



# **Partnerships and Security Risk Management:**

a joint action guide for  
local and international  
aid organisations

## Global Interagency Security Forum (GISF)

In 2020, EISF (European Interagency Security Forum) became GISF (Global Interagency Security Forum), reflecting the extension of its network.

- GISF is a peer-to-peer network of security focal points who represent over 100 aid organisations operating internationally.
- GISF is committed to achieving sustainable access to populations in need and keeping aid workers safe.
- As a member-led NGO forum, GISF harnesses the collective knowledge of its members to drive positive change in the humanitarian security risk management (SRM) sector through original research, events and more.

*For GISF, **humanitarian** refers to not-for-profit activities that seek to improve lives and reduce suffering.*

GISF is a collaborative forum and believes that breaking down silos and pooling expertise from a variety of sectors is crucial for improving humanitarian SRM. As such, we facilitate exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector and a broad range of international NGOs.

GISF takes an inclusive approach to SRM and doesn't believe in 'one-size-fits-all' security. We recognise that different staff face different risks, based on the diversity of their profiles, their context and their role and organisation.

In a rapidly changing humanitarian landscape, GISF values the importance of continuous innovation and adaptation. We strive to improve practice by producing original research and practical guides that fill knowledge gaps across the sector. The forum also invests in capacity building by promoting learning through training and events, and an online resource hub.

GISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Federal Department of Foreign Affairs (FDFA), the UK Foreign, Commonwealth and Development Office (FCDO), and member contributions.

**[www.gisf.ngo](http://www.gisf.ngo)**

## Background

This GISF guide builds on previous research carried out by GISF, particularly the paper *Partnerships and Security Risk Management: from the local partner's perspective*. Its development was also supported by findings from interviews with experts as well as the results of a testing phase in which eight international and national/local non-governmental organisations trialled parts of the draft guide with their partner organisations.

The author and GISF would like to thank the individuals and organisations that took the time to share resources and insight, as well as test the draft guide. These contributions were fundamental to the development of this document. The contributors are listed in the acknowledgements below.

## Suggested citation

GISF. (2021) *Partnerships and Security Risk Management: a joint action guide for local and international aid organisations*. Global Interagency Security Forum (GISF).

## Disclaimer

GISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'GISF' in this disclaimer shall mean the member agencies, observers and secretariat of GISF.

The content of this document is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this document. While GISF endeavours to ensure that the information in this document is correct, GISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk.

Accordingly, to the maximum extent permitted by applicable law, GISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. GISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

© 2021 Global Interagency Security Forum

## Acknowledgements

**Project manager:** Léa Moutard

**Author:** Adelia Fairbanks

### Contributing experts:

CAFOD former partner in 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 Whelan

ICVA: 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

Partner Myanmar: Tuja

Plan International: Elodie Leroy-Lemoigne

RICE WN: Jackson Olema, Pax Sakari

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






SARD: Fares Alsaleh

Titi Foundation South Sudan: Gloria Modong Morris Soma

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

WACSOF: Komlan Messie

## Finding your way

-  key points and tips
-  expert accounts
-  cross-references
-  further resources
-  six tools included here (from page 81) and available in editable format from [www.gisf.ngo](http://www.gisf.ngo)

**Words in maroon** are in the Glossary (page 108)

## Key definitions

**Duty of care:** The legal and moral obligation of an organisation to take all possible and reasonable measures to reduce the risk of harm to those working for, or on behalf of, the organisation.

**Local/national non-governmental organisation (L/NNGO):** A local or national NGO whose operations take place in their home country.

**International non-governmental organisation (INGO):** An NGO with operational reach beyond one country or sub-region.

**Partnership:** Any formalised (contractual) relationship between aid organisations, usually international-local/national partnerships. Partnerships in the aid sector can vary in form, length, scope and degree of collaboration.

**Risk transfer:** The formation or transformation of risks (increasing or decreasing) for one actor caused by the presence or action of another, whether intentionally or unintentionally.

**Risk sharing:** Organisations share responsibility for security risks that affect them.

▶ See **Glossary** for more definitions



# Contents

|   |               |
|---|---------------|
| <b>Introduction</b>   | <b>10</b>     |
| Who is this guide for?  | 11            |
| How to use the guide and tools  | 11            |
| What is security risk management?   | 13            |
| <br><b>1. Establish the foundations of an equitable security risk management partnership</b>                | <br><b>15</b> |
| 1.1. Why an equitable and joint approach to security in partnerships is important                           | 15            |
| 1.2. Understanding and addressing security risk transfer between partners                                   | 17            |
| 1.3. Adopting partnership principles  | 21            |
| 1.4. Communicating and building trust in partnerships   | 22            |
| 1.5. Exploring security risk attitudes within the partnership   | 24            |
| <br><b>2. Part 2: Carry out a joint review of security risk management processes within the partnership</b> | <br><b>26</b> |
| 2.1. The joint SRM review   | 26            |
| 2.2. Plan the approach  | 27            |
| 2.3. Complete the questionnaire and assess the indicators   | 31            |
| 2.3.1. Duty of care   | 35            |
| 2.3.2. Governance and accountability  | 38            |

