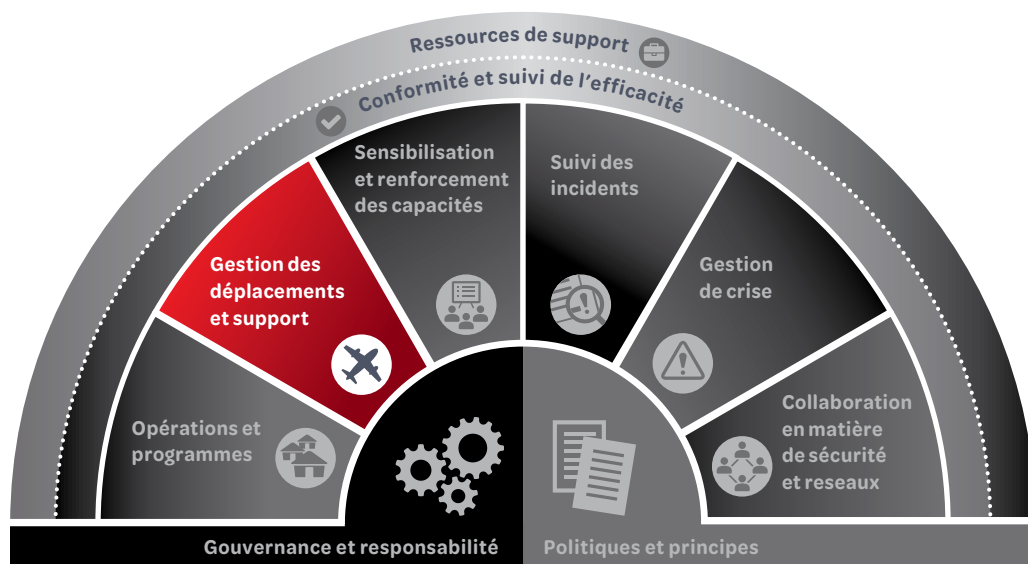
Les partenaires pourront aussi :

- Schématiser ensemble une journée type sur les différents sites de projet. Cet exercice permettra d'identifier les éventuels problèmes de sécurité
- Réaliser ensemble une évaluation du risque sécurité
 Voir **OUTIL 5**
- Dresser ensemble une liste des besoins de sécurité en vue de la mise en œuvre des programmes, les classer par ordre de priorité et en évaluer le coût
 Voir **OUTIL 6**
- Passer en revue le budget du programme/partenariat et y ajouter les coûts sécuritaires susceptibles de ne pas avoir été pris en compte
- Partager ou, si cela est pertinent, créer ensemble un plan de gestion du risque sécurité
 Voir **OUTIL 5**

Complément d'information :

- *GISF – La sécurité en pratique*
- *EISF – The Cost of Security Risk Management for NGOs*
- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *EISF – Gérer la sécurité du personnel humanitaire aux profils diversifiés*
- *EISF – Genre et sécurité : Orientations pour l'intégration du genre à la gestion du risque sécurité*
- *ODI-GPR8 – Operational Security Management in Violent Environments*

2.3.5. Gestion des déplacements et support



« Le personnel d'ONG L/N doit souvent se rendre dans des zones dangereuses et emprunter des véhicules ou des moyens de transport moins sécurisés que le personnel d'ONGI. Il est important d'en être conscient et de résoudre ce problème. »

Un point focal sécurité d'une ONGI

Les collaborateurs devront parfois se rendre sur les sites du projet pour assister à des réunions ou d'autres événements. Dans le cadre du partenariat, certaines organisations devront aller sur le site du projet et/ou dans un bureau de leur partenaire. Les deux partenaires doivent donc convenir d'un moyen de gérer les risques associés à ces déplacements, y compris les déplacements vers les sites de projets ayant trait au partenariat, ou les déplacements requis du fait du partenariat à proprement parler. Il faudra notamment que les règles relatives aux modes de communication et de déplacement tiennent compte des connaissances et de la langue locale.



Il est primordial que le secteur de l'aide adopte une culture qui encourage un soutien égal pour un travail égal. Les différences dans le soutien apporté aux personnels internationaux, nationaux et locaux des ONGI et des ONG L/N doivent être justifiées (p. ex. prouver que les profils de risque sont très distincts d'après les évaluations du risque sécurité).



OUTIL 5. Modèle d'évaluation et de plan de gestion conjoints du risque sécurité

Exemples de questions

- 5.1. Comment gérer les risques de sécurité découlant des déplacements effectués dans le cadre du partenariat ? Quelles doivent être les exigences minimales en termes de gestion des déplacements et d'accords de support (pour les déplacements sur le terrain, l'hébergement de nuit, les procédures de communication et toute autre forme de support) ?
- 5.2. Le soutien apporté au personnel des deux organisations sur les sites de projet en matière de déplacements et d'hébergement est-il équitable ?
- 5.3. Les partenaires sont-ils d'accord sur la politique et les procédures de sécurité à observer lors des déplacements des partenaires, et sur l'entité chargée du **duty of care** dont font l'objet les collaborateurs de passage ?
- 5.4. Le budget du partenariat comprend-il une assurance couvrant le personnel en déplacement des deux organisations partenaires ?
- 5.5. Les différents besoins du personnel en déplacement sont-ils pris en compte dans les procédures de déplacement, par exemple risque plus élevé en raison de caractéristiques personnelles (genre, ethnicité, handicap, etc.) ?

Exemples d'indicateurs

- 5.1. Les partenaires sont d'accord sur les dispositions et responsabilités s'appliquant à la sécurité lors des visites de personnels des deux organisations vers leurs bureaux et sites de programme.
- 5.2. Les partenaires communiquent entre eux les procédures de sécurité s'appliquant aux visites de personnel pertinentes pour le partenariat (p. ex. informations sur les rôles et responsabilités, formations, briefings, procédures pour signaler sa présence et procédures d'urgence).
- 5.3. La diversité des risques et besoins de sécurité des personnels en déplacement est prise en compte dans les procédures régissant les déplacements, par exemple si le risque est plus élevé en raison des caractéristiques personnelles de certains individus (genre, ethnicité, handicap, etc.).

Gestion des déplacements et support – étapes suivantes et complément d'information

Les partenaires pourront aussi :

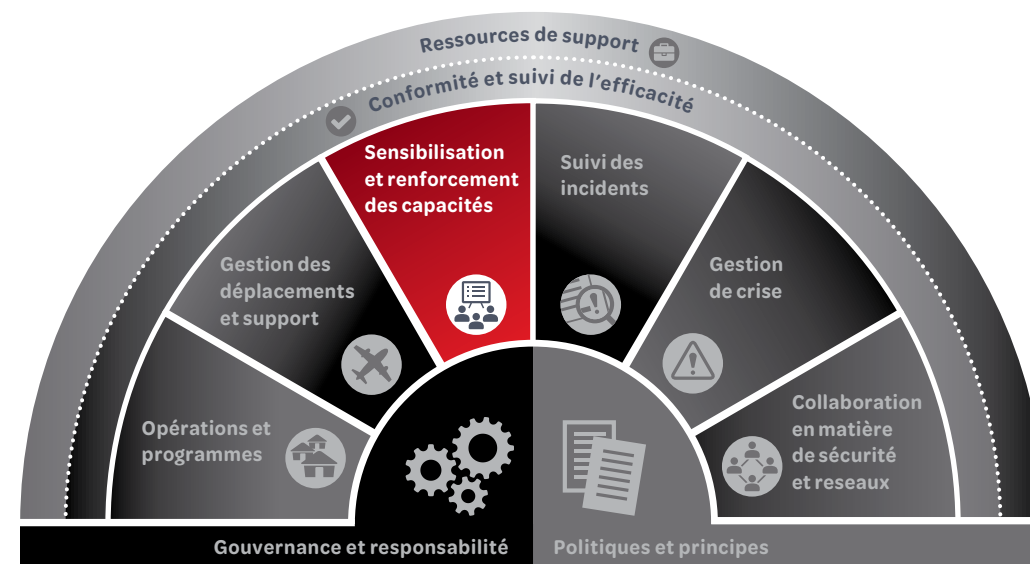
- Envisager un scénario hypothétique dans lequel le personnel d'une des deux organisations se rend dans le bureau ou le site projet de l'organisation partenaire, et déterminer laquelle des deux organisations doit se charger de planifier le déplacement, de vérifier l'existence de mesures de sécurité pour la visite et d'apporter une réponse en cas d'incident.
- Discuter des déplacements que les deux partenaires devront effectuer afin de mener à bien les programmes, et élaborer des procédures/exigences sécuritaires pour chaque site (ensemble ou de manière indépendante, comme en conviendront les deux partenaires).
- Consulter les collaborateurs au profil personnel diversifié sur leur vécu lors de leurs déplacements et sur les risques que les deux partenaires doivent prendre en compte pour réduire les risques encourus par le personnel en raison de leur profil individuel (voir 5.7, « Déplacements », dans le document de recherche d'EISF *Gérer la sécurité du personnel humanitaire aux profils diversifiés*).
- Discuter des mesures de sécurité minimales s'appliquant aux déplacements (réunions d'information, procédures pour signaler sa présence, entretien des véhicules, évaluations des risques associés aux déplacements, formation des conducteurs et gestion de l'information confidentielle relative aux déplacements).



Complément d'information :

- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *EISF – Gérer la sécurité du personnel humanitaire aux profils diversifiés (en particulier la section 5.7. « Déplacements » et le chapitre 2 « Duty of care et lutte contre la discrimination »)*

2.3.6. Sensibilisation et renforcement des capacités



Le renforcement des capacités est une question clé pour tout partenariat. Il est essentiel de sensibiliser les collaborateurs des ONGI et des ONG L/N aux risques de sécurité et aux capacités nécessaires pour les gérer. Le personnel de chaque organisation partenaire se sentira ainsi davantage responsabilisé face aux décisions sécuritaires et aux outils à employer.



L'apprentissage, un processus à double sens.

Lorsqu'elles nouent un partenariat, les organisations doivent s'interroger sur leurs forces et faiblesses et trouver ensemble des moyens de mieux sensibiliser le personnel aux risques sécurité et aux capacités nécessaires pour les gérer.



Ne pas confondre approches différentes et manque de capacités.

Les partenaires devront se mettre d'accord sur les besoins les plus importants en termes de renforcement des capacités, et identifier le format le mieux adapté aux activités de sensibilisation (formation en distanciel/présentiel, communications auprès du personnel, etc.). Les activités de renforcement devront être aussi durables que possible afin d'appuyer les capacités des personnels et des organisations sur le long

terme. Les partenaires pourront aussi envisager d'engager des formateurs privés ou des consultants externes.

► Voir 3.3, *Renforcer les capacités de gestion du risque sécurité au sein du partenariat*

Exemples de questions

6.1. De quelle manière les partenaires comptent-ils identifier les besoins de sensibilisation à la sécurité et de renforcement des capacités dans ce domaine, et travailler sur ces questions ensemble (aussi bien en termes de sécurité personnelle que de gestion du risque sécurité) ?

6.2. Les deux partenaires sont-ils d'accord sur les lacunes qu'il leur faut combler en termes de capacités de gestion du risque sécurité, et sur ce que chaque organisation peut faire pour y remédier ?

6.3. Le budget du partenariat comprend-il des fonds pour des activités de renforcement des capacités axées sur le long terme ?

6.4. Les mesures prises dans le cadre du partenariat, notamment concernant la gestion du risque sécurité, sont-elles communiquées aux collaborateurs pertinents, nouveaux ou plus anciens, des deux organisations partenaires ?

6.5. Les collaborateurs chargés de l'exécution du programme ont-ils accès à une formation sur la sécurité personnelle – notamment ceux qui travaillent dans des lieux à haut risque ?

6.6. La formation sécurité des collaborateurs est-elle fournie sous un format adapté à ses besoins (en distanciel/présentiel) ?

6.7. Cette formation répond-elle aux besoins à long terme du personnel tout en s'appuyant sur les connaissances et compétences existantes, et de manière aussi durable que possible ?

6.8. La stratégie de gestion du risque sécurité dans le partenariat permet-elle aux deux organisations partenaires de répondre aux besoins de sécurité de manière autonome ?

6.9. Est-il envisageable de mettre en place un encadrement de longue durée pour les points focaux sécurité au sein du partenariat ?

Exemples d'indicateurs

6.1. Les partenaires sont d'accord sur leurs besoins de capacités en matière de GRS.

6.2. Il existe une stratégie d'apprentissage, de développement et de

renforcement des capacités, assortie d'un plan de mise en œuvre clair, dont l'objectif est d'améliorer les capacités des partenaires sur le long terme.

6.3. L'organisation partage régulièrement ses ressources avec ses partenaires et soutient l'accès aux opportunités de renforcement des capacités, d'apprentissage et de développement en matière de gestion du risque sécurité.

Sensibilisation et renforcement des capacités – étapes suivantes et complément d'information

Les partenaires pourront aussi :

- Identifier les opportunités de formation et de renforcement des capacités auxquelles chaque partenaire a accès, ainsi que la méthode à employer pour les transmettre aux autres partenaires.
- Dresser une liste des besoins de formation à long terme et des stratégies à employer.
- Partager régulièrement les ressources entre partenaires (par exemple, sites Internet utiles, outils, documents, listes de formateurs, interlocuteurs locaux, etc.).

Les organisations et plateformes suivantes proposent des formations à la sécurité personnelle et à la gestion du risque sécurité :

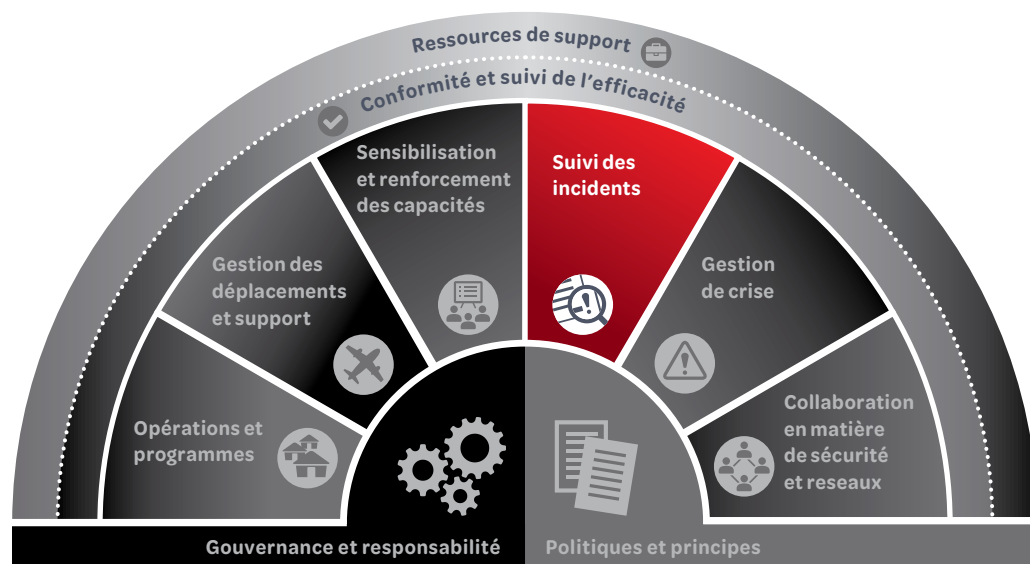
- [Site de l'INSSA](#)
- [DisasterReady Platform](#)
- [UNDSS](#)
- [Formation Stay Safe du FICR](#)
- [Kaya Connect](#)

Complément d'information :

- *EISF – Security Management and Capacity Development: International agencies working with local partners*
- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONGs*



2.3.7. Suivi des incidents



Le signalement et le suivi des incidents sont essentiels pour la gestion du risque sécurité car ils permettent de mieux comprendre le contexte opérationnel et les risques de sécurité pour les organisations et leur personnel. Cette information éclairera la prise de décisions pour tous les services de l'organisation, y compris au niveau des opérations, des programmes, du financement, du plaidoyer et de la gestion du risque sécurité.



Toutes les organisations sont sujettes à des incidents de sécurité. Les partenaires dotés de systèmes de signalement performants comprendront mieux les risques de sécurité auxquels leur personnel est confronté et pourront ainsi réduire la probabilité que des incidents se produisent.

Les partenariats sont plus performants si les organisations partagent les informations sur les incidents susceptibles d'affecter les autres partenaires, et le partenariat dans son ensemble. Le manque de confiance constitue ici un problème majeur : soit au sein de l'organisation, si son personnel a peur de signaler les incidents, soit entre organisations partenaires, si elles craignent que le fait de partager des informations sur un incident n'affecte le partenariat, leur réputation ou leur financement. Pour améliorer le signalement au sein des partenaires et entre eux, des

mécanismes de signalement puissants et confidentiels doivent être mis en œuvre pour gérer les problèmes de confidentialité et de sanctions.



Les partenaires doivent faire preuve de transparence entre eux ainsi qu'avec leur personnel sur la manière dont l'information relative aux incidents sera utilisée et dont la confidentialité sera préservée.

► Voir 1.4, *Communiquer et instaurer la confiance au sein du partenariat*

Exemples de questions

- 7.1.** De quelle manière les partenaires doivent-ils partager entre eux l'information sur les incidents ?
- 7.2.** Comment les partenaires peuvent-ils s'entraider en matière de gestion des informations sur les incidents de sécurité ? Par exemple, au moyen de procédures de signalement des incidents, de systèmes d'enregistrement des incidents et d'outils d'analyse des données d'incident afin d'éclairer les décisions dans les domaines de la sécurité, des programmes, des opérations, du plaidoyer, du financement, etc.
- 7.3.** Sur chaque site, à quelles données d'incidents de sécurité chaque organisation peut-elle accéder, soit à travers ses propres opérations, soit par le biais de ses réseaux, et pouvant être partagées régulièrement avec son partenaire ?
- 7.4.** Que peuvent faire les deux partenaires si les incidents ne sont pas tous signalés ?
- 7.5.** Sont-ils d'accord sur les types d'incidents à signaler ?
- 7.6.** Comment les partenaires peuvent-ils s'aider à améliorer la confidentialité des mécanismes de signalement afin de protéger le personnel et d'éviter que l'information ne tombe entre les mains d'acteurs ou d'autorités hostiles (p. ex. solutions technologiques et conseils sur les meilleures pratiques) ?

Exemples d'indicateurs

- 7.1.** Il existe une procédure de gestion et de partage de l'information de sécurité (y compris des données d'incidents) entre les partenaires et pour le contexte opérationnel, et cette procédure est respectée.
- 7.2.** Les partenaires sont d'accord sur la façon dont les données d'incident doivent éclairer les décisions, y compris à travers une politique indiquant clairement si des sanctions peuvent être prises suite au signalement ou

au non-signallement d'un incident.

7.3. L'organisation passe périodiquement en revue les incidents qui affectent son personnel afin d'identifier les tendances et les préoccupations, et elle en fait part aux organisations partenaires.

Suivi des incidents – étapes suivantes et complément d'information

Les partenaires pourront aussi :

- Partager et passer en revue ensemble les procédures et mécanismes internes de signallement des incidents déjà en place
- Désigner un point focal chargé de signaler les incidents
- Identifier un moyen de partager les informations sur les incidents entre eux
- Former le personnel au signallement des incidents, à la gestion de l'information et à la confidentialité (voir par exemple les guides DisasterReady cités ci-après)
- Discuter des types d'incidents à signaler, et des répercussions que certains types d'incidents pourraient avoir sur le partenariat.

Les plateformes suivantes collectent et partagent des données sur les incidents de nombreuses organisations:

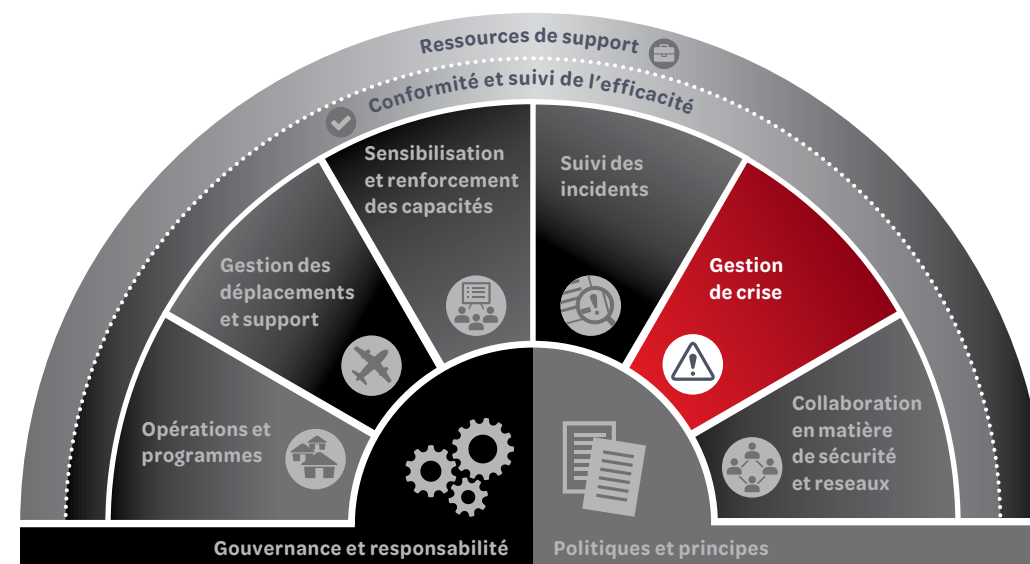
- [Aid Worker Security Database – Humanitarian Outcomes](#)
- [Projet Aid in Danger – Insecurity Insight](#)
- [INSO Key Data Dashboard](#)

Complément d'information et ressources :

- [RedR UK, Insecurity Insight et EISF - Manuel de gestion de l'information issue des incidents de sécurité](#)
- [DisasterReady Safety and Security Incident Information Management \(SIIM\) mobile guide for organisations](#)
- [DisasterReady Safety and Security Incident Information Management \(SIIM\) mobile guide for staff](#)



2.3.8. Gestion de crise



Les organisations qui opèrent dans des contextes à haut risque sont plus susceptibles de faire l'objet d'un incident critique qui ne sera pas gérable au moyen des procédures organisationnelles standard. Ce type d'incidents (généralement qualifié de « crise » ou d'« incident critique ») peut être, par exemple, un décès, un enlèvement ou l'arrestation d'un membre du personnel (en raison de **menaces** externes ou internes). Une crise peut aussi être un événement qui, du fait de sa gravité, a des répercussions plus larges sur l'organisation. Les organisations dotées de systèmes de gestion du risque sécurité bien établis disposeront déjà d'une méthode dédiée pour répondre aux crises (on parle parfois de « structure de gestion de crise »).

Bien que les crises soient exceptionnelles, les partenaires doivent s'y préparer et convenir d'une méthode pour gérer les incidents graves. Ils devront identifier l'organisation la mieux placée pour apporter une réponse en cas de crise affectant le partenariat (en termes de logistique, d'accès et d'expertise, par exemple).



La gestion de crise est une question complexe qui n'est abordée que brièvement dans ce guide. Les partenaires sont invités à consulter des ressources complémentaires (voir « Complément d'information » ci-après).

Exemples de questions

8.1. De quelle manière les partenaires comptent-ils collaborer/coordonner leurs actions en cas de crise ou d'incident critique les affectant sur le site concerné ?

8.2. En cas de crise ou d'incident critique qui affecte les deux partenaires, qui doit se charger de la réponse de gestion de crise ? Quelles sont les responsabilités et qui a l'autorité de prendre les décisions ?

8.3. Quel support chaque partenaire peut-il apporter à l'autre en cas d'incident critique sur le site du partenariat ?

8.4. Faut-il que les partenaires incluent le personnel de chaque organisation dans un système de partage rapide de l'information de sécurité pour assurer une bonne prise en charge du personnel présent sur le site affecté par une crise ou un incident critique ?

8.5. Existe-t-il des procédures d'évaluation et de débriefing post-incident au sein du partenariat qui permettent de comprendre voire de réduire le risque que des incidents se reproduisent ?

8.6. À quelle forme d'assurance les deux partenaires ont-ils accès en cas de crise ou d'incident critique ?

Système de partage rapide de l'information de sécurité

En cas d'incident de sécurité ou de changement soudain dans le contexte sécuritaire, les organisations doivent disposer d'un processus pour communiquer rapidement la nouvelle en leur sein – et avec les autres organisations au sein du partenariat – sans solliciter à l'excès une personne spécifique. C'est ce que l'on appelle parfois le processus de l'**arborescence sécurité**, qui consiste à charger chaque collaborateur d'appeler un petit nombre d'individus en cas d'urgence. Autre possibilité, les organisations peuvent se servir de plateformes de messageries de masse, par exemple WhatsApp, pour diffuser rapidement l'information de sécurité auprès d'un grand nombre (il faudra tenir compte des exigences en matière de sécurité numérique).

Exemples d'indicateurs

8.1. Il a été convenu des responsabilités et de l'autorité de décision en cas de crise ou d'incident critique affectant les deux partenaires, dans l'idéal par écrit ou schématisé (par ex. organigramme).

8.2. Les partenaires disposent d'une structure et d'un plan de gestion de crise.

8.3. Les partenaires ont accès à des services de support d'urgence (médicale et non médicale) dans le cadre de l'assurance contractée par chaque organisation.

Gestion de crise – étapes suivantes et complément d'information

Les partenaires pourront aussi :

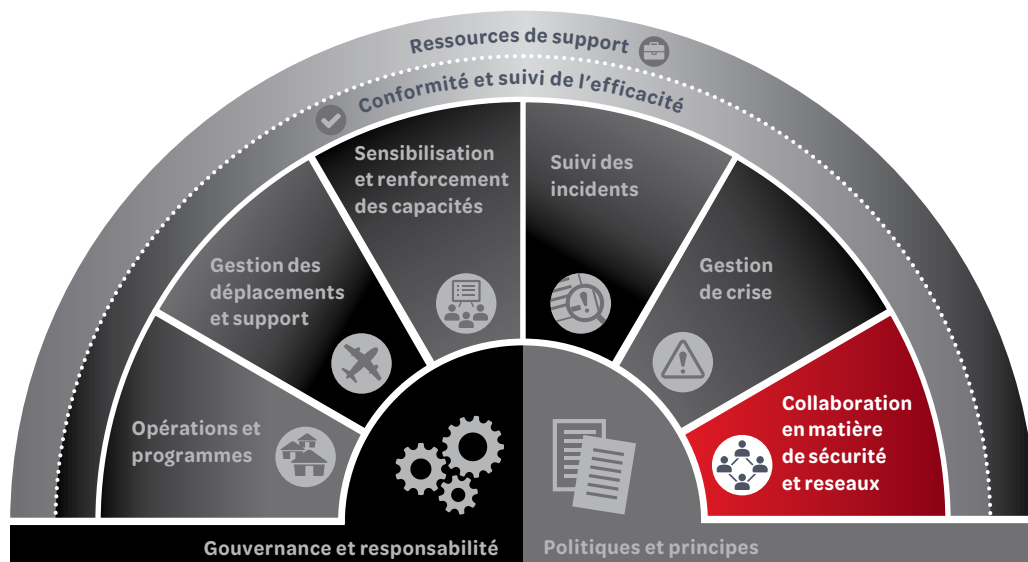
- Convenir d'un système de communication à employer en cas de crise.
- Instaurer une équipe de gestion de crise comprenant des collaborateurs des deux organisations, à déclencher en cas de crise.
- Organiser des exercices de simulation de crise.
- Explorer les options en matière d'assurance pour se préparer à une crise ou un incident critique.
- Se préparer à l'éventualité d'une crise en consultant les ressources relatives à la bonne gestion des crises et des incidents critiques et en les partageant (voir liste de ressources ci-après).

Complément d'information :

- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *EISF – Crisis Management of Critical Incidents*
- *EISF – Gérer la violence sexuelle à l'encontre du personnel humanitaire*



2.3.9. Collaborations et réseaux dans le domaine de la sécurité



Les organisations qui collaborent sur les questions de sécurité avec des acteurs opérant dans le même contexte opérationnel bénéficieront non seulement d'une meilleure gestion du risque sécurité, mais aussi d'une sécurité collective accrue. Les collaborations doivent s'étendre au-delà des organisations partenaires, pour inclure des relations actives avec les réseaux et les forums de partage d'information à différents niveaux, y compris à l'échelon local ou communautaire, national, régional ou international.



Les deux partenaires devront envisager de soutenir les réseaux qui traitent des questions de sécurité.

Exemple de collaboration en matière de sécurité

Le groupe de travail pour l'accès humanitaire au nord-ouest de la Syrie, dirigé par OCHA, qui rassemble différentes ONG L/N, ONGI et agences internationales, est un bon exemple de collaboration fructueuse en matière de GRS, avec un impact positif sur le statut du risque sécurité des organisations opérant dans ce contexte. Par exemple, cette plateforme a permis aux ONG L/N de soulever leurs problèmes communs sans avoir à exposer leurs **vulnérabilités** individuelles aux

Exemple de collaboration en matière de sécurité *suite*

donateurs ou aux organisations partenaires, d'où une discussion plus ouverte et plus honnête. Cela a permis de protéger les ONG L/N de tout impact négatif que ces discussions auraient pu avoir sur leur réputation et/ou leurs opportunités de financement.

Les partenaires doivent s'aider à accéder aux collaborations et réseaux de sécurité pour améliorer la sécurité de leur personnel. Cela exigera parfois de mener un plaidoyer auprès d'autres organisations.

► Voir le chapitre 4 pour un complément d'information sur le plaidoyer dédié aux questions de gestion du risque sécurité

Exemples de questions

- 9.1.** Existe-t-il des plateformes qui traitent des questions de sécurité ? Si oui, les deux partenaires y ont-ils accès et peuvent-ils s'y exprimer de manière égale dans leurs domaines opérationnels (y compris plateformes de partage de l'information) ?
- 9.2.** Quels obstacles et défis empêchent une participation active des deux partenaires aux forums, réunions et discussions interagences sur la sécurité aux niveaux local, national, régional et international ?
- 9.3.** Quelles mesures chacune des deux organisations peut-elle prendre pour inclure son partenaire dans ces discussions ?
- 9.4.** Quelles mesures chacune des deux organisations peut-elle prendre à titre individuel et collectif afin d'améliorer la collaboration dans le domaine de la sécurité avec les autres organisations actives dans le domaine opérationnel (nationales et internationales) ?

Exemples d'indicateurs

- 9.1.** Les deux partenaires participent activement aux forums, plateformes, réunions et consortiums sur la gestion du risque sécurité, et ils partagent l'information sur la sécurité avec d'autres acteurs aux niveaux local, national, régional et/ou international.
- 9.2.** Dans la mesure du possible, les deux organisations encouragent et facilitent la participation de leurs partenaires aux forums, plateformes, réunions et discussions interagences afin de renforcer le partage de l'information et la collaboration dans le domaine de la sécurité. Elles fournissent à leurs partenaires les coordonnées d'acteurs propices à la gestion du risque sécurité.