|            |   |           |
|------------|---|-----------|
| 2.3.3.     | Policy and principles   | 41        |
| 2.3.4.     | Operations and programmes   | 44        |
| 2.3.5.     | Travel management and support   | 48        |
| 2.3.6.     | Awareness and capacity strengthening  | 51        |
| 2.3.7.     | Incident monitoring   | 54        |
| 2.3.8.     | Crisis management   | 57        |
| 2.3.9.     | Security collaboration and networks   | 60        |
| 2.3.10.    | Compliance and effectiveness monitoring   | 63        |
| 2.3.11.    | Supporting resources  | 65        |
| <b>2.4</b> | <b>Develop and implement a joint SRM review action plan</b>                                       | <b>67</b> |
| <b>3.</b>  | <b>Part 3. Jointly identify and address SRM needs, gaps and challenges</b>                        | <b>68</b> |
| 3.1.       | Jointly identify and address security risks   | 68        |
| 3.2.       | Funding security risk management in partnerships  | 69        |
| 3.3.       | Strengthening security risk management capacity in partnerships                                   | 71        |
| <b>4.</b>  | <b>Part 4: Advocate for change: strengthening security in the aid sector through partnerships</b> | <b>76</b> |
| 4.1.       | Joint advocacy  | 76        |
| 4.2.       | Security risk management and advocacy efforts   | 79        |
| 4.2.1      | Protecting aid workers against targeted attacks   | 79        |
| 4.2.2.     | Security risk management advocacy and the localisation agenda                                     | 80        |
| 4.2.3.     | Security risk management advocacy and funding   | 80        |

|           |   |            |
|-----------|---|------------|
| <b>5.</b> | <b>Part 5: Tools</b>  | <b>83</b>  |
| Tool 1.   | Good communication in partnerships                          | 84         |
| Tool 2.   | Risk attitude in partnerships                               | 85         |
| Tool 3:   | Joint SRM review questionnaire and worksheet template       | 87         |
| Tool 4.   | Joint SRM review action plan template                       | 99         |
| Tool 5:   | Joint security risk assessment and management plan template | 101        |
| Tool 6.   | Security risk management in partnerships budget template    | 106        |
|           | <b>Glossary</b>   | <b>110</b> |
|           | <b>References</b>   | <b>114</b> |
|           | <b>Other GISF publications</b>                              | <b>118</b> |



# Introduction

This guide is the third element of a multi-phase GISF project which aims to improve **security risk management (SRM)** in partnership arrangements between international non-governmental organisations (INGOs) and local and national non-governmental organisations (L/NNGOs) in the aid sector.

## What is a partnership?

In this guide, a **partnership** refers to any formalised (contractual) relationship between an INGO and an L/NNGO. Partnerships in the aid sector can vary in form, length, scope and degree of collaboration. Partnerships can be, for example, strategic and long-term, or project-based and short-term.

- The first phase of this project involved an analysis of the relationship between international NGOs and their local partners. This analysis focused on INGO perspectives and capacity development.

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

- The second phase focused on the perspectives and experiences of staff working in L/NNGOs. The research found that the transfer of responsibility for delivering aid to local actors (as part of the **localisation** agenda) has not been accompanied by honest and open conversations around the transfer of **security risks**.

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

- This guide constitutes the third phase of the project and builds on the findings of previous research to address the challenges, highlight opportunities, and present guidance for more equitable, sustainable, transparent, trusting, and mutually beneficial partnerships from a security risk management perspective.

 **Please note that this is not a training guide.**

## Who is this guide for?

This guide is targeted at INGOs and L/NNGOs in the process of entering into a partnership or already working in partnership.

- For organisations that are considering – or are in the early stages of – a partnership arrangement, this guide can steer early conversations around security risk management.
- For organisations that are already in a partnership, this guide can support partners with reviewing existing security risk management arrangements.



**Where partnerships are already in place, organisations should use this guide and its tools to review and amend existing processes as appropriate, rather than starting anew.**

This guide is targeted at staff with responsibilities relating to operations, security or partnerships within INGOs and L/NNGOs. It is also relevant for non-security experts. Security risk management cannot operate effectively in a silo.



**Individuals are encouraged to consult and work with all relevant colleagues throughout their organisation to strengthen security risk management within the partnership.**

## How to use the guide and tools

This document serves as an action guide for aid organisations to adopt a more equitable approach to managing security risks within a partnership.

The guide is divided into five parts:

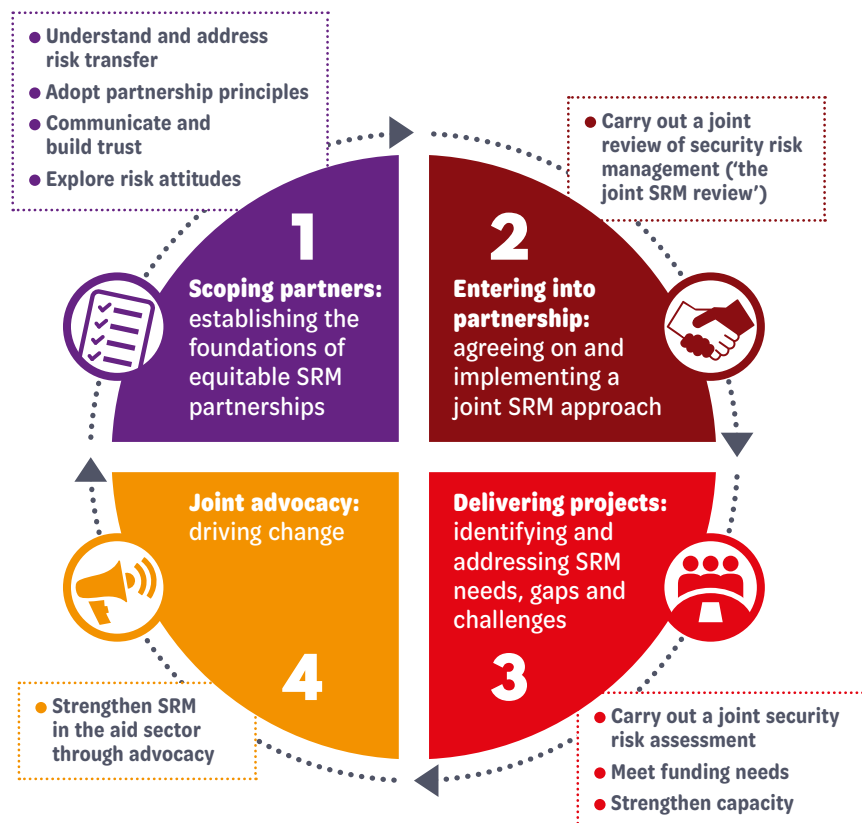
- **Part 1:** initial conversations to establish the foundations of an equitable partnership
- **Part 2:** the steps of a 'joint review of security risk management'
- **Part 3:** how to identify and address security risk management needs, gaps and challenges
- **Part 4:** how to engage in advocacy to improve security risk management within the aid sector
- **Part 5:** tools to support security risk management in partnerships.

Figure 1. visualises the structure of this guide.

At the start of a partnership it is essential that certain issues are discussed, and equitable ways of working are adopted. This includes the application of partnership principles, good communication, as well as honest conversations around risk transfer and risk attitudes within the partnership.

Building on these foundations, this guide introduces a **joint security risk management review** (or the 'joint SRM review') which walks partners through a series of questions and indicators to support a better mutual understanding of each partner's position in relation to security risk management. The review concludes with the development and implementation of a **joint security risk management review action plan** (or the 'joint SRM review action plan') to monitor efforts to strengthen security risk management within the partnership.

**Figure 1: Security risk management within partnerships**



**The joint review of security risk management should form part of any broader partnership risk assessment, and not be a separate or parallel process.**

This guide then shares guidance on how partners can identify and address security risk management needs, gaps and challenges, particularly how to carry out a joint security risk assessment and meet funding and capacity strengthening needs. Finally, the guide discusses opportunities for using advocacy to strengthen partners' security risk management.

Partnership arrangements can manifest themselves in many different ways, depending on the nature and length of the relationship, the types and sizes of the NGOs involved, as well as the context. The guidance presented here can be adapted by organisations to reflect their partnership structure and the operating context.

## What is security risk management?

Partners should have a shared understanding of 'security risk' and 'security risk management'.

Within this guide, a **risk** is how a **threat** could affect an organisation, its staff, assets, reputation or programmes. A threat is something that may result in harm or injury to staff, or loss or damage to the organisation.

**Vulnerability** refers to the extent to which the organisation, staff, assets or programmes are exposed to a threat.

Risks from unintentional events – such as road traffic collisions – are often described as '**safety** risks'.

Risks that arise from intentional actions – such as acts of violence or abductions – are usually described as '**security** risks'.

Please note that in this guide, we use 'security' as an umbrella term that includes safety, and the term 'staff' also refers to volunteers working for an organisation.

**Security risk management** uses a set of approaches and tools to help reduce the risks that may arise from intentional or unintentional acts. Security risk management is a means to an end and not an end itself; it is about putting in place practices that enable organisations to effectively reach those most in need while protecting staff.





## Find out more about security risk management

This guide is not an introductory guide to security risk management or an organisational security risk management audit process guide.

To learn more about security risk management as a whole, please see:

- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *GISF – Security to Go*
- *ODI-GPR8 – Operational Security Management in Violent Environments*

For guidance on how to conduct a general organisational security risk management audit, please consult:

- *EISF – Security Audits*
- *EISF – The Cost of Security Risk Management for NGOs*



# Establish the foundations of an equitable security risk management partnership

## 1.1. Why an equitable and joint approach to security in partnerships is important



*'Security risk management is an essential enabler of relief action and a condition for fair partnerships. As L/NGOs take responsibility for, and leadership in delivering humanitarian assistance in partnerships, they also take on security risks – even when risk transfer is not intended.'*

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

In partnerships, L/NGOs often bear the greatest burden of security risk, particularly in day-to-day operations in high-risk contexts. When it comes to managing security risks in partnership arrangements, NGOs often struggle with:

- A gap in discussions and analyses of **risk transfer** and **risk attitudes**.
- Difficulties in reaching a shared understanding of the context and associated risks.
- A lack of adequate funding for security risk management, particularly in L/NGO budgets, but also in INGO budgets.
- Inadequate and insufficient support and time to strengthen the security risk management capacity of both partners, even where gaps are jointly identified.
- Misunderstandings due to language barriers, limited physical engagement between partners, and a lack of a common vocabulary around security risks and security risk management.
- Barriers to open and honest communication, influenced by differences in communication cultures, power imbalances, pressures to be competitive, and fears of losing funding.
- Challenges in accessing and sharing relevant security-related information (a challenge often faced by both partners).