Exemples de plateformes de coordination qui traitent de la sécurité

- *Saving Lives Together (SLT)*
- *International NGO Safety Organisation (INSO)*
- *MENA Region Humanitarian Safety and Security Forum*
- *South Sudan NGO Forum*

Collaborations et réseaux dans le domaine de la sécurité – étapes suivantes et complément d'information

Les partenaires pourront aussi :

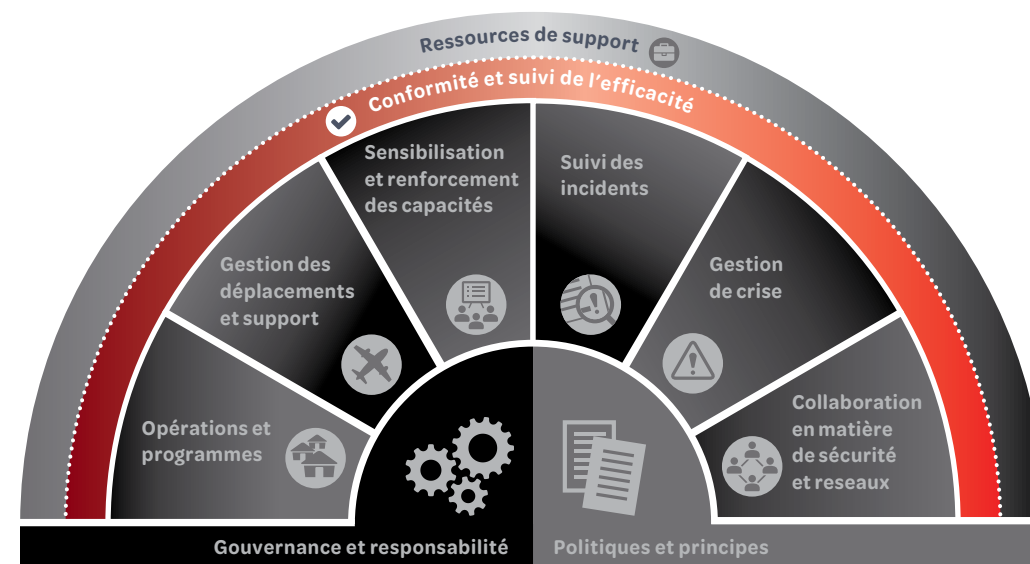
- Faire participer leurs partenaires à des plateformes de collaboration sur la sécurité.
- Étudier et chercher à résoudre les obstacles à une participation active des deux partenaires aux plateformes existantes.
- Contacter les plateformes de collaboration sur la sécurité et charger un point focal de leur organisation d'établir un contact régulier avec ces plateformes.
- Créer des réseaux de collaboration sur la sécurité s'il n'en n'existe pas, et inviter différentes organisations à y participer.

Complément d'information :

- *RedR UK, Insecurity Insight et EISF – Manuel de gestion de l'information issue des incidents de sécurité*
- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*



2.3.10. Compliance⁴ et suivi de l'efficacité



« Faire preuve de compliance, cela signifie maintenir l'approche sécurité de l'organisation (en veillant à sa viabilité et sa durabilité à long terme) et en assurer le suivi. »

Un point focal sécurité d'une ONGI

Les organisations doivent régulièrement surveiller et passer en revue leur **cadre de gestion du risque sécurité** pour vérifier le respect des procédures par leur personnel et la pertinence de leur stratégie sécuritaire. Dans les accords de partenariat, il faut également s'assurer que chaque partenaire assume les responsabilités convenues en matière de gestion du risque sécurité.

Exemples de questions

10.1. Comment les deux partenaires doivent-ils s'y prendre pour passer en revue régulièrement la gestion du risque sécurité au sein du partenariat ?

10.2. Quel niveau de *compliance* et de suivi de l'efficacité de la GRS au sein de chaque organisation et/ou du partenariat est acceptable pour les deux partenaires ?

10.3. Quelle quantité d'informations les partenaires sont-ils prêts à

⁴ La notion de compliance se traduit en français par « conformité » mais cela lui fait perdre la dimension culturelle et l'origine anglo-saxonne qui lui sont attachées. Nous utilisons ici le terme « compliance », étant entendu que certaines organisations utilisent le terme « conformité ».

partager entre eux concernant les enseignements, les examens, les audits sécurité et l'analyse post-incident propres au contexte, au partenariat ou à un projet particulier ?

10.4. Le processus de *compliance* signifie-t-il qu'un des partenaires est sollicité à l'excès ?

10.5. Les attentes en matière de *compliance* et de suivi de l'efficacité sont-elles en phase avec les capacités ? Ce suivi de l'efficacité vient-il compléter les autres types de suivi liés au partenariat et dont se chargent d'autres départements, par exemple le service financier ?

10.6. Existe-t-il déjà des processus de gestion des partenariats dédiés au suivi au sein desquels la gestion du risque sécurité pourrait être intégrée ?

10.7. Quelles mesures les deux partenaires peuvent-ils prendre pour instaurer et faire respecter une culture disciplinaire solide en cas de non-respect des politiques sécuritaires et des exigences minimales ?

Exemples d'indicateurs

10.1. Les enseignements, les examens, les analyses post-incident et les audits sécurité relatifs au contexte, au partenariat ou au projet/programme sont partagés entre partenaires et font l'objet de discussions.

10.2. Les collaborateurs chargés de contrôler la mise en œuvre des systèmes de sécurité et leur utilisation conforme (au sein de chaque organisation et du partenariat) sont formés de manière appropriée, ont été impliqués dans l'**examen conjoint de la GRS**, et ces responsabilités sont explicitement indiquées dans leur descriptif de poste.

10.3. Les systèmes de gestion de la performance des employés font explicitement référence aux responsabilités en matière de sécurité et au respect des politiques de l'organisation.



Compliance et suivi de l'efficacité – étapes suivantes et complément d'information

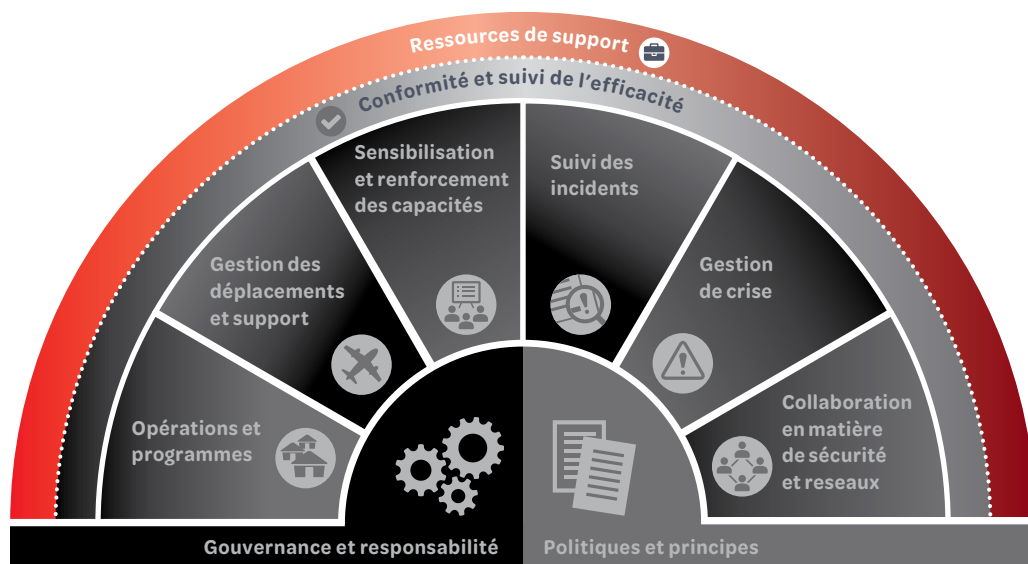
Les organisations pourront aussi :

- Créer une check-list *compliance* (par exemple outil 3, « Check-list pour la revue des documents » dans le guide *Évaluations de la sécurité* d'EISF).
- Employer les mécanismes de *compliance* que leur partenaire utilise déjà dans le cadre d'autres partenariats pour ne pas dupliquer leur travail.

Complément d'information :

- *EISF – Évaluations de la sécurité*
- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*

2.3.11. Ressources complémentaires



« Les ONGI doivent soutenir leurs partenaires d'ONG L/N dans la gestion du risque sécurité. »

Un point focal sécurité d'une ONG L/N

L'ensemble du personnel doit avoir accès à des directives, des outils et d'autres ressources pour soutenir ses efforts en matière de gestion du risque sécurité. La plupart de ces ressources sont disponibles gratuitement en ligne et dans de nombreuses langues (voir l'encadré Complément d'information de ce chapitre).



Les deux partenaires doivent activement partager les ressources de gestion du risque sécurité au sein du partenariat.

Les partenaires doivent améliorer l'accès de leur personnel aux ressources en les rendant disponibles hors-ligne, dans des formats non écrits et dans les langues pertinentes.

Exemples de questions

11.1. Des ressources complémentaires sur la gestion du risque sécurité sont-elles disponibles et l'ensemble du personnel peut-il y accéder ? Dans le cas contraire, quelles mesures prendre pour en améliorer l'accessibilité ?

11.2. Les partenaires ont-ils partagé entre eux leurs ressources en matière de gestion du risque sécurité ?

11.3. De quelles autres ressources les partenaires bénéficieraient-ils pour mieux gérer leurs risques de sécurité ?

Exemples d'indicateurs

11.1. Les ressources relatives à la gestion du risque sécurité répondant aux besoins de tous les collaborateurs pertinents des partenaires sont régulièrement partagées sous un format accessible à tous.

11.2. Les partenaires mettent à disposition toute une série d'orientations, d'outils et de modèles dans un registre sécurité pour pouvoir s'entraider dans la gestion du risque sécurité.

Ressources complémentaires – étapes suivantes et complément d'information

Les partenaires pourront aussi :

- Partager entre eux les ressources complémentaires et en discuter pour bien les comprendre.
- Adapter les ressources pour les rendre plus accessibles (p. ex. visualisation des processus de décisions, traduction dans les langues pertinentes, etc.).

Complément d'information :

- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG (disponible en anglais, en espagnol et en français. Une version en arabe sera disponible en 2021)*
- *Page Web GISF Library*
- *Plateforme de formation de GISF*
- *Ressources et formation DisasterReady (disponibles dans plusieurs langues)*



2.4. Élaborer et mettre en œuvre un plan d'action en vue d'un examen conjoint de la GRS

Une fois le questionnaire et les indicateurs d'évaluation renseignés, la dernière étape de l'**examen conjoint de la GRS** consiste à aborder les indicateurs partiellement présents ou absents, par exemple en élaborant un **plan d'action dédié à l'examen conjoint de la GRS**. Les deux organisations devront mettre en œuvre ce plan d'action conjoint et convenir d'un calendrier de suivi.

L'objectif de ce plan d'action est d'améliorer la coordination entre partenaires autour du système de gestion du risque sécurité (il s'agit donc d'un « outil de gestion du partenariat », et non d'un « outil de gestion du risque sécurité »).

Les indicateurs déjà jugés présents lors de l'exercice d'évaluation n'ont pas besoin d'être inclus dans le plan d'action.

Ce guide présente un **modèle de plan d'action en vue d'un examen conjoint de la GRS** pour aider les partenaires à renseigner le statut de chaque indicateur, les rôles et responsabilités, les objectifs clés et le calendrier de mise en œuvre. Les partenaires pourront adapter ce modèle afin de mieux discuter et suivre les mesures prises dans le cadre de l'examen conjoint de la GRS.

OUTIL 4. Modèle de plan d'action en vue d'un examen conjoint de la GRS

Plan d'action en vue d'un examen conjoint de la GRS vs plan de gestion du risque sécurité

Le **plan d'action en vue de l'examen conjoint de la GRS** présenté dans ce guide désigne plus spécifiquement une check-list de tâches que les deux partenaires conviennent de mettre en œuvre dans le cadre du processus d'**examen conjoint de la GRS**.

Chaque organisation est susceptible de disposer de son propre « plan de gestion du risque » (parfois appelé « plan de gestion du risque sécurité », « plan de gestion de la sécurité » ou « plan de sécurité »), qui décrit spécifiquement les mesures qu'elle doit prendre pour gérer les risques de sécurité identifiés (par exemple, gérer le risque de vol ou de mise en détention).

► Voir 3.1, Identifier et répondre ensemble au risque sécurité



Identifier et répondre ensemble aux besoins, lacunes et défis en matière de GRS

3.1. Identifier et répondre ensemble au risque sécurité

Le partage des responsabilités à l'égard du risque sécurité permet aux partenaires d'étudier ensemble les différents risques de sécurité auxquels ils sont exposés et leur impact potentiel sur les deux organisations et les personnels. Cela signifie aussi qu'ensemble, ils doivent identifier et mettre en œuvre les mesures nécessaires à la gestion du risque sécurité.

Le partage des responsabilités à l'égard du risque sécurité est essentiel pour une gestion du risque sécurité équitable au sein du partenariat.

Pour partager les risques, les partenaires doivent d'abord avoir une compréhension commune des risques qui les affectent et qui affectent le partenariat. Cette discussion consiste à réfléchir aux perceptions de chaque partenaire par rapport au risque sécurité et à leur attitude à leur égard. Elle permettra aux deux organisations d'expliquer ce qu'elles entendent concrètement par « degré de probabilité » et « impact ». Les partenaires pourront ensuite expliquer ce qui constitue pour eux un niveau acceptable de risque.

OUTIL 2. Attitude face au risque au sein du partenariat

Il est aussi important que les partenaires comprennent et travaillent ensemble sur les problématiques résultant du transfert du risque sécurité au sein du partenariat. Si un partenaire fait face à un risque sécurité, il se peut fort que l'autre partenaire, et le partenariat dans son ensemble, soient également affectés. En identifiant ensemble les risques et en convenant d'une stratégie, les partenaires conjuguent leurs capacités et leurs connaissances pour réduire la probabilité qu'un incident se produise et pour améliorer leur aptitude à gérer un éventuel incident.

Par exemple, lors d'un projet mené en partenariat, une ONG L/N peut s'exposer à un risque d'accident de la route. Un incident de ce type affecterait non seulement directement le personnel de l'ONG L/N, mais aussi le budget du partenariat, la capacité des deux partenaires à atteindre les objectifs de leur programme et la réputation des deux partenaires. Pour réduire le risque d'accident de la route, l'ONG L/N peut par exemple aider l'ONGI partenaire à comprendre la probabilité d'un accident de la route, et les raisons pour lesquelles le risque peut être élevé (p. ex. manque de sécurité routière, sécurité insuffisante des véhicules). Quant à l'ONGI, elle peut aider les conducteurs de l'ONG L/N à bénéficier d'une formation à la sécurité routière ou de fonds supplémentaires pour acquérir des véhicules plus adaptés.

Pour bien comprendre les besoins de support de chacun et mettre en œuvre les mesures d'atténuation adéquates, il est primordial que les partenaires réalisent une évaluation conjointe du risque sécurité. Celle-ci peut se faire à un niveau plus global, en tenant compte des risques généraux découlant du partenariat, ou au niveau du pays, en étudiant les risques spécifiques au contexte. Cette évaluation peut ensuite servir à élaborer un plan conjoint de gestion du risque sécurité afin d'atténuer les risques identifiés. Ce guide présente un modèle d'évaluation et de plan de gestion conjoints du risque sécurité.



OUTIL 5. Modèle d'évaluation et de plan de gestion conjoints du risque sécurité

Cette évaluation conjointe, et d'une manière plus générale l'examen conjoint de la GRS, peuvent mettre en évidence des besoins, lacunes et défis plus globaux en matière de GRS, par exemple dans les domaines du financement et des capacités. Ces défis sont abordés plus en détail dans les sections suivantes.



Complément d'information

- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *GISF – La sécurité en pratique*

3.2. Financer la gestion du risque sécurité au sein du partenariat

Les coûts de la gestion du risque sécurité doivent être envisagés le plus tôt possible, dans l'idéal avant même le lancement du programme, afin que les deux partenaires disposent des fonds nécessaires pour exécuter leurs activités en toute sécurité.

Il est primordial d'octroyer un budget pour la gestion du risque sécurité afin de permettre au personnel d'atteindre les communautés ciblées en toute sécurité. Malheureusement, le personnel d'ONG L/N se retrouve souvent confronté à des obstacles qui l'empêchent de demander des fonds supplémentaires, et les budgets sécurité sont bien souvent inexistantes afin de réduire le coût global. Les partenaires d'ONGI peuvent répondre à certains de ces défis en initiant des discussions au sujet du financement de la gestion du risque sécurité avec les ONG L/N, plutôt que d'attendre une demande de fonds.



Les partenaires doivent s'aider à identifier et aborder ouvertement la question des besoins de fonds dédiés à la GRS, car il s'agit d'une condition préalable à une planification de qualité et à la réalisation des obligations organisationnelles au titre du *duty of care*.

Les coûts de la GRS comprennent toutes les dépenses servant à réduire la probabilité de préjudice ou de pertes pour l'organisation ou son personnel, ou la probabilité de devoir verser des réparations. Ces coûts peuvent inclure :

- Le développement et la mise en œuvre de politiques et procédures
- Les salaires des points focaux sécurité
- La formation et les activités de sensibilisation à la sécurité
- La réalisation d'**évaluations du risque sécurité**
- La réponse aux incidents, y compris la suspension ou la fermeture du programme
- L'assurance
- Les équipements nécessaires à la sécurité, y compris les communications
- La fourniture d'une sécurité physique, dont des portillons de sécurité, des verrous, etc.
- Les services destinés au bien-être et au soutien psychosocial des employés.



OUTIL 3 & 4. Le modèle de questionnaire et de fiche de travail en vue de l'examen conjoint de la GRS et le modèle de plan d'action en vue de l'examen conjoint de la GRS peuvent aider les partenaires à tenir compte des déficits de financement et à identifier des moyens de prendre en charge les frais de GRS d'une manière plus générale au sein du partenariat.

OUTIL 5. Le modèle d'évaluation et de plan de gestion conjoints du risque sécurité peut servir à établir le coût de la gestion du risque sécurité au sein du partenariat.

Si le financement est insuffisant pour prendre en charge adéquatement les risques de sécurité du personnel, les partenaires devront réexaminer le projet ou le programme en tenant compte du seuil de risque convenu.

De précédents travaux de recherche de GISF ont révélé que la plupart des donateurs internationaux étaient disposés à inclure les coûts de la gestion du risque sécurité dans les budgets des projets. Il est impératif que les propositions soient dotées du budget GRS requis en s'appuyant sur les conclusions d'**évaluations du risque sécurité** spécifiques au contexte. Les collaborateurs chargés de rédiger les propositions devront connaître la position des donateurs en matière de financement de la gestion du risque sécurité, ainsi que les besoins en matière de GRS de leur propre organisation et des partenaires, afin que les ressources adéquates soient attribuées.



OUTIL 6. Modèle de budget dédié à la gestion du risque sécurité au sein du partenariat

S'il s'avère problématique d'inclure les coûts de la sécurité dans les propositions, les responsables des subventions, le personnel du programme et les dirigeants des organisations devront plaider auprès des donateurs pour qu'ils soient bel et bien pris en charge.

► *Voir 4.2.3, Plaidoyer en faveur de la gestion du risque sécurité et financement*



Complément d'information

- *EISF – The Cost of Security Risk Management for NGOs*
- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*

3.3. Renforcer les capacités de gestion du risque sécurité au sein du partenariat



« Tous les collaborateurs doivent savoir gérer les risques de sécurité inhérents à leur propre rôle. »

Un point focal sécurité

D'après les travaux de recherche de GISF, on croit souvent à tort que ce sont les ONGI qui détiennent les connaissances et les compétences en matière de GRS – et de nombreux autres aspects de l'aide. Pour le personnel des ONG L/N, le renforcement des capacités est souvent perçu comme une nécessité par défaut, pour laquelle des séances de formation ou d'information sur la sécurité d'une journée ou deux sont éventuellement organisées. Certes, la situation est différente pour chaque ONG L/N, mais cette perspective ne rend pas compte des capacités d'un grand nombre d'ONG L/N du secteur de l'aide.

Ces recherches ont montré que les ONG L/N affichaient des compétences de premier plan s'agissant de :

- Développer et entretenir un sentiment d'acceptation, par exemple préserver des relations de qualité et de longue durée avec les bénéficiaires
- Coordonner et négocier
- Analyser et comprendre le contexte local (y compris les dynamiques communautaires, les conflits locaux et les politiques locales)
- Nouer un contact avec les personnes affectées et comprendre leurs besoins et aspirations.

Les partenaires internationaux auraient tort de penser qu'une ONG L/N manque de réflexion et de mesures axées sur la sécurité pour la simple raison qu'elle ne dispose pas de règles écrites ou d'une stratégie de gestion du risque sécurité identique à la leur. De même, on aurait tort de croire que les ONG L/N qui comprennent parfaitement le contexte local ne courent aucun risque sécurité ou ont la capacité de les gérer. Inversement, les ONG L/N ne devraient pas penser que les ONGI disposent de toutes les capacités, connaissances ou ressources



nécessaires pour gérer effectivement les risques de sécurité. Les ONGI s'appuient souvent sur le savoir et les méthodes de travail au niveau local pour opérer en toute sécurité dans les contextes à haut risque.

Les partenaires doivent commencer par identifier les capacités présentes au sein du partenariat et convenir des catégories à renforcer. L'**examen conjoint de la GRS** donnera un aperçu des besoins et des lacunes.

► Voir le chapitre 2, *Réaliser un examen conjoint de la gestion du risque sécurité*

Dans le cas de partenariats de longue durée, il est conseillé d'adopter une approche plus détaillée du renforcement des capacités de GRS. Il existe plusieurs outils pertinents à cet égard.

Complément d'information

- L'outil de Cinfo intitulé *Duty of Care Maturity Model Tool* peut aider les organisations à mesurer leur maturité dans des domaines essentiels pour remplir leurs obligations de **duty of care** et améliorer la gestion du risque sécurité.
- L'annexe 1 du projet d'EISF *Security Management and Capacity Development: International agencies working with local partners* présente une version simplifiée de l'outil d'évaluation de la sécurité des partenaires.

Lors des discussions sur le renforcement des capacités, les partenaires devront viser une complémentarité des différentes approches GRS, en s'appuyant sur les éléments efficaces et déjà en place pour gérer les risques de sécurité. Il s'agira notamment de cerner les opportunités de développement.



« Certains de nos partenaires bénéficient déjà de capacités renforcées grâce à d'autres acteurs – le fait d'en discuter permettra d'éviter de dupliquer les ressources. Cela permet aussi de cerner les situations où différents acteurs souhaitent travailler ensemble sur une mission spécifique (formation collective). »

Un point focal sécurité d'une ONGI



Les activités de renforcement des capacités en matière de GRS doivent être aussi durables que possible et perdurer au-delà du partenariat.

Parmi les activités de renforcement des capacités, citons les suivantes :

- Fournir des informations et des ressources sur la sécurité et veiller à les rendre accessibles au personnel qui en a besoin (éventuellement les traduire ou les fournir sous un format non écrit).
- Fournir une formation sécurité répondant aux besoins du personnel, dispensée par les ONG L/N à l'attention de leurs partenaires internationaux, sur le contexte local et les stratégies de sécurité efficaces, ou assurée par des ONGI fournissant au personnel des ONG L/N une formation sécurité propre au contexte (y compris en aidant le personnel d'ONG L/N à accéder aux programmes de formation sécurité interagences régionaux ou nationaux).
- Adopter une approche « formation des formateurs » pour que le personnel formé transmette les connaissances et ressources nouvellement acquises.
- Ancrer les compétences techniques au sein des organisations partenaires. Par exemple en détachant certains collaborateurs d'une organisation vers son organisation partenaire afin d'encourager un partage approfondi de l'information, des connaissances et des méthodes de travail.
- Développer des programmes de mentorat officiels entre les points focaux sécurité des deux organisations ou avec des mentors externes (voir l'INSSA, par exemple, dans les ressources complémentaires ci-après).
- Collaborer avec d'autres organisations, internationales et locales, afin de partager les ressources propices au renforcement des capacités de sécurité, y compris une formation sécurité interagences, directement ou via des tiers, par exemple des consultants indépendants ou des formateurs sécurité.



Il est important que les partenaires suivent et évaluent les activités de renforcement des capacités à court et long terme. Ils pourront pour cela passer régulièrement en revue le **plan d'action en vue de l'examen conjoint de la GRS**.



OUTIL 4. Modèle de plan d'action en vue de l'examen conjoint de la GRS

Adapter les activités de renforcement des capacités en fonction des facteurs externes

Certains facteurs environnementaux et sécuritaires peuvent rendre les activités de renforcement des capacités plus complexes. Les stratégies doivent faire preuve de souplesse, en s'adaptant à l'évolution rapide de chaque situation. Les organisations devront tenir compte des besoins des collaborateurs les plus vulnérables.

Le défi du débauchage de personnel

L'une des conséquences malencontreuses du renforcement des capacités peut être de rendre les personnels locaux plus attractifs aux yeux des organisations, et plus spécialement des ONGI, qui offrent des salaires plus élevés. Une ONG L/N peut avoir du mal à concurrencer une ONGI en tant qu'employeur, surtout si son financement de base est peu élevé, ce qui peut affecter sa capacité à fidéliser une équipe centrale solide.

Ce point mérite que les partenaires en discutent dans le cadre de l'agenda plus général de la **localisation**. La charte Charter4Change, avalisée par plusieurs centaines d'organisations, exige des signataires qu'ils indemnisent équitablement (par exemple en versant des honoraires de recrutement) les organisations locales s'ils embauchent des membres de leur personnel dans un cadre humanitaire.



Complément d'information

- *EISF – Security Management and Capacity Development: International agencies working with local partners (notamment l'annexe 1)*
- *EISF – Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*
- *ODI – From the Ground Up*
- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*
- *GISF – Developing a 'COVID-19 Secure' HEAT course*
- *Site de GISF – plateforme de formation*
- *CICR – Safer Access Framework*

Les plateformes suivantes proposent une formation gratuite à la sécurité personnelle et à la gestion du risque sécurité :

- *Site de l'INSSA*
- *Plateforme DisasterReady*
- *UNDSS*
- *Formation Stay Safe du FICR*
- *Kaya Connect*

Pour mesurer la maturité d'une organisation en matière de gestion du risque sécurité sous l'angle du *duty of care*, voir :

- *EISF et cinfo – Duty of Care Maturity Model*
- *cinfo – Duty of Care Maturity Model Tool*



Plaidoyer en faveur du changement : améliorer la sécurité dans le secteur de l'aide humanitaire au moyen du partenariat



4.1. Mener un plaidoyer conjoint

« Une voix qui s'exprime clairement, avec des preuves à l'appui, qui représente de nombreux acteurs, et dont l'avis est partagé par un grand nombre, est une voix puissante à même d'influencer les tierces parties et les cibles. »

ICVA – NGO Fora Advocacy Guide

Le plaidoyer est une démarche qui consiste à influencer le changement. Dans le cadre d'un partenariat, il peut arriver que les organisations découvrent des problèmes sécuritaires qui dépassent leurs capacités. Ils devront donc envisager des activités de plaidoyer collectives.

Les objectifs d'un plaidoyer axé sur la sécurité peuvent être les suivants :

- Placer la gestion du risque sécurité au cœur des discussions programmatiques, au lieu de la traiter comme une question secondaire.
- Inclure les points focaux sécurité dans les débats stratégiques et de haut niveau.
- Inclure la gestion du risque sécurité dans les discussions sur l'agenda de la **localisation**.
- Veiller à ce que les donateurs répondent aux besoins de financement de la GRS des deux organisations partenaires.
- Permettre aux deux partenaires d'accéder plus facilement aux ressources, collaborations et réseaux axés sur la sécurité.

Les organisations partenaires sont particulièrement bien placées pour participer aux activités de plaidoyer car elles peuvent s'attaquer à ces défis ensemble et s'appuyer sur leurs forces mutuelles pour exercer une influence.

Elles peuvent élaborer une stratégie de plaidoyer conjointe en identifiant

les objectifs, cibles, messages, alliés et opportunités communs, et ce, de manière formelle (directives présentées dans le schéma 5 ci-après), ou informelle :

1. En identifiant ensemble les changements que les partenaires souhaitent voir intervenir.
2. En se faisant des alliés au sein de chaque organisation, aussi bien au sein du partenariat qu'en dehors de celui-ci.
3. En s'exprimant d'une seule voix, en s'appuyant sur les connaissances et les preuves recueillies.



Le personnel du plaidoyer et les points focaux sécurité des deux organisations partenaires doivent collaborer afin que les activités de plaidoyer s'appuient sur les compétences et les connaissances des experts de la sécurité.

Efforts de plaidoyer distincts

Pour les organisations, le partenariat offre une opportunité unique de prendre part à un plaidoyer commun, mais elles peuvent aussi juger utile de participer à des efforts de plaidoyer distincts.

Les ONGI, par exemple, sont souvent mieux placées auprès des donateurs et en tant que membres de groupes internationaux de plaidoyer pour défendre une cause au nom des ONG L/N. Les ONGI doivent tirer parti de leur influence pour promouvoir une meilleure sécurité pour les ONG L/N, par exemple en plaidant auprès des donateurs en faveur de budgets de sécurité appropriés.



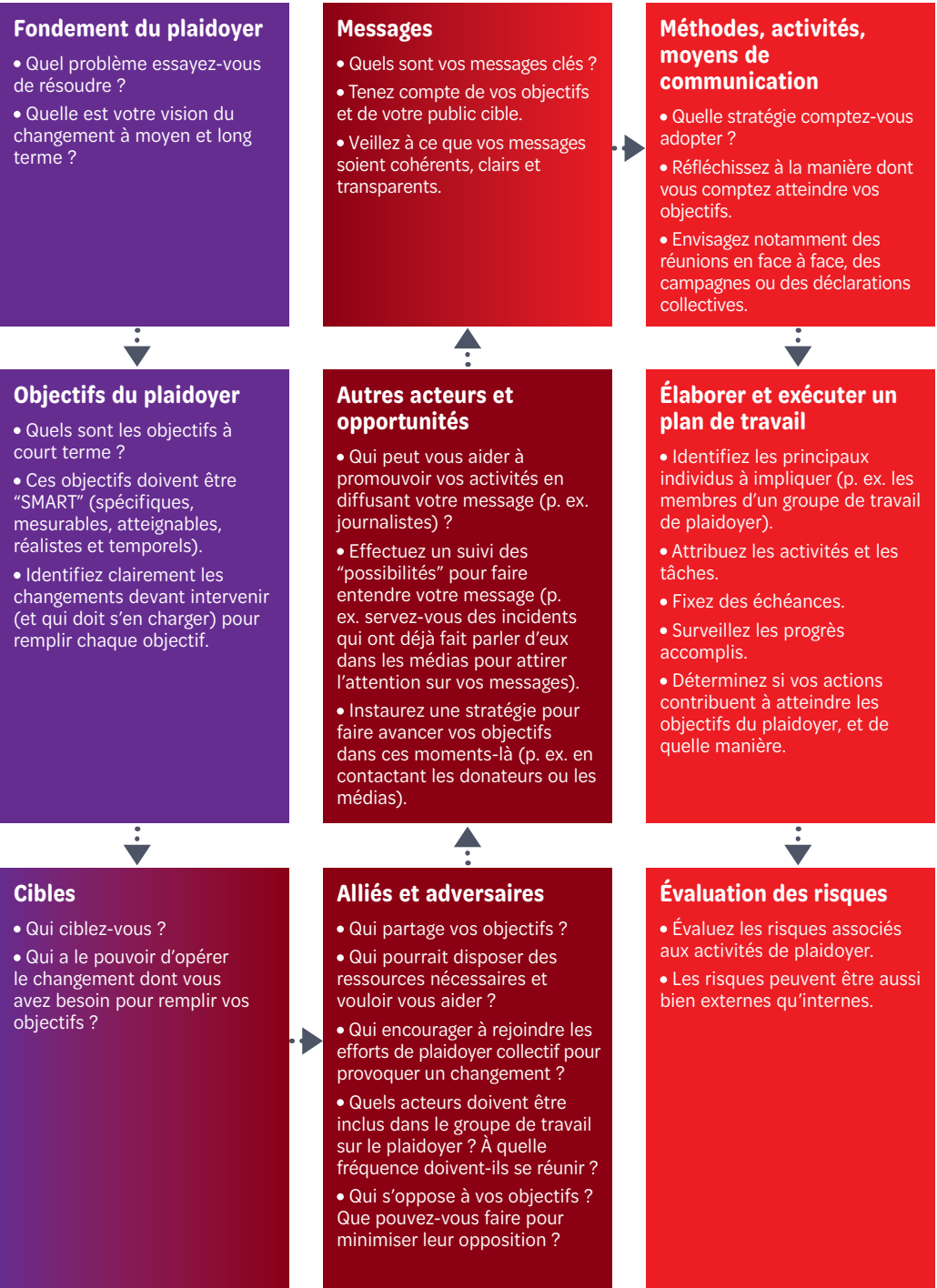
Il incombe aux ONGI de tirer parti de leur position pour mener un plaidoyer au nom des ONG L/N.