A key gap in INGO-L/NNGO partnerships is an equitable and joint discussion to explore the challenges listed above. When conversations take place, these often focus on the INGO ascertaining what the L/NNGO has in place and whether it is adequate by the INGO's standards.

While these conversations can be helpful, they place the L/NNGO under scrutiny and can relegate the local partner to the status of an entity that needs 'assessing'. This 'top-down assessment' assumes that the INGO's approach to security risk management is better than that of the L/NNGO – which may not be the case.

There is a need to shift security risk management conversations away from a predominantly top-down evaluation of L/NNGOs' security capacity to a joint conversation around risks, resources, needs, and opportunities for collaboration and capacity strengthening.



**An equitable SRM approach in partnerships shifts the conversation from the challenges of 'risk transfer' to discussions on how to 'share risk'.**

To share responsibility for security risks, organisations should adopt an approach that fosters a more equitable relationship between partners. This means:

- carrying out a joint review of what each partner has in place in terms of **security risk management**;
- identifying gaps and challenges and how partners can work together to address them;
- ensuring that the voices and experiences of staff in both partner organisations are equally heard and valued;
- exploring security risks and mitigation measures that build on the strengths of L/NNGO staff;
- acknowledging that the most effective approaches to security are adaptive and context-specific (which may mean that conventional security approaches by INGOs may not always be appropriate).

## What 'joint' action means in practice

### DO:

- Have open and honest conversations about what works and what does not
- Challenge each other to improve ways of working
- Brainstorm solutions together
- Share information and practices regularly
- Consult each other to inform new policies and practices
- Adapt existing resources to meet the realities and needs of both partners

### DON'T:

- Take decisions alone that could affect the partner organisation
- Ignore concerns or ideas
- Give up on the first try (engagement takes work)
- Avoid difficult conversations or challenging situations

To establish strong foundations for an equitable SRM partnership, organisations should openly discuss **risk transfer**, adopt partnership principles, engage in good communication, and jointly explore the **risk attitudes** of each partner. These foundational issues are discussed in more depth in the following sections.



## Further 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. Understanding and addressing security risk transfer between partners

When entering into partnership, organisations automatically transfer risk, both intentionally and unintentionally. It is important for partners to unpack what this risk transfer means for both organisations and jointly find ways to address any challenges that may be identified.

### Power imbalances in partnerships

A key challenge within partnerships is that often one partner has more power than the other. Sources of power include:

- **Access to or use of resources:** staff, money, equipment, communication tools.
- **Access to information:** including the ability to control that information and how it is communicated and shared.
- **Connections and networks:** relationships with other individuals, agencies or groups with power (for example, donors).
- **Authority and legitimacy:** a formal recognition, or one built on the organisation's reputation, which gives the organisation the ability to make decisions and take actions that are widely accepted.
- **Legal / registered status:** differences in legal or registered status, for example, nationality/type of passport, evacuation vs relocation opportunities, perceived or implied 'neutrality'.

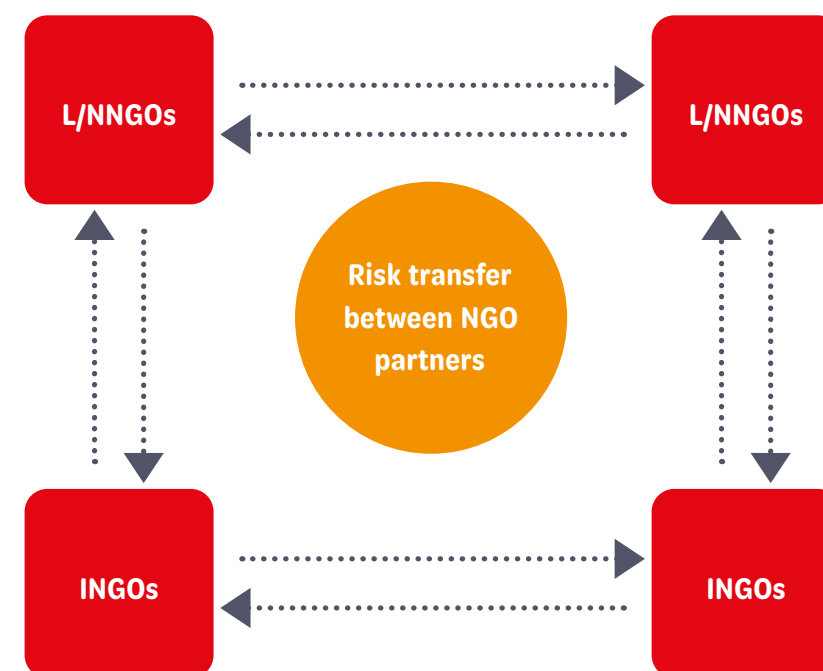
An organisation with less power may feel obliged to accept the decisions and expectations of a more powerful partner. For example, a local organisation that is dependent on the funding it receives through a partnership with an INGO may feel unable to raise concerns, for fear of losing funding or damaging the partnership. More powerful organisations have a responsibility to consider the contextual pressures weighing on their partners and should be proactive in ensuring that their partners feel able to voice their opinions and concerns without fearing repercussions.