Quant aux ONG L/N, elles peuvent lancer leurs propres activités de plaidoyer, par exemple pour modifier leurs relations avec leurs partenaires internationaux si ceux-ci ne répondent pas à leurs besoins.



Il est conseillé aux ONG L/N d'élaborer un agenda du plaidoyer de manière indépendante ou avec d'autres ONG L/N afin de plaider en faveur du changement si les acteurs internationaux, y compris leurs partenaires d'ONGI, n'accèdent pas à leurs requêtes.

Schéma 5. Stratégie de plaidoyer : principales étapes et questions



Adapté du manuel 'NGO Fora Advocacy Guide' de l'ICVA

4.2. Gestion du risque sécurité et actions de plaidoyer

Cette partie illustre les différentes manières dont les organisations peuvent prendre part à un plaidoyer sur la sécurité ; elle indique aussi les défis qu'un plaidoyer sécuritaire peut contribuer à résoudre.

4.2.1. Protéger les travailleurs humanitaires des attaques ciblées

À travers leur collaboration, les organisations humanitaires peuvent attirer l'attention sur les risques de sécurité auxquels leur personnel est confronté et réclamer une protection accrue. Le mouvement **NotATarget** est un exemple de ce type d'efforts (dans les médias sociaux, les activités liées à ce mouvement utilisent le hashtag #NotATarget).

Une collaboration entre organisations humanitaires – et en particulier entre acteurs internationaux et locaux – est essentielle à cet égard. Une grande partie des travaux utilisés pour mettre en évidence les attaques contre les personnels de santé s'appuient sur des preuves provenant de sources locales. Par exemple, les rapports du Syrian Network for Human Rights rendent compte d'attaques visant les civils, les professionnels de santé et d'autres victimes. Ces preuves permettent à l'organisation et à ses partenaires de plaider en faveur d'une protection accrue des civils et des autres acteurs non combattants, y compris des personnels de santé, en Syrie.



Démontrer l'existence du risque sécurité peut renforcer le message et contribuer à répondre aux objectifs du plaidoyer.

Même si cet exercice n'est au départ pas conçu pour contribuer au plaidoyer, le fait de recueillir des données sur les incidents de sécurité affectant le personnel de différentes organisations permet d'identifier des tendances et de démontrer les défis sécuritaires, ce qui peut encourager des efforts de plaidoyer collectifs. Par exemple, l'organisation Safeguarding Health in Conflict Coalition se sert des données relatives aux incidents de sécurité signalés par différentes organisations pour plaider en faveur d'une protection accrue des personnels de santé dans les environnements de conflit. Le regroupement des données d'incidents émanant de diverses organisations est important pour ces activités.

Signalons aussi qu'en cas d'incident grave, les partenaires peuvent décider de lancer un plaidoyer commun. Par exemple, en août 2020, sept membres du personnel de l'ONG ACTED ont été tués dans des circonstances tragiques au Niger. Cet incident a conduit ACTED à lancer

un appel mondial à l'action afin d'améliorer la protection des travailleurs humanitaires. Soixante-trois organisations se sont jointes à cet appel, et des dialogues de haut niveau s'en sont suivis avec le gouvernement français et les Nations Unies sur les questions du respect du droit humanitaire international et de l'amélioration de la protection des personnels humanitaires.

4.2.2. Plaidoyer en faveur de la gestion du risque sécurité et agenda de localisation

Les organisations internationales et locales peuvent aussi envisager de mener un plaidoyer afin de mieux comprendre les défis sécuritaires et de mieux orienter les efforts au sein d'un partenariat. L'accord du Grand Bargain et l'agenda de **localisation** ont largement cherché à octroyer aux ONG L/N un pouvoir de décision accru dans l'espace humanitaire. Ce mouvement a été appuyé par des initiatives telles que Charter4Change et Alliance for Empowering Partnership (A4EP). Il n'a toutefois pas conduit à un dialogue plus poussé sur les besoins de sécurité des ONG L/N dans l'agenda de localisation ou le secteur de l'aide en général. Il s'agit là d'une faille significative et très révélatrice.

Les équipes de plaidoyer qui travaillent sur l'agenda de localisation des deux organisations partenaires devront collaborer avec les points focaux sécurité pour défendre une meilleure prise en compte et un dialogue plus poussé autour du risque sécurité des ONG L/N. Il pourrait par exemple s'agir de mieux inclure la gestion du risque sécurité dans les outils de localisation, comme le *Cadre de mesure de la performance de la localisation* de l'ONG NEAR.

4.2.3. Plaidoyer en faveur de la gestion du risque sécurité et financement

Les organisations ont besoins de budgets GRS suffisants et dédiés. Cependant, la question du financement est de plus en plus compliquée pour les organisations, notamment pour les ONG L/N, et les fonds octroyés sont souvent insuffisants. Afin d'obtenir un financement de la sécurité adéquat, les organisations devront éventuellement mener des travaux de plaidoyer ciblant leurs partenaires ou donateurs, soit en tant qu'organisations individuelles, soit au moyen d'un plaidoyer collectif.

Les organisations qui craignent d'exprimer aux donateurs et aux partenaires leurs préoccupations quant à l'inadéquation de leur financement de la GRS pourront préférer peut-être participer à des campagnes de plaidoyer collectives avec d'autres ONG. Les ONG L/N,

par exemple, pourraient se servir de plateformes telles que celle de NEAR pour plaider auprès de leurs partenaires d'ONGI en faveur d'un financement adéquat de la sécurité.



Les ONGI qui peinent à financer la sécurité doivent inclure dans leur plaidoyer auprès des donateurs un soutien en faveur de la gestion du risque sécurité, aussi bien pour elles-mêmes que pour leurs ONG L/N partenaires.

Pour être efficace, la stratégie de plaidoyer doit présenter clairement les besoins et les insuffisances du financement sécurité des deux partenaires. À cet égard, il sera utile que les points focaux sécurité fournissent à leurs confrères du plaidoyer des exemples de défis sécuritaires susceptibles d'apparaître si les fonds alloués à la sécurité sont insuffisants.

► Voir 3.2, *Financer la gestion du risque sécurité au sein du partenariat*

Exemple – la campagne « At What Cost »

En juillet 2019, GISF (alors appelé EISF) a lancé la campagne « At What Cost? » (À quel coût ?) pour attirer l'attention sur l'insuffisance des fonds dédiés à la sécurité dans le secteur de l'aide. La lettre ouverte de cette campagne remettait en question la pratique qui veut qu'un pourcentage arbitraire soit attribué à la sécurité dans les budgets – pratique qui ne tient pas compte de la diversité des contextes, des opérations, des organisations et des risques auxquels les organisations humanitaires sont confrontées. Cette lettre réclamait l'inclusion de lignes budgétaires dédiées et explicites en faveur de la sûreté du personnel et de la sécurité, avec des messages clés adaptés en fonction du groupe cible :

« EISF [...] demande au secteur de l'aide de relancer le débat sur le financement de la gestion du risque sécurité afin que la sûreté du personnel et la sécurité ne soient pas exclues des budgets. Travailleurs humanitaires, quel que soit le niveau auquel vous œuvrez, interrogez-vous sur la manière dont le coût réel de votre sécurité est inclus dans les budgets des programmes. Responsables de la sécurité, faites pression sur votre organisation pour que la sûreté et la sécurité deviennent des lignes budgétaires directes. Donateurs, coordonnez votre action avec les organisations non





Exemple – la campagne « At What Cost » suite

gouvernementales afin de réformer les processus de financement dédiés à la gestion du risque sécurité. »

Lettre ouverte d'EISF aux organisations non gouvernementales et donatrices

Cette lettre ouverte a été signée par près de 200 parties prenantes œuvrant dans 38 pays du monde entier. En appelant les donateurs, les responsables sécurité et tous les travailleurs humanitaires à prendre davantage conscience de la situation et à réclamer un financement adéquat de la sécurité, cette lettre a réussi à sensibiliser et à provoquer des changements concrets. À l'issue de la campagne, le ministère britannique des Affaires étrangères, du Commonwealth et du Développement (DFID) a annoncé qu'il actualiserait le modèle et les conseils associés à sa facilité de réponse rapide afin d'inclure une ligne spécifiquement dédiée à la gestion du risque sécurité.

Complément d'information

- *Oxfam et Open University – formation Make Change Happen*
- *ICVA – NGO Fora Advocacy Guide*
- *Working Group on Protection of Humanitarian Action – Toolkit: Responding to Violence against Humanitarian Action on the Policy Level*
- *Call for Action for Safeguarding of Humanitarian Space and Ending Impunity for Attacks against Humanitarians*
- *GISF – How to effectively advocate for aid workers' protection?*
- *RedR UK, Insecurity Insight et EISF – Manuel de gestion de l'information issue des incidents de sécurité (en particulier 4.5, Utilisation de l'information issue des incidents de sécurité pour le plaidoyer stratégique)*
- *NEAR – Localisation Performance Measurement Framework*
- *Syrian Network for Human Rights*
- *Safeguarding Health in Conflict Coalition*

- *Reflections on GISF's 'At What Cost?' Campaign*
- *An open letter to non-governmental and donor organisations from the European Interagency Security Forum*

Exemples d'organisations et d'initiatives impliquées dans le travail de localisation :

- *NEAR*
- *Ressources Charter4Change*
- *A4EP*

5 Outils

- **Outil 1**
Une communication de qualité au sein du partenariat
- **Outil 2**
Attitude face au risque au sein du partenariat
- **Outil 3**
Modèle de questionnaire et de feuille de travail en vue de l'examen conjoint de la GRS
- **Outil 4**
Modèle de plan d'action en vue de l'examen conjoint de la GRS
- **Outil 5**
Modèle d'évaluation et de plan de gestion conjoints du risque sécurité
- **Outil 6**
Modèle de budget dédié à la gestion du risque sécurité au sein du partenariat



Outil 1. Une communication de qualité au sein du partenariat

Cet outil sert à évaluer la qualité des communications au sein des accords de partenariat.

Les contextes et les risques de sécurité sont souvent sources de malentendus entre partenaires. Les barrières linguistiques et les différences culturelles de communication sont particulièrement problématiques si l'on veut mener des discussions utiles et approfondies sur les risques de sécurité (cultures orales contre cultures écrites, absence de contacts en face à face). Qui plus est, le personnel qui opère dans le domaine de la sécurité s'exprime souvent dans un jargon bien particulier, avec des concepts difficiles à traduire dans les différentes langues.

Les partenaires devront régulièrement passer en revue la qualité de leur communication et identifier les principaux obstacles à leurs échanges. Cet outil doit les aider à améliorer leur communication, ou à évaluer et comparer les différentes stratégies de communication et résoudre tout malentendu.

Exercice – Évaluer la qualité de votre communication (par exemple courriels, courriers, appels téléphoniques, réunions en face à face)

1. La communication est-elle claire ?
2. La communication évite-t-elle l'emploi de jargon et d'acronymes ?
3. La communication sur les motivations et les objectifs est-elle transparente (autrement dit, est-il facile de comprendre la raison pour laquelle vous communiquez et ce que vous espérez en retirer ?) ?
4. Le mode de communication est-il adapté au destinataire ?
5. La communication est-elle respectueuse, équitable et sensible sur le plan culturel (en évitant un langage négatif, exigeant ou trop autoritaire) ?
6. La communication témoigne-t-elle d'une certaine compassion à l'égard des circonstances particulières du destinataire et de l'organisation dans son ensemble ?

Évaluation – Passer en revue la communication au sein du partenariat d'une manière plus générale

1. Une confiance mutuelle est-elle manifeste dans les communications entre partenaires ?
2. L'information est-elle partagée de manière proactive entre les partenaires ?
3. Les partenaires cherchent-ils à obtenir un retour réciproque régulier, aussi bien formellement qu'informellement, y compris sur l'efficacité de la communication entre eux ?
4. Les produits de la communication sont-ils nécessaires ou excessifs ?
5. Les partenaires assument-ils ce qui a été dit ou fait ?
6. La communication est-elle cohérente ? (en termes de fréquence, de teneur et d'attentes de chaque partenaire)
7. La communication parvient-elle jusqu'aux personnes appropriées ? Si ce n'est pas le cas, pourquoi ? Explorer les barrières culturelles ou linguistiques.
8. Un interlocuteur peut-il être mis en place pour renforcer la communication entre les partenaires ?

Exercice – Évaluer la qualité de votre communication (par exemple courriels, courriers, appels téléphoniques, réunions en face à face)
suite

7. La communication est-elle pertinente pour tous les destinataires ? Si elle ne l'est pas, que faire pour qu'elle le devienne ? (P. ex., certains collaborateurs sont susceptibles de trouver qu'il est superflu d'être impliqués dans les discussions sur la sécurité s'ils n'ont pas de responsabilités en matière de sécurité ou s'ils opèrent dans une zone à faible risque.)

Évaluation – Passer en revue la communication au sein du partenariat d'une manière plus générale
suite

9. Les partenaires peuvent-ils chercher ensemble à résoudre les préoccupations relatives à la sécurité numérique susceptibles d'empêcher le personnel d'utiliser des plateformes de communication particulières ? (En effet, dans certains contextes, les courriels et appels téléphoniques peuvent être interceptés par des acteurs gouvernementaux.)
10. Si la sécurité de certains modes de communication pose problème, existe-t-il d'autres formes (par exemple en face à face) auquel l'ensemble du personnel peut accéder ?

► Voir 1.4 pour de plus amples informations sur une communication de qualité



Outil 2.
Attitude face au risque au sein du partenariat

Cet outil permet aux partenaires d'étudier et d'élaborer une conception commune de l'attitude face au risque et du niveau d'acceptation de celui-ci. Il leur servira à lancer une discussion permanente et devra être passé en revue régulièrement.

Étape 1 : Définir le niveau de probabilité et l'impact

La gravité d'un risque dépend d'abord de la probabilité de l'événement ; et si cet événement venait à se produire, quelle serait la gravité de son impact ? Les partenaires devront débattre de ce qu'ils entendent concrètement par « probabilité » et « impact » en définissant chacune des catégories d'impact et de probabilité (ci-après). Cette discussion les amènera à comparer les risques à partir d'une conception similaire. Par exemple, un partenaire pourrait considérer qu'un événement « improbable » risque de se produire une fois par mois, tandis que pour l'autre partenaire, cela pourrait signifier une fois par an. Lors de cet exercice, les partenaires devront tenir compte du personnel, des équipements et des programmes pertinents.

PROBABILITÉ		DÉFINITIONS
1	Très improbable	Par exemple : plus d'une fois tous les dix ans Moins d'une fois par an
2	Improbable	
3	Modérément probable	
4	Probable	
5	Très probable	

IMPACT		DÉFINITIONS
1	Négligeable	Par exemple : Personnel : un membre du personnel légèrement blessé Équipement : perte d'équipement non essentiel Programme : perte temporaire d'accès en raison de difficultés météorologiques
2	Faible	
3	Modéré	
4	Grave	
5	Critique	

Étape 2 : Élaborer une matrice afin de convenir des niveaux de risque acceptables

Les partenaires pourront employer une matrice pour comparer la probabilité d'un incident à son impact (parfois calculé de manière numérique sous la forme Probabilité x Impact) afin de déterminer, pour chaque partenaire, le niveau de risque acceptable au sein du partenariat. Les niveaux de risque acceptables apparaîtront en vert. La matrice ci-dessous n'est donnée qu'à titre d'exemple ; le niveau d'acceptation du risque sera différent pour chaque organisation/partenariat et il faudra donc adapter l'évaluation de l'acceptation du risque aux besoins.

PROBABILITÉ	IMPACT				
	Négligeable = 1	Faible = 2	Modéré = 3	Grave = 4	Critique = 5
Très probable = 5	(1x5) = 5	(5x2) = 10	15	20	25
Probable = 4	4	8	12	16	20
Modérément probable = 3	3	6	9	12	15
Improbable = 2	2	4	6	8	10
Très improbable = 1	1	2	3	4	5



Les partenaires ne doivent pas uniquement se focaliser sur le chiffre obtenu ; ils sont encouragés à s'interroger sur le niveau de risque et à faire une évaluation en fonction de leur réponse.