### What is risk transfer?

**Risk transfer** is the formation or transformation of risks (increasing or decreasing) for one actor, caused by the presence or actions of another.

Security risks are not only transferred from the global to the local level. They can be transferred from L/NNGOs to INGOs, and between actors operating at the same level (see Figure 2). For example, being associated with an INGO can increase the risks an L/NNGO may face in its operations by affecting how local communities and authorities perceive and respond to the L/NNGO. Conversely, partnership arrangements with L/NNGOs can affect an INGO's security and acceptance in particular contexts due to existing perceptions of the L/NNGO. Risks can also be transferred within organisations, for example from staff in a capital city to staff in field offices.

**Figure 2:** The different directions of risk transfer



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

An organisation's identity – or perceived identity – can influence how their partners are perceived, which can impact risk transfer and generate security risks for both partners' staff. An organisation's identity relates to its mandate, mission and primary programming activities, for example, the faith-based nature of some organisations, or organisations with a particular programmatic focus, such as the provision of sexual and reproductive health services and rights. The personal profiles of staff may also affect the risks that partners are exposed to (*see box overleaf*).



**Remember to consider internal as well as external threats when assessing perceptions and identity-related risks and how they form or transform because of the partnership.**

Partners should understand and jointly address issues arising from the transfer of security risk within the partnership and can do this by asking each other key questions early on in the partnership and by incorporating risks that may arise from the partnership within a security risk assessment process and security management plan.



► See section 2.3.2. for key questions that explore the security risks that can emerge from partnerships

#### TOOL 5: Joint security risk assessment and management plan template

##### Personal profiles and related risks

Staff members have different risk profiles, which relate to their personal characteristics, both visible and hidden, such as their gender, nationality, ethnicity, etc. These characteristics interact with each other, with the context, as well as with the staff member's role and organisation, and the partner organisation.

As a result, risks can be different for each individual. Each staff member's profile plays a role in what threats they face and how **vulnerable** they are to those threats. It is important that throughout the partnership the diverse risks faced by staff are considered.

Partners should also not forget that sometimes threats can come from within the organisation or partnership itself. For example, L/NNGO staff belonging to certain ethnic groups may be particularly exposed to internal threats, which are not always visible to, or understood by, INGO staff.

**The personal profiles of staff in one organisation can be very different to another – as can their exposure to threats. Organisations should not rely on their partners' security risk assessments and mitigation measures but instead consider the particular risks their staff face due to their personal profiles.**

► See section 2.3.2. for key questions that explore the security risks that can emerge from partnerships



#### Further 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. Adopting partnership principles

Partners are encouraged to reflect on – and proactively take action to support – the following principles throughout the partnership.

| Equity  | Transparency and trust  | Mutual benefit  | Complementarity  | Result-oriented approach  | Responsibility   |
|---|---|---|--|---|--|
| Power imbalances between local and international organisations may exist, but the principle of equity ensures that despite these imbalances both partners have equal rights to be heard and their contributions are valued in the same way. This equity must be built upon 'respect' and 'fairness'.<br><br>With regards to security risk management, this means, for example, that the security concerns of both partners are equally heard, understood and addressed. | Honest and open interactions – that take place on an equal footing – between partners are the foundations of a trust-based relationship.<br><br>Partners must hold open and honest conversations about what the security needs are, and how to most realistically address these. This means listening to and trusting those most at risk, often L/NNGO staff. | The positive outcomes of the partnership should be more than simply meeting the partnership's objectives. To achieve this, partners need to ensure there is good communication and a clear understanding of each partner's broader interests, motivations, and goals.<br><br>By proactively strengthening the capacity of staff and addressing the long-term security needs of both partners, organisations are not only ensuring the security of the partnership's programmes, but also building sustainable security risk management approaches that can outlast the partnership. | Partners should recognise that diversity is an asset. Activities by both partners should build upon the knowledge and expertise that each brings to the partnership, avoiding duplication and proactively addressing barriers, such as language and culture.<br><br>Local capacity and knowledge are fundamental tools to effectively manage security risks. Any security risk management approach within a partnership must build on both partners' comparative advantages and complement each other's contributions. | Actions taken by partners should be focused on results and be realistic in scope.<br><br>In security risk management, this involves coordination between partners to develop and implement realistic security-related actions. Activities should directly support improved security and programme outcomes for both partners. | Partners have an ethical obligation to undertake their work responsibly, with integrity and in an appropriate way.<br><br>Partners should only commit to work that they have the competencies, skills, capacity and resources to undertake.<br><br>Where partners feel they cannot responsibly carry out their work due to security challenges, these should be openly discussed and addressed by both partners. |

Adapted from the Principles of Partnership endorsed by The Global Humanitarian Platform and the principles presented by The Partnering Initiative



#### Further 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. Communicating and building trust in partnerships

Communication is a primary challenge in building an equitable partnership. The complexity and sensitivity of security risks is not an excuse for vagueness or relying on assumptions.