Outil 3. Modèle de questionnaire et de feuille de travail en vue de l'examen conjoint de la GRS

Ce modèle présente des exemples de questions, suivies d'exemples d'indicateurs, auxquelles les partenaires peuvent répondre ensemble. Les indicateurs peuvent être évalués pour le partenariat dans son ensemble ou par chaque organisation partenaire au moyen d'un système d'évaluation à trois niveaux : présent, partiellement présent ou absent. L'objectif de cet outil est d'encourager une conversation franche et ouverte entre partenaires sur les capacités, les ressources, les lacunes et les besoins en matière de GRS, tant pour chaque organisation que pour le partenariat dans son ensemble. Il reprend des questions et indicateurs déjà présentés dans le chapitre 2.



Il ne s'agit pas d'un « outil de gestion du risque sécurité » mais d'un « outil de gestion du partenariat ». Il n'est pas conçu pour évaluer les forces et les faiblesses du système de gestion du risque sécurité d'une organisation partenaire.

Notez qu'il ne s'agit là que d'exemples de questions et d'indicateurs ; le modèle devra être adapté par les partenaires afin d'inclure des questions et indicateurs correspondant à leurs besoins et situations spécifiques.

► Vous trouverez des questions et indicateurs supplémentaires dans le chapitre 2.

1re partie : *Duty of care*

Réf.	Question	Réponse			Commentaires
1.1.	Quelles sont les obligations légales et morales (<i>duty of care</i>) respectives de chaque partenaire ?	ONG L/N			
		ONGI			
1.2.	Quelles sont les obligations légales et morales (<i>duty of care</i>) de chaque partenaire à l'égard de son personnel, de ses bénéficiaires et des communautés affectées ?	ONG L/N			
		ONGI			
1.3.	Les besoins psychosociaux de l'ensemble du personnel sont-ils pris en compte, et quelles mesures chaque partenaire peut-il prendre pour améliorer le <i>duty of care</i> dont bénéficie les collaborateurs (p. ex. assurance, bien-être psychosocial) ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
1.1.	Les deux partenaires comprennent et remplissent leurs obligations légales au titre du <i>duty of care</i> .	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
1.2.	Les deux partenaires se sont mis d'accord sur les obligations morales au titre du <i>duty of care</i> .				

2e partie : Gouvernance et responsabilité

Réf.	Question	Réponse			Commentaires
2.1.	Les deux partenaires disposent-ils de structures de gestion du risque sécurité adaptées aux objectifs du partenariat ?	ONG L/N			
		ONGI			
2.2.	Les deux partenaires comprennent-ils parfaitement les rôles et responsabilités associés à la gestion du risque sécurité au sein du partenariat et des programmes ? Par exemple, les deux organisations ont-elles un point focal sécurité pouvant servir de principal interlocuteur des partenaires en cas de questions relatives à la sécurité ?	ONG L/N			
		ONGI			
2.3.	De quelle manière chaque partenaire conçoit-il le transfert du risque au sein du partenariat (le cas échéant) ? Quelles mesures chaque partenaire estime-t-il pouvoir prendre pour passer du transfert du risque au partage du risque ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
2.1.	Il existe une déclaration de responsabilité et de gouvernance relative à la gestion du risque sécurité au sein du partenariat.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
2.2.	Il existe un processus de signalement et de responsabilité (dont le contenu et la fréquence ont été définis) pour informer chaque partenaire en cas de problème lié à un risque sécurité. Les responsabilités des deux partenaires à l'égard de la gestion de la sécurité au sein du partenariat y sont clairement définies.				
2.3.	Les deux partenaires disposent d'un point focal explicitement désigné, qui est chargé de la gouvernance du risque sécurité pour l'organisation et le partenariat.				

3e partie : Politique et principes

Réf.	Question	Réponse		Commentaires
3.1.	Les deux partenaires comprennent-ils parfaitement le mandat, la mission, les valeurs et les principes de chaque organisation, et se sentent-ils à l'aise avec le travail de l'autre partenaire et son approche à l'égard des opérations et de la sécurité (p. ex. les partenaires sont-ils d'accord avec leur position respective concernant le plus strict respect des principes humanitaires) ?	ONG L/N		
		ONGI		
3.2.	Les partenaires sont-ils d'accord sur les exigences sécuritaires minimales concrètes devant être en place sur chaque site ou pour chaque activité ? (Bien que ces exigences s'appliquent aux deux partenaires, elles doivent aussi être réalistes et adaptées aux capacités de chaque organisation.)	ONG L/N		
		ONGI		
3.3.	De quelle manière les partenaires définissent-ils et appréhendent-ils l'attitude face au risque, et sont-ils d'accord sur ce qui constitue un seuil de risque acceptable pour le partenariat et les programmes connexes ?	ONG L/N		
		ONGI		

3e partie : Politique et principes *suite*

Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
3.1.	Les politiques de gestion du risque sécurité et leur mise en œuvre (au moyen de plans, de procédures et/ou de directives) sont adaptées au contexte local et aux circonstances du partenariat, et tout le personnel peut y accéder (p. ex. disponibles dans des langues et sous un format pertinent).	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
3.2.	L'accord de partenariat comprend une déclaration commune relative au seuil de risque régissant les activités du partenariat.				
3.3.	L'accord de partenariat est conforme aux politiques de sécurité des deux partenaires – voire les renforce (p. ex. dispositions relatives à l'emploi d'escortes armées).				

4e partie : Opérations et programmes

Réf.	Question	Réponse		Commentaires
4.1.	Quels sont les besoins et attentes de chaque partenaire en matière de sécurité ?	ONG L/N		
		ONGI		
4.2.	Les partenaires se sont-ils mis d'accord sur un système permettant d'identifier et de contrôler les risques de sécurité auxquels le personnel est exposé ? (Constate-t-on une cohérence entre les évaluations du risque sécurité et les plans de sécurité des deux organisations sur les sites où opère le partenaire d'exécution ? Quelles sont les divergences, et pourquoi ?)	ONG L/N		
		ONGI		
4.3.	Les partenaires se sont-ils mis d'accord sur les individus à qui confier la gestion des risques identifiés, et sur la manière dont ces individus doivent être supervisés et financés ?	ONG L/N		
		ONGI		

4e partie : Opérations et programmes *suite*

Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
4.1.	Une évaluation conjointe du risque sécurité lié aux opérations, ainsi que des risques associés et de l'impact pour chaque partenaire a été réalisée, et un processus clair est en place pour l'actualiser régulièrement. L'évaluation comprend une analyse des risques internes et des risques pouvant résulter du partenariat à proprement parler.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
4.2.	Il existe dans le budget du partenariat des lignes budgétaires explicites pour répondre aux besoins sécuritaires, y compris pour des activités de renforcement des capacités, et ces lignes budgétaires sont jugées suffisantes pour répondre à tous les besoins de ressources des deux partenaires.				
4.3.	Les partenaires se sont mis d'accord sur des stratégies ou des approches sécuritaires spécifiques au contexte, qui ont été communiquées à l'ensemble des services pertinents de chaque organisation.				

5e partie : Gestion des déplacements et support

Réf.	Question	Réponse	Commentaires
5.1.	Comment gérer les risques de sécurité découlant des déplacements effectués dans le cadre du partenariat ? Quelles doivent être les exigences minimales en termes de gestion des déplacements et d'accords de support (pour les déplacements sur le terrain, l'hébergement de nuit, les procédures de communication et toute autre forme de support) ? Par exemple briefings d'information, procédures pour signaler sa présence, entretien des véhicules, évaluations des risques posés par les déplacements, formation des conducteurs, gestion des informations de déplacement confidentielles.	ONG L/N	
		ONGI	
5.2.	Le soutien apporté au personnel des deux organisations sur les sites de projet en matière de déplacements et d'hébergement est-il équitable ?	ONG L/N	
		ONGI	
5.3.	Les partenaires sont-ils d'accord sur la politique et les procédures de sécurité à observer lors des déplacements des partenaires, et sur l'entité chargée du <i>duty of care</i> dont font l'objet les collaborateurs de passage ?	ONG L/N	
		ONGI	

5e partie : Gestion des déplacements et support *suite*

Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
5.1.	Les partenaires sont d'accord sur les dispositions et responsabilités s'appliquant à la sécurité lors des visites de personnels des deux organisations vers leurs bureaux et sites de programme.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
5.2.	Les partenaires communiquent entre eux les procédures de sécurité s'appliquant aux visites de personnel pertinentes pour le partenariat (p. ex. informations sur les rôles et responsabilités, formations, briefings, procédures pour signaler sa présence et procédures d'urgence).				
5.3.	La diversité des risques et besoins de sécurité des personnels en déplacement est prise en compte dans les procédures régissant les déplacements, par exemple si le risque est plus élevé en raison des caractéristiques personnelles de certains individus (genre, ethnicité, handicap, etc.).				

6e partie : Sensibilisation et renforcement des capacités

Réf.	Question	Réponse			Commentaires
6.1.	De quelle manière les partenaires comptent-ils identifier les besoins en matière de sensibilisation à la sécurité et de renforcement des capacités dans ce domaine, et y répondre ensemble (aussi bien en termes de sécurité personnelle que de gestion du risque sécurité) ?	ONG L/N			
		ONGI			
6.2.	Les deux partenaires sont-ils d'accord sur les lacunes qu'il leur faut combler en termes de capacités de gestion du risque sécurité, et sur ce que chaque organisation peut faire pour y remédier ?	ONG L/N			
		ONGI			
6.3.	Le budget du partenariat comprend-il des fonds pour des activités de renforcement des capacités sur le long terme ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
6.1.	Les partenaires sont d'accord sur leurs besoins de capacités en matière de GRS.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
6.2.	Il existe une stratégie d'apprentissage, de développement et de renforcement des capacités, assortie d'un plan de mise en œuvre clair, dont l'objectif est d'améliorer les capacités des partenaires sur le long terme.				
6.3.	L'organisation partage régulièrement ses ressources avec ses partenaires et soutient l'accès aux opportunités de renforcement des capacités, d'apprentissage et de développement en matière de gestion du risque sécurité.				

7e partie : Suivi des incidents

Réf.	Question	Réponse		Commentaires
7.1.	De quelle manière les partenaires doivent-ils partager entre eux l'information sur les incidents ?	ONG L/N		
		ONGI		
7.2.	Comment les partenaires peuvent-ils s'entraider en matière de gestion des informations sur les incidents de sécurité ? Par exemple, au moyen de procédures de signalement des incidents, de systèmes d'enregistrement des incidents et d'outils d'analyse des données d'incident afin d'éclairer les décisions dans les domaines de la sécurité, des programmes, des opérations, du plaidoyer, du financement, etc.	ONG L/N		
		ONGI		
7.3.	Sur chaque site, à quelles données d'incidents de sécurité chaque organisation peut-elle accéder, soit à travers ses propres opérations, soit par le biais de ses réseaux, et pouvant être partagé régulièrement avec son partenaire ?	ONG L/N		
		ONGI		

7e partie : Suivi des incidents *suite*

Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
7.1.	Il existe une procédure de gestion et de partage de l'information de sécurité (y compris des données d'incidents) entre les partenaires pour le contexte opérationnel, et cette procédure est respectée.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
7.2.	Les partenaires sont d'accord sur la façon dont les données d'incident doivent éclairer les décisions, y compris à travers une politique indiquant clairement si des sanctions peuvent être prises suite au signalement ou au non-signalement d'un incident.				
7.3.	L'organisation passe périodiquement en revue les incidents qui affectent son personnel afin d'identifier les tendances et les préoccupations, et elle en fait part aux organisations partenaires.				

8e partie : Gestion de crise

Réf.	Question	Réponse			Commentaires
8.1.	De quelle manière les partenaires comptent-ils collaborer/coordonner leurs actions en cas de crise ou d'incident critique les affectant sur le site concerné ?	ONG L/N			
		ONGI			
8.2.	En cas de crise ou d'incident critique qui affecte les deux partenaires, qui doit se charger de la réponse de gestion de crise ? Quelles sont les responsabilités et qui a l'autorité de prendre les décisions ?	ONG L/N			
		ONGI			
8.3.	Quel support chaque partenaire peut-il apporter à l'autre en cas d'incident critique sur le site du partenariat ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
8.1.	Il a été convenu des responsabilités et de l'autorité de décision en cas de crise ou d'incident critique affectant les deux partenaires, dans l'idéal par écrit ou sous forme imagée (par ex. organigramme).	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
8.2.	Les partenaires disposent d'une structure et d'un plan de gestion de crise.				
8.3.	Les partenaires ont accès à des services de support d'urgence (médicale et non médicale) dans le cadre de l'assurance contractée par chaque organisation.				

9e partie : Collaborations et réseaux dans le domaine de la sécurité

Réf.	Question	Réponse			Commentaires
9.1.	Existe-t-il des plateformes qui traitent des questions de sécurité ? Si oui, les deux partenaires y ont-ils accès et peuvent-ils s'y exprimer de manière égale dans leurs domaines opérationnels (y compris plateformes de partage de l'information) ?	ONG L/N			
		ONGI			
9.2.	Quels obstacles et défis empêchent une participation active des deux partenaires aux forums, réunions et discussions interagences sur la sécurité aux niveaux local, national, régional et international ?	ONG L/N			
		ONGI			
9.3.	Quelles mesures chacune des deux organisations peut-elle prendre pour inclure son partenaire dans ces discussions ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
9.1.	Les deux partenaires participent activement aux forums, plateformes, réunions et consortiums sur la gestion du risque sécurité, et ils partagent l'information sur la sécurité avec d'autres acteurs aux niveaux local, national, régional et/ou international.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
9.2.	Dans la mesure du possible, les deux organisations encouragent et facilitent la participation de leurs partenaires aux forums, plateformes, réunions et discussions interagences afin de renforcer le partage de l'information et la collaboration dans le domaine de la sécurité. Elles fournissent à leur partenaire les coordonnées d'acteurs propices à la gestion du risque sécurité.				

10e partie : *Compliance* et suivi de l'efficacité

Réf.	Question	Réponse			Commentaires
10.1.	Comment les deux partenaires doivent-ils s'y prendre pour passer en revue régulièrement la gestion du risque sécurité au sein du partenariat ?	ONG L/N			
		ONGI			
10.2.	Quel niveau de <i>compliance</i> et de suivi de l'efficacité de la GRS au sein de chaque organisation et/ou du partenariat est acceptable pour les deux partenaires ?	ONG L/N			
		ONGI			
10.3.	Quelle quantité d'informations les partenaires sont-ils prêts à partager entre eux concernant les enseignements, les examens, les audits sécurité et l'analyse post-incident propres au contexte, au partenariat ou à un projet particulier ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
10.1.	Les enseignements, les examens, les analyses post-incident et les audits sécurité relatifs au contexte, au partenariat ou au projet/programme sont partagés entre partenaires et font l'objet de discussions.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
10.2.	Les collaborateurs chargés de contrôler la mise en œuvre des systèmes de sécurité et leur utilisation conforme (au sein de chaque organisation et du partenariat) sont formés de manière appropriée, ont été impliqués dans l'examen conjoint de la GRS, et ces responsabilités sont explicitement indiquées dans leur descriptif de poste.				
10.3.	Les systèmes de gestion de la performance des employés font explicitement référence aux responsabilités en matière de sécurité et au respect des politiques de l'organisation.				

11e partie : Ressources complémentaires

Réf.	Question	Réponse	Commentaires		
11.1.	Des ressources complémentaires sur la gestion du risque sécurité sont-elles disponibles et l'ensemble du personnel peut-il y accéder ? Dans le cas contraire, quelles mesures prendre pour en améliorer l'accessibilité ?	ONG L/N			
		ONGI			
11.2.	Les partenaires ont-ils partagé entre eux leurs ressources en matière de gestion du risque sécurité ?	ONG L/N			
		ONGI			
11.3.	De quelles autres ressources les partenaires bénéficieraient-ils pour mieux gérer leurs risques de sécurité ?	ONG L/N			
		ONGI			
Réf.	Indicateur d'évaluation	Partenariat	ONG L/N	ONGI	Commentaires et preuves
11.1.	Les ressources relatives à la gestion du risque sécurité qui répondent aux besoins de tous les collaborateurs pertinents des partenaires sont régulièrement partagées sous un format accessible à tous.	<i>Critère non rempli</i>	<i>Critère rempli</i>	<i>Critère partiellement rempli</i>	
11.2.	Les partenaires mettent à disposition toute une série d'orientations, d'outils et de modèles dans un registre dédié à la sécurité pour pouvoir s'entraider dans la gestion du risque sécurité.				