Partners should be encouraged to ask each other questions and feel empowered to seek information to improve mutual understanding. To support this and build trust, staff who are tasked with liaising with partners should:

1. **Demonstrate genuine care:** question the possible prejudice and bias you may hold before entering the conversation.
2. **Listen to understand, not to respond.**
3. **Look for commonalities to build the relationship:** identify joint goals and interests and build upon these.
4. **Assume difference until you have proven commonality:** ensure that you do not make assumptions of common understanding. Always consider each partner's culture and traditions to reinforce messaging.
5. **Express empathy:** tell the truth with compassion and consider the circumstances of the partner that may affect their engagement with you (e.g., personal circumstances, background, needs).
6. **Be transparent and set the right expectations:** be honest about the constraints and limits you are working with and do not over-promise.
7. **Be positive and respectful:** focus on common objectives to create cohesion between you and your partner.
8. **Separate people from the problem:** approach issues together with your partner, rather than placing responsibility on them.
9. **Choose the right time, place and method to communicate:** consider the culture of the partner (e.g., oral versus written traditions), and make important communication easily accessible. Ensure that this communication mode is safe and that both partners feel comfortable using it.
10. **Say what you mean, mean what you say:** take responsibility for actions and words, including owning up to mistakes and misunderstandings.
11. **Ask for and receive feedback in an empowering manner:** in both anonymous and direct ways that give staff confidence to speak up.
12. **Be clear and specific in communication:** be clear on what is expected from the partner through the communication.
13. **Communicate regularly,** particularly during uncertain times.

Organisations should always ensure that the communication approach is appropriate for the context and individuals involved.



*'In some contexts we can't use the term security because it is associated with intelligence and may place the local partner at additional risk from state authorities.'*

L/NGO Staff Member



**Partners should have an interlocutor present in these conversations who is not only familiar with both partners' language, but also their culture and could serve as an interpreter.**

Make sure that the right people are a part of the conversation. Consider also at what level these conversations should take place – should staff from the organisation's headquarters and main country office only be present or also field office and/or frontline staff?



*'Sometimes at headquarters we put in place all of these measures to improve partnership arrangements, but these can fall apart at the field level when national staff members communicate poorly with local partners and perpetuate a top-down power structure.'*

INGO Staff Member



**Organisations should consider making good communication either a part of staff training or an aspect of a staff members' performance appraisal.**



### TOOL 1: Good communication in partnerships

Partnership arrangements and communication methods also need to be built with the understanding that bias remains pervasive between partners, and within the aid sector more broadly. **Bias**, in this context, is understood as the unfair inclination or prejudice for (or against) a particular group, on the basis of race, ethnicity, and other identity aspects, including nationality.

► See the Glossary for further information on different types of bias

Bias by either partner can severely impact partnership relationships and communication, especially where power imbalances and a lack of trust



may already be causing challenges. Both partners should consider what conscious and unconscious biases may be present.

#### Example of bias

In the aid sector, bias is often seen in the form of different security standards being applied to different groups of staff. In an example from GISF's previous research, L/NGO staff received less cash than their INGO colleagues to fund their trip, resulting in the L/NGO staff having to compromise on their overnight accommodation; something which their INGO partners did not have to do.

### Further 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. Exploring security risk attitudes within the partnership

Risk can be mitigated (reduced) in various ways. For example, the risk of road traffic incidents can be mitigated by vehicle maintenance and training drivers in appropriate driving and emergency procedures. However, even with mitigation in place, the risk of a road traffic incident taking place is still present, albeit reduced. This is the **residual risk**. An organisation's specific risk attitude will determine whether it accepts the residual risk (described as 'risk acceptance' or reaching an organisation's 'risk threshold').



**The decision to 'accept' security risks is not always made on equal terms between INGOs and L/NGOs.**

### Risk acceptance, risk attitude and risk threshold

**Risk acceptance**, **risk attitude** and **risk threshold** are all terms used to describe the amount of risk an organisation is willing (or compelled) to take on in order to meet its objectives.

It is imperative that partners understand, unpack and discuss the risk attitude of both organisations. This is key to an equitable partnership. Partners should respect each other's concerns and be aware of the possibility of **risk habituation** or of organisations feeling pressure to exceed their risk threshold in order to continue operating.

The following ethical principles can support organisations when assessing their own risk attitude in partnership arrangements:

1. **Criticality:** how critical is the programme?
2. **Do no harm:** what harm might ensue from a security incident?
3. **Autonomy:** have the staff of both partners – especially those at most risk – provided free and informed consent to take on the security risks, or has the partnership played a role in this decision?
4. **Custodial:** how accountable and responsible is the organisation's use of resources?
5. **Justice:** are the partners treating each other and others fairly?
6. **Fidelity:** are the partners being faithful to institutional and professional vision and roles?

Each partner's risk attitude should be an essential topic of discussion at the beginning of the partnership – and regularly revisited throughout the partnership lifecycle.



### TOOL 2: Risk attitude in partnerships

### Further 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 (particularly, 'Figure 3: Framework for ethical decision-making')*
- *EISF – Risk Thresholds in Humanitarian Assistance*

# Carry out a joint review of security risk management processes within the partnership

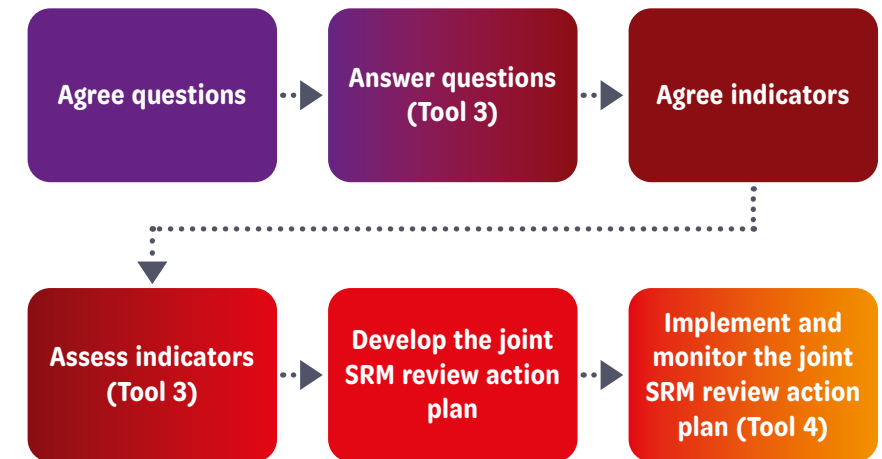
## 2.1. The joint SRM review

To equitably share responsibility for security, partners should support each other in managing security risks. A first step in doing this is holding open, honest and constructive conversations on how each partner understands and manages security risks, and how partners can collaborate to support each other's approach to security risk management. This guide presents a joint review of security risk management to support these conversations. The **'joint SRM review'** is a process with two overarching steps:

1. Reviewing each organisation's understanding and approach to security risk management and identifying gaps and challenges; and
2. Jointly addressing the gaps and challenges each partner faces in managing security by developing and implementing the **'joint SRM review action plan'**.

The joint SRM review starts with a questionnaire. The answers to the questions inform the development of key indicators. Partners then assess these indicators to identify what is already in place and what gaps remain. This assessment can be used to inform the development of an action plan with a checklist of tasks to improve both partners' coordination on security risk management. This 'joint SRM review action plan' is then regularly monitored by both partners. See Figure 3 for a visualisation of the different parts of the joint SRM review process. This guide includes tools to support the different steps of the process, also highlighted in Figure 3.

Figure 3: Steps of the joint SRM review



The following **security risk management framework** is used in this guide to frame the different parts of the joint SRM review (see Figure 4). Partners are strongly encouraged to use it as a reference map for their discussions.

### Managing actual security risks

The joint SRM review is about exploring approaches to security risk management within partnership arrangements. The review is, therefore, a 'partnership management tool', not a 'security risk management tool'.

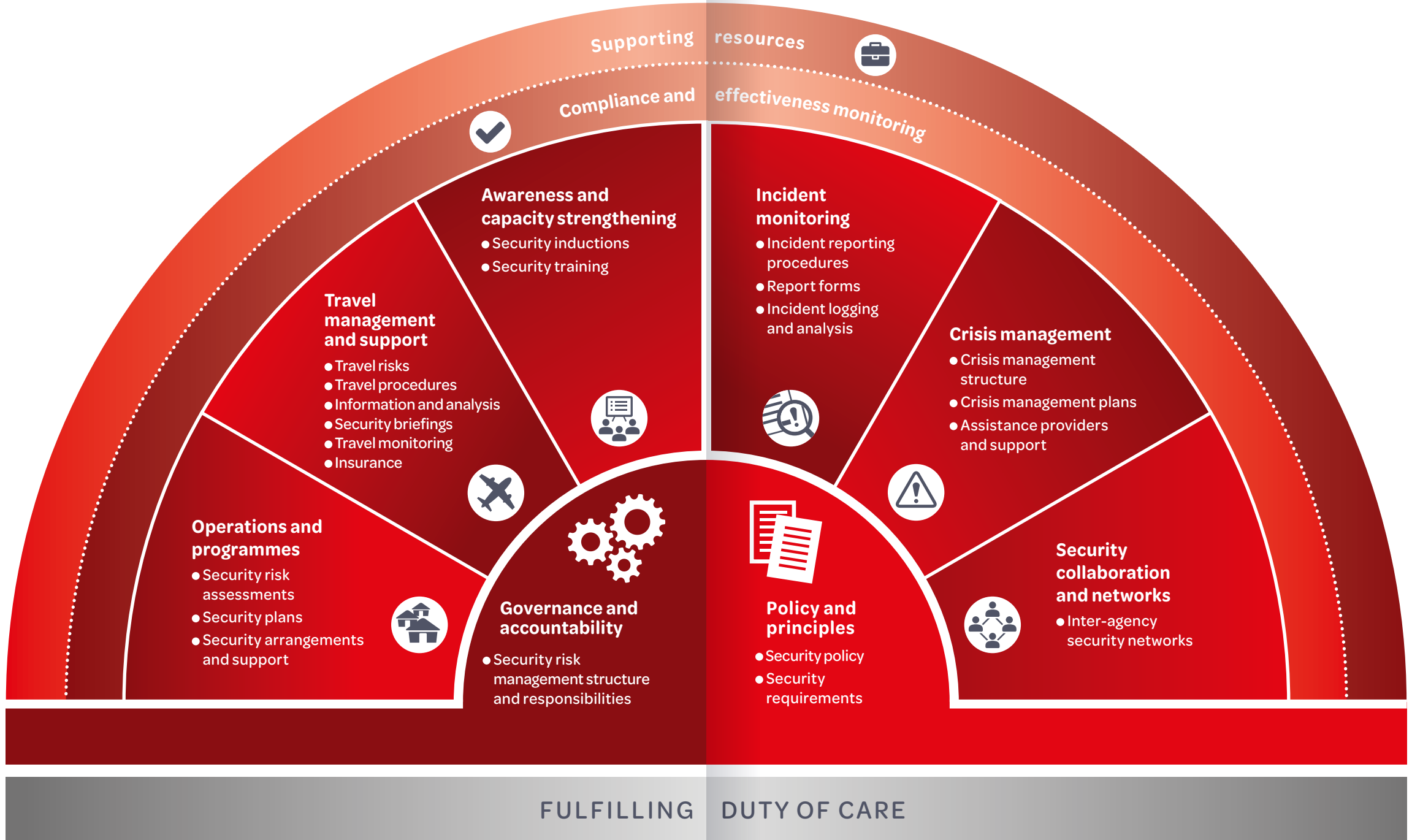
Following the joint SRM review, partners should look at the actual security risks that threaten their staff, organisations and the partnership, such as road traffic accidents or attacks against staff. This can be done by carrying out a **joint security risk assessment** and developing a **joint security risk management plan**. These 'security risk management tools' are discussed in more depth in Part 3 of this guide.

## 2.2. Plan the approach

As a first step, partners should plan the approach. This involves:

- Agreeing that improving security risk management is the objective of the review;
- Setting dates and times that are acceptable to both partners to hold the discussions;
- Agreeing on how the review will take place.

Figure 4: Security risk management framework



Source: EISF – Security Risk Management: a basic guide for smaller NGOs



The joint SRM review will need to be adapted to the circumstances of the partner organisations and consider relevant factors. For example, the relationship of each partner with the communities and other actors they work with, their risk attitudes and capacity to respond to security risk challenges, but also their locations, type of work, etc.

In long-term partnerships, joint reviews of security risk management in the partnership should ideally be carried out every two years, and possibly more frequently in fragile contexts. Partners may also find it helpful to carry out the review in case of significant changes in the operational context that affect the implementation of programmes in any way or changes in the relationship between the partners (e.g., scale up in operations). ‘Trigger points’ that start these conversations should be jointly identified and agreed by the partners.

Ideally, the majority of security risk management discussions should take place before entering into a partnership. When this is not possible, however, organisations should hold security-related conversations as soon as possible and regularly throughout the partnership.

It is important to also consider other assessments that may be taking place at the same time within the partnership. Local organisations are often juggling the expectations of multiple INGO partners as well as multiple departments from the same INGO, not only in the area of security, but broader risk management, particularly fiduciary risk.



**Due to the sensitivities surrounding security issues, staff from L/NGOs may feel more comfortable discussing their challenges and concerns in face-to-face meetings rather than through written communication.**

Partners should critically ask themselves which individuals should be involved. For example, these might be senior management, staff with security responsibilities, and partnership focal points. However other staff may bring useful insights, e.g., programme staff who are most at risk and staff with finance and/or advocacy responsibilities.

► See Part 4 to learn more about the role of advocacy

### Adapting the approach due to external factors

Partner organisations will need to adapt the approach presented in this guide to meet the opportunities and constraints presented by the nature of the partnership, the context, and other circumstances, such as environmental challenges (e.g., epidemics and insecurity). Adaptations may include:

- conducting workshops remotely by phone or online – ensuring that all necessary stakeholders have access to the communication channel or platform used;
- being flexible to quickly changing circumstances, relating to the environment, **safety** and **security**;
- ensuring all stakeholders are aware of the risks that may impact the way this approach is undertaken and are prepared to address these risks and/or adapt to accommodate the **vulnerability** of individuals involved in the process;
- ensuring regular and appropriate communication with all stakeholders, as well as keeping communication channels open to foster flexibility and adaptability.

As a proactive measure, organisations should consider the long-term needs of both partners and establish strong partnership structures and trusting relationships in order to build resilience against future shocks and crises.

### 2.3. Complete the questionnaire and assess the indicators

First, partners should agree on key questions for discussion to improve the understanding of what security risk management involves within each organisation and within the partnership as a whole.

The answers to the questions can be used to develop key indicators for the partnership as a whole or, where appropriate, for each partner organisation. Indicators can be judged