Outil 4.

Modèle de plan d'action en vue de l'examen conjoint de la GRS

Ce modèle de plan d'action aidera les partenaires à convenir des mesures à prendre pour combler les lacunes identifiées lors de l'évaluation des indicateurs de la gestion du risque sécurité. Inutile d'inclure dans ce plan d'action les indicateurs dont on estime qu'ils étaient présents lors de l'exercice d'évaluation.



Le plan d'action en vue d'un examen conjoint de la GRS aidera les partenaires à mettre en œuvre le processus d'examen conjoint de la GRS présenté dans ce guide. Il s'agit donc d'un outil de gestion du partenariat, et non d'un outil de gestion du risque sécurité à proprement parler.

1e partie : Duty of care

Référence		Noter le numéro de référence de l'indicateur.
Indicateurs		Noter le nom de l'indicateur.
Évaluation	Partenariat	Présent
	ONG L/N	Partiellement présent
	ONGI	Absent
Priorité		Urgent/ Moyennement urgent/ Non urgent
Mesures requises		Indiquer les mesures requises pour combler les lacunes. Déterminer s'il existe des fonds suffisants pour mettre en œuvre les mesures pertinentes.
Responsable		Identifier un individu ou un service au sein de l'organisation partenaire qui sera responsable de cette mesure.
Échéance		Fixer une échéance réaliste.
Date du passage en revue		Convenir de la date à laquelle les deux partenaires devront passer en revue les progrès accomplis.

2e partie : Gouvernance et responsabilité

Référence	Par exemple : 2.2.	
Indicateurs	Par exemple : Il existe un processus de signalement et de responsabilité (dont le contenu et la fréquence ont été définis) pour informer chaque partenaire en cas de problème lié à un risque sécurité.	
Évaluation	Partenariat	Par exemple : Présent
	ONG L/N	Par exemple : Absent
	ONGI	Par exemple : Sans objet
Priorité	Par exemple : Urgent	
Mesures requises	Par exemple : Convenir d'un processus et l'élaborer dans le cadre du groupe de travail du partenariat sur la sécurité. Des fonds ou autres ressources complémentaires ne sont pas nécessaires.	
Responsable	Par exemple : Groupe de travail du partenariat sur la sécurité (noter les noms)	
Échéance	Par exemple : au plus tard le 15 février 2022	
Date du passage en revue	Par exemple : mars 2022, réunion mensuelle	

3e partie : Politique et principes**4e partie : Opérations et programmes****5e partie : Gestion des déplacements et support****6e partie : Sensibilisation et renforcement des capacités****7e partie : Suivi des incidents****8e partie : Gestion de crise****9e partie : Collaborations et réseaux dans le domaine de la sécurité****10e partie : Compliance et suivi de l'efficacité****11e partie : Ressources complémentaires****Outil 5.****Modèle d'évaluation et de plan de gestion conjoints du risque sécurité**

Ce modèle d'évaluation et de plan de gestion conjoints du risque sécurité permet aux partenaires de préciser ensemble les risques auxquels ils sont exposés et la manière dont chacun d'eux est susceptible d'être affecté par le partenariat ; il permet aussi de trouver des moyens d'atténuer les menaces identifiées. Cet outil servira à lancer une discussion durable pour les partenaires, et il devra être revu régulièrement.



Il s'agit là d'un exemple de modèle ; chaque partenariat évaluera les risques de sécurité à sa manière. Cet outil est différent de l'« examen conjoint de la GRS » présenté dans ce guide. En effet, il sert à identifier et gérer les risques de sécurité concrets – c'est donc un « outil de gestion du risque sécurité » –, alors que l'« examen conjoint de la GRS » et les outils connexes permettent de réfléchir à la GRS d'une manière plus générale au sein des accords de partenariat – on parlera alors d'« outil de gestion du partenariat ».

Étape 1 : Évaluer les risques

1.1. Identifier les menaces.

1.2. Réfléchir aux menaces externes à chaque organisation (p. ex. enlèvement, vol à main armée), aux menaces internes à chaque organisation et aux menaces internes au partenariat (p. ex. harcèlement, fraude).

1.3. Réfléchir à la manière dont chaque partenaire est affecté par cette menace. Quelles sont les similitudes et les différences ?

1.4. Réfléchir aux différents degrés de vulnérabilité de chaque partenaire face aux menaces, et déterminer si cette vulnérabilité est affectée par la relation entre les partenaires (p. ex. si des personnels internationaux d'une origine ethnique particulière sont détachés auprès de l'organisation locale).

1.5. Étudier les différents impacts des menaces sur chaque partenaire, et

voir si les impacts sont affectés par le partenariat (p. ex. changements au niveau des perceptions des communautés locales du fait du partenariat – affiliations politiques, richesse).

1.6. Au moyen d’une matrice des risques dont il aura été convenu, évaluer la probabilité et l’impact et déterminer si le niveau de risque est acceptable pour l’une ou l’autre des parties ou pour les deux.

Note : L’outil téléchargeable est un tableur Excel. Il est décomposé ici pour en faciliter la compréhension.

Réf.	Menace	Acteur	Vulnérabilité	Impact des menaces sur les partenaires	Risque inhérent			Risque acceptable ? Oui/Non
					Probabilité (L) (1-5)	Impact (1-5)	Degré de risque (L x I)	
ex : 1a	Par exemple : Un accident de la route sur le site du programme.	Partenariat	La vulnérabilité/l’exposition à cette menace se trouve-t-elle modifiée du fait du partenariat ? Exposition de l’ONG L/N. Exposition de l’ONGI.	Dans quelle mesure la menace a-t-elle un impact sur le partenariat ? Dans quelle mesure la menace a-t-elle un impact sur l’ONG L/N ? Dans quelle mesure la menace a-t-elle un impact sur l’ONGI ?	Modérément probable : 3	Faible : 1	3	Oui
1b		ONG L/N	L’exposition des collaborateurs de l’ONG L/N est élevée car ce sont eux qui exécutent le programme et qui sont le plus susceptibles de se déplacer avec des conducteurs non formés ou en transports en commun.	L’impact sur l’ONG L/N serait plus élevé car un accident de la route affecterait le personnel d’exécution, les véhicules de l’ONG L/N et les personnes les plus étroitement associées à l’ONG L/N sur les plans juridique et réputationnel.	Modérément probable : 3	Modéré : 3	9	Oui
1c		ONGI	L’exposition du personnel de l’ONGI est faible car il n’a pas à se rendre sur le site du programme, sauf visite programmée.	L’ONGI peut être impactée indirectement par l’accident si celui-ci affecte l’exécution du programme, la réputation du partenariat/des partenaires et s’il a des implications budgétaires dont l’ONGI est responsable.	Très improbable : 1	Modéré : 3	3	Oui

Étape 2 : Identifier les mesures d'atténuation

2.1. Identifier les risques jugés particulièrement préoccupants pour le partenariat et/ou chaque partenaire.

2.2. Identifier des mesures d'atténuation pour chaque risque, y compris le rôle que doit jouer chaque partenaire.

2.3. Identifier les ressources/contributions supplémentaires qui pourraient être requises afin d'atténuer les risques de manière durable/à long terme (p. ex. matériel de communication, formation).

2.4. Calculer le risque résiduel.

Réf.	Risque acceptable ? Oui/Non	Mesures d'atténuation Réfléchir au rôle de chaque acteur pour atténuer les risques (ONG L/N, ONGI ou collectivement à travers le partenariat).	Ressources requises Indiquer toute ressource requise, par exemple personnel, équipement, formation.	Risque résiduel			Risque acceptable ? Oui/Non	Plan de gestion permanent du risque sécurité • Résumer la marche à suivre pour appliquer les mesures d'atténuation et créer un plan de gestion du risque sécurité • Identifier les points de suivi réguliers • Identifier les indicateurs clés d'un changement au niveau des menaces
				Probabilité (L) (1-5)	Impact (1-5)	Degré de risque (L x I)		
1b	Non	ONG L/N : Limiter les déplacements en transports en commun dans la mesure du possible. Former les conducteurs appelés à acheminer le personnel. ONGI : Partager des ressources sur la conduite en sécurité avec l'ONG L/N.	Formation du personnel	Très improbable : 1	Modéré : 2	2	Oui	Cartographier le recours aux transports en commun. Communiquer les restrictions de déplacement au personnel. Dispenser une formation.
1c	Non	ONGI : Disposer de règles formelles à l'attention du personnel de l'ONGI qui limitent les déplacements en transports en commun. Former les conducteurs appelés à acheminer le personnel. ONG L/N : Partager avec l'ONGI l'information sur les routes à haut risque.	Formation du personnel	Très improbable : 1	Modéré : 2	2	Oui	

Étape 3 : Plan de gestion du risque sécurité

3.1. Résumer la marche à suivre pour appliquer les mesures d'atténuation et créer un plan de gestion du risque sécurité.

3.2. Identifier les points de suivi réguliers.

3.3. Identifier les indicateurs clés d'un changement au niveau des menaces.

Réf.	Plan de gestion permanent du risque sécurité	Indicateurs de changement	Suivi
1b	Cartographier le recours aux transports en commun. Communiquer les restrictions de déplacement au personnel. Identifier les individus pouvant dispenser une formation à la conduite en sécurité. Assurer la formation.	Hausse du nombre des accidents de la route.	Qui :
		Preuve de non-respect des règlements – p. ex. utilisation des transports en commun.	Quand :
			Comment :



Outil 6.

Modèle de budget dédié à la gestion du risque sécurité au sein du partenariat

Il s'agit là d'un modèle de portefeuille des dépenses en matière de gestion du risque sécurité. Il donne un exemple des coûts de GRS que chaque partenaire devrait envisager d'inclure dans le budget du partenariat. Si nécessaire, les deux dernières colonnes permettent aux partenaires de calculer le montant du financement spécifiquement dédié à la gestion du risque sécurité en indiquant les coûts pris en charge en partie par d'autres départements (p. ex. les salaires des responsables qui ont certaines responsabilités en matière de sécurité).

Cet outil a été adapté de l'outil Risk Management Expense Portfolio (RMEP) du document d'information d'EISF « The Cost of Security Risk Management for NGOs ». Pour de plus amples exemples de dépenses associées à la gestion du risque sécurité pour les ONG, veuillez consulter cet outil.

Réf.	Catégorie	Partenaire	Description de la dépense	Unités	Coût unitaire	Total	% de la ligne budgétaire affecté à la gestion du risque sécurité	Gestion du risque sécurité - Total
	Salaires	ONGI	Par exemple, point focal sécurité du partenariat.			= unités x coût unitaire		= x % total de la ligne budgétaire affecté à la gestion du risque sécurité
		ONG L/N	Par exemple, points focaux sécurité au siège et sur le terrain, responsables chargés de tâches liées à la gestion du risque sécurité.					
	Administration et logistique	ONGI	Dépenses pour soutenir la gestion du risque sécurité au sein du partenariat, p. ex. déplacements vers les sites de terrain d'un partenaire.					
		ONG L/N	Par exemple, transport et logement des points focaux sécurité.					
	Formation, apprentissage et développement	ONGI	Par exemple, soutien apporté pour renforcer les capacités du partenariat (traduction, etc.).					
		ONG L/N	Par exemple, journées de formation du personnel à la sécurité (y compris HEAT, formation des conducteurs, premiers secours) et frais de transport et de logement connexes.					

suite page suivante

Réf.	Catégorie	Partenaire	Description de la dépense	Unités	Coût unitaire	Total	% de la ligne budgétaire affecté à la gestion du risque sécurité	Gestion du risque sécurité - Total
	Gestion de l'information et des connaissances	ONGI	Par exemple, coûts liés à la réalisation de l'évaluation de la gestion du risque sécurité.			= unités x coût unitaire		= x % total de la ligne budgétaire affecté à la gestion du risque sécurité
		ONG L/N	Par exemple, frais liés à la réalisation des évaluations des risques, à l'élaboration des plans et procédures de sécurité et au suivi du respect des règles par le personnel.					
	Accès	ONGI	Par exemple, plaidoyer avec les principales parties prenantes afin d'améliorer la sécurité des partenaires.					
		ONG L/N	Par exemple, activités de rapprochement avec la communauté.					
	Gestion des installations	ONGI	Ne concerne généralement pas l'ONGI lorsque l'ONG L/N est le partenaire d'exécution.					
		ONG L/N	Par exemple, loyers, système d'alarme, construction d'une salle sécurisée et maintenance.					
	Communications	ONGI	Par exemple, services de traduction afin d'améliorer l'accessibilité des communications sur la sécurité.					
		ONG L/N	Par exemple, équipement de communication, Internet.					
	Médical	ONGI	Ne concerne généralement pas l'ONGI lorsque l'ONG L/N est le partenaire d'exécution.					
		ONG L/N	Par exemple, trousses de premier secours.					
	Transport	ONGI	Ne concerne généralement pas l'ONGI lorsque l'ONG L/N est le partenaire d'exécution.					
		ONG L/N	Par exemple, véhicules aux normes de sécurité adéquates, conducteurs.					
	Gestion de crise	ONGI	Par exemple, coût de gestion d'une crise, comme les frais de déplacement du personnel international, si les partenaires conviennent de ce que l'ONGI sera impliquée dans la gestion de crise.					
		ONG L/N	Par exemple, fournitures nécessaires à la relocalisation et à l'hibernation.					
	Assurance	ONGI	Par exemple, police d'assurance pour le personnel participant au partenariat.					
		ONG L/N	Par exemple, relocalisation pour raisons médicales, assurance accidents personnels.					
	Imprévus	ONGI	Ne concerne généralement pas l'ONGI lorsque l'ONG L/N est le partenaire d'exécution.					
		ONG L/N	Fonds non affectés pouvant être disponibles immédiatement en cas de crise ou d'incident imprévu.					



Glossaire

Acceptation du risque : démarche qui conduit à une décision délibérée, que l'organisation comprend et accepte, quant au degré de risque résiduel que celle-ci est prête à assumer.

Accoutumance au risque : processus généralement inconscient par lequel une entité s'habitue à la présence de risques du fait de son exposition permanente au danger, d'où une diminution du niveau de réaction consciente face à ces risques. L'accoutumance au risque est un véritable problème auquel le personnel d'ONGI et d'ONG L/N peut être confronté après des séjours prolongés sur un même site.

Arborescence sécurité : processus permettant de communiquer rapidement une nouvelle à travers l'organisation sans solliciter à l'excès une personne en particulier. Consiste à donner à chaque membre du personnel la charge d'appeler un petit nombre d'individus en cas d'urgence.

Attitude face au risque : stratégie d'une organisation pour évaluer et éventuellement poursuivre, contenir, accepter ou refuser les risques.

Cadre de gestion du risque de sécurité : un ensemble de politiques, protocoles, plans, mécanismes et responsabilités qui permet de réduire les risques de sécurité que rencontrent le personnel.

Culture de la sécurité : chaque organisation a sa propre culture à l'égard de la sécurité, de la sûreté et des risques en général.

Duty of care : obligation légale et morale d'une organisation de prendre toutes les mesures possibles et raisonnables afin de réduire le risque de préjudice causé à celles et à ceux qui travaillent pour elle ou en son nom.

Évaluation conjointe du risque sécurité : démarche par laquelle l'organisation identifie les différentes menaces sécuritaires pouvant affecter son personnel, ses actifs et ses programmes, et analyse les menaces en fonction de leur probabilité et de leur impact pour déterminer le degré de risque. L'évaluation conjointe du risque sécurité est réalisée par des partenaires et sert à analyser les menaces pouvant découler du partenariat.

Examen conjoint de la gestion du risque sécurité (« examen conjoint de la GRS ») : démarche ou processus par lequel les partenaires étudient ensemble les concepts et stratégies de sécurité et identifient

ce qu'ils doivent tous les deux faire. Cela implique veiller à mettre en place des mesures pour renforcer la gestion du risque sécurité au sein du partenariat. Cet exercice repose sur un questionnaire à remplir en convenant d'indicateurs clés et en évaluant leur présence ou absence chez chacun des partenaires.

Gestion du risque sécurité : démarche qui vise à maximiser l'accès aux communautés en améliorant la sécurité du personnel humanitaire, des programmes et organisations. La gestion du risque sécurité (GRS) cherche à atteindre un juste équilibre entre les risques encourus et les bénéfices apportés par ses opérations. La GRS permet aux organisations de continuer leur actions tout en mettant en place des mesures s'assurant que leur ressource la plus importante, c'est-à-dire leur personnel, n'est pas excessivement exposé à des risques.

Localisation : « *Processus de reconnaissance, de respect et de renforcement de l'indépendance du leadership et de la prise de décision par les acteurs [locaux et] nationaux de l'action humanitaire afin de mieux répondre aux besoins des populations affectées.* »⁴

Menace : toute forme de défi posé à l'organisation, son personnel, ses actifs, sa réputation ou ses programmes, visant la sûreté, la sécurité ou tout autre aspect, dans le contexte au sein duquel l'organisation opère.

Organisation non gouvernementale internationale (ONGI) : ONG dont les opérations s'étendent au-delà d'un seul pays ou d'une seule sous-région.

Organisation non gouvernementale locale (ONGL) : ONG qui opère principalement dans une zone géographique spécifique d'un pays. Son personnel se compose majoritairement de membres des communautés desservies par l'ONG. Les ONG locales sont généralement d'une taille plus importante que les organisations communautaires et les organisations de la société civile et elles sont dotées d'une structure plus formelle et plus élaborée.

Organisation non gouvernementale locale/nationale (ONG L/N) : ONG locale ou nationale dont les opérations se déroulent dans son pays d'origine.

Organisation non gouvernementale nationale (ONGN) : ONG qui opère dans plusieurs régions d'un même pays. Son personnel peut être amené à travailler dans une zone différente de sa région d'origine.

Partage du risque : les organisations partagent la responsabilité à l'égard du risque sécurité qui les affecte.

⁴ Définition du CICR extraite de <https://media.ifrc.org/ifrc/document/ifrc-policy-brief-localization/>

Partenaire : membre d'un partenariat formel (contractuel) conclu entre organisations humanitaires. Ce type de partenariat est souvent conclu entre une ONG internationale et une ONG locale/nationale.

Partenariat : relation formelle (contractuelle) conclue entre organisations humanitaires. Il s'agit généralement de partenariats conclus entre une ONG internationale et une ONG locale/nationale. Dans le secteur de l'aide, les partenariats peuvent revêtir différentes formes, aussi bien en termes de durée que d'envergure ou de degré de collaboration.

Plan (conjoint) de gestion du risque sécurité : parfois appelé "plan de sécurité". Il s'agit d'un document clé, généralement axé au niveau du pays, qui indique les mesures et procédures de sécurité en place, et les rôles et responsabilités de l'ensemble du personnel en matière de gestion des risques identifiés. Le plan conjoint de gestion du risque sécurité est un plan de sécurité élaboré et exécuté conjointement par les organisations partenaires.

Plan d'action en vue de l'examen conjoint de la gestion du risque sécurité (« plan d'action en vue de l'examen conjoint de la GRS ») : liste détaillée des tâches que les partenaires doivent exécuter afin de combler les lacunes identifiées lors de l'examen conjoint de la GRS.

Préjugés : tendance à avoir un avis injuste ou des inclinaisons à l'égard (ou à l'encontre) d'un groupe particulier sur la base de la race, de l'ethnicité et d'autres aspects identitaires, y compris la nationalité. Les préjugés comprennent quatre dimensions :

- 1. Structurelle :** le maintien de politiques et de pratiques biaisées par de multiples institutions. Que ce soit volontaire ou non, celles-ci résultent en des inégalités de pouvoir, d'opportunité, d'accès, de traitement, d'impact et de résultats des politiques.
- 2. Institutionnelle :** des politiques et pratiques qui renforcent les préjugés en raison d'une répartition inégale systématique des ressources, du pouvoir et des opportunités au sein d'une organisation.
- 3. Interpersonnelle :** l'ensemble des actions et micro-agressions entre individus sur la base de préjugés.
- 4. Internalisée :** messages subtils et directs de la part d'individus qui renforcent les croyances négatives, les stéréotypes et la haine de soi.

Propriété du risque : lorsqu'une personne ou une entité doit rendre compte de la gestion du risque et en a l'autorité.

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

Risque sécurité : risque physique ou psychologique découlant d'actes de guerre, de violence, de criminalité ou d'autres dangers.

Risque résiduel : risque qui subsiste une fois les mesures d'atténuation mises en place.

Sécurité : absence de risque ou de préjudice résultant d'actes, d'événements ou de dangers non voulus ou accidentels.

Seuil de risque : le seuil de risque acceptable est atteint lorsque, suite à la mise en œuvre de mesures d'atténuation, le niveau de risque résiduel/actuel n'est pas conforme à l'attitude face au risque déclarée de l'organisation.

Sûreté : absence de risque ou de préjudice résultant d'actes de violence, d'agression et/ou d'actes criminels à l'encontre du personnel, des actifs ou des biens d'une organisation.

Transfert du risque : apparition ou transformation d'un risque (qu'il diminue ou s'accroît) pour un acteur du fait de la présence ou des actions d'un autre acteur, que cela soit intentionnel ou non.

Vulnérabilité : exposition de l'organisation à une menace. Dépend de la nature de l'organisation, de son mode de fonctionnement, de ses programmes, des particularités de son personnel et de sa capacité à gérer les risques.



Références

(n.d.) *Stop Impunity: Call for Action for Safeguarding of Humanitarian Space and Ending Impunity for Attacks against Humanitarians*. Retrieved from: <https://www.stopimpunity.net/>

Aid Reimagined (n.d.): <https://medium.com/aidreimagined>

Alliance for Empowering Partnership (A4EP). (n.d.). 'Resource Centre'. Sur le site : <https://a4ep.net/?cat=17>

Behn, O. et Kingston, M. (2010). *Risk Thresholds in Humanitarian Assistance*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/risk-thresholds-in-humanitarianassistance/>

Bickley, S. (2017). *Gestion du Risque Sécurité : manuel de référence à l'attention des petites ONG*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>

Buth, P. (2010). *Crisis Management of Critical Incidents*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/crisis-management-of-critical-incidents/>

Charter4Change (n.d.). 'Resources'. Sur le site : <https://charter4change.org/resources/>

cinfo (n.d.). 'Duty of Care Maturity Model Tool', cinfo. Extrait de : <http://dutyofcare.cinfo.ch/>

Davis, J. et al. (2020). *Security to go: a risk management toolkit for humanitarian aid agencies, 4th edition*. Global Interagency Security Forum (GISF). Extrait de : <https://gisf.ngo/resource/security-to-go/>

DisasterReady (n.d.): https://get.disasterready.org/?gclid=Cj0KCQiAgomBBhDXARIsAFNyUqPRVm_69sS6omcjFq5CmlpTLNLdpl8ppnlibqLHMfMxaAYe994pikMaAkKaEALw_wcB

EISF (2019). *Gérer la violence sexuelle à l'encontre du personnel humanitaire : prévention, préparation, réponse et suivi post-incident*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>

EISF et cinfo (2018). *Duty of Care Maturity Model*. EISF et cinfo. Extrait de : https://www.cinfo.ch/sites/default/files/matrix_web_pdf.pdf

EISF (2018). *Gérer la sécurité du personnel humanitaire aux profils diversifiés*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/>

Fairbanks, A. (2018). *Duty of Care under Swiss law: How to improve your safety and security risk management processes*. EISF et cinfo. Extrait de : https://www.cinfo.ch/sites/default/files/duty_of_care_eisf.pdf

Fast, L. et Bennett, C. (2020). *From the ground up: it's about time for local humanitarian action*. Humanitarian Practice Group (HPG). Extrait de : <https://www.odi.org/publications/16991-ground-it-s-about-time-local-humanitarian-action>

Featherstone, A. (2019). *Localisation Performance Measurement Framework*. Network for Empowered Aid Response (NEAR). Extrait de : <https://ngocoordination.org/system/files/documents/resources/near-localisation-performance-measurement-framework.pdf>

Finucane, C. (2013). *Évaluations de la sécurité*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/security-audits/>

Finucane, C. (2013). *The Cost of Security Risk Management for NGOs*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/the-cost-of-srm-for-ngos/>

EISF (2017). *Abduction and Kidnap Risk Management*. European Interagency Security Forum (EISF).

EISF (2019). 'An open letter to non-governmental and donor organisations from the European Interagency Security Forum', *European Interagency Security Forum (EISF)*. Extrait de : <https://gisf.ngo/an-open-letter-to-non-governmental-and-donor-organisations-from-the-european-interagency-security-forum/>

FICR (n.d.). 'Learning Platform'. Sur le site : <https://www.ifrc.org/en/get-involved/learning-education-training/learning-platform1/>

FICR (2018). *IFRC Policy Brief: Localization – what it means and how to achieve it*. IFRC. Extrait de : <https://media.ifrc.org/ifrc/document/ifrc-policy-brief-localization/>

GISF (2020). *Partnerships and Security Risk Management: from the local partner's perspective*. Global Interagency Security Forum (GISF). Extrait de : <https://gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/>

Global Mentoring Initiative (2019). *Partnerships: Pre-conditions, Principles and Practices*. Global Mentoring Initiative. Extrait de : <https://static1.squarespace.com/static/58256bc615d5db852592fe40/t/5d93782768d49710fa7a8349/1569945640280/Partnership+conditions+principles+practices.pdf>

Global Mentoring Initiative (n.d.). Resources. Sur le site : <https://www.gmentor.org/competencies-development-centre>

Humanitarian Leadership Academic (n.d.). 'Kaya Connect'. Sur le site : <https://kayaconnect.org/>

Humanitarian Outcomes (n.d.). 'Aid Worker Security Database'. Sur le site : <https://aidworkersecurity.org/>

INSSA (n.d.): <https://inssa.org/>

Insecurity Insight (n.d.). 'Aid in Danger'. Sur le site : <http://www.insecurityinsight.org/aidindanger/>

International NGO Safety Organisation (INSO) (n.d.). 'INSO Key Data Dashboard'. Sur le site : <https://ngosafety.org/keydata-dashboard/>

Kemp, E. et Merkelbach, M. (2016). *Duty of Care: a review of the Dennis v. Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/>

McManus, S. et Tennyson, R. (2008). *Talking the Walk: A Communication Manual for Partnership Practitioners*. International Business Leaders Forum on behalf of The Partnering Initiative. Extrait de : <https://thepartneringinitiative.org/wp-content/uploads/2014/08/TalkingTheWalk.pdf>

Moutard, L. (2021). 'How to effectively advocate for aid workers' protection?', Global Interagency Security Forum (GISF). Extrait de : <https://gisf.ngo/blogs/how-to-effectively-advocate-for-aid-workers-protection/>

NEAR (n.d.): <https://www.near.ngo/>

Newton, M. (2020). 'Developing a 'COVID-19 Secure' HEAT course', Global Interagency Security Forum (GISF). Extrait de : <https://gisf.ngo/blogs/developing-a-covid-19-secure-heat-course/>

Persaud, C. (2012). *Genre et sécurité : Orientations pour l'intégration du genre à la gestion du risque sécurité*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/gender-and-security/>

Race Forward (2015). *Race Reporting Guide*. Race Forward. Extrait de : https://www.raceforward.org/sites/default/files/Race%20Reporting%20Guide%20by%20Race%20Forward_V1.1.pdf

RedR UK, Insecurity Insight et EISF (2017). *Manuel de gestion de l'information issue des incidents de sécurité*. Extrait de : <https://www.eisf.eu/library/security-incident-information-management-handbook/>

Safeguarding Health in Conflict Coalition (n.d.): <https://www.safeguardinghealth.org/>

Singh, I. (2012). *Security Management and Capacity Development: International agencies working with local partners*. European Interagency Security Forum (EISF). Extrait de : <https://gisf.ngo/resource/international-agencies-working-with-local-partners/>

Stoddard, A., Czwarno, M. et Hamsik, L. (2019). *NGOs and Risk: Managing Uncertainty in Local-International Partnerships*. Global Report. Humanitarian Outcomes/Interaction. Extrait de : <https://www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships>

Sweeney, A. (2019). 'Reflections on GISF's 'At What Cost?' Campaign', *European Interagency Security Forum (EISF)*. Extrait de : <https://gisf.ngo/blogs/reflections-on-eisfs-at-what-cost-campaign/>

Syrian Network for Human Rights (n.d.): <https://sn4hr.org/>

The Global Humanitarian Platform (2007). *Partnership Principles: A Statement of Commitment*. Extrait de : <https://www.icvanetwork.org/system/files/versions/Principles%20of%20Partnership%20English.pdf>

The Partnering Initiative (n.d.). 'The Partnering Cycle and Partnering Principles', The Partnering Initiative. Extrait de : <https://thepartneringinitiative.org/the-partnering-cycle-and-partnering-principles/>

UNDSS (n.d.). 'Training'. Sur le site : <https://training.dss.un.org/>

van Brabant, K. (2010). *GPR8 – Operational Security Management in Violent Environments, Revised Edition*. Overseas Development Institute (ODI). Extrait de : <https://odihpn.org/resources/operational-security-management-in-violent-environments-revised-edition/>

Whiting, C. (2016). *NGO Fora Advocacy Guide: Delivering Joint Advocacy*. ICVA. Extrait de : https://www.icvanetwork.org/system/files/versions/NGO_Fora_Advocacy_Guide_English_July2017.pdf

Working Group on Protection of Humanitarian Action. (2018). *Toolkit: Responding to Violence against Humanitarian Action on the Policy Level*. Extrait de : <https://reliefweb.int/report/world/toolkit-responding-violence-against-humanitarian-action-policy-level>



Autres publications de GISF

Disponibles sur www.gisf.ngo

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

Octobre 2020
Moutard, L. – GISF

Duty of Care under Swiss law: how to improve your safety and security risk management processes

Octobre 2018
Fairbanks, A. info et EISF

Managing the Security of Aid Workers with Diverse Profiles

Septembre 2018 – Versions française et espagnole disponibles
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

Mars 2014
Armstrong, J. Avec le soutien du Secrétariat de l'EISF

The Cost of Security Risk Management for NGOs

Février 2013
Finucane, C. Édité par Zumkehr, H. J. – Secrétariat de l'EISF

Security Management and Capacity Development: International Agencies Working with Local Partners

Décembre 2012
Singh, I. et Secrétariat de l'EISF

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management

Septembre 2012 – Versions française et espagnole 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. Édité par Fairbanks, A.

Organisational Risk Management in High-risk Programmes: The Non-medical Response to the Ebola Outbreak

Juillet 2015 (dans *Humanitarian Exchange*, numéro 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.

Manuels

Security to go: a risk management toolkit for humanitarian aid agencies – 4th edition

Octobre 2020 – 2ème version disponible en français et espagnol

Davis, J. et al.

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

Mars 2019 – Versions française et espagnole disponibles

EISF

Abduction and Kidnap Risk Management

Novembre 2017

EISF

Security Incident Information Management Handbook

Septembre 2017

Insecurity Insight, RedR UK, EISF

Security Risk Management: a basic guide for smaller NGOs

Juin 2017 – Versions française, espagnole et arabe disponibles

Bickley, S.

Office Opening

Mars 2015 – Version française disponible

Security Audits

Septembre 2013 – Versions française et espagnole disponibles

Finucane C. Édité par French, E. et

Vazquez Llorente, R. (esp. et fr.) –

Secrétariat de l'EISF

Managing the Message: Communication and Media Management in a Crisis

Septembre 2013 – Version 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

gisf



Global Interagency Security Forum

Directrice exécutive

M: +44 (0) 77 6099 2239

gisf-director@gisf.ngo

Conseillère en recherche

M: +44 (0) 77 6099 2240

gisf-research@gisf.ngo

www.gisf.ngo

Édition en anglais : Première publication en Avril 2021

Édition en français : Première publication en Décembre 2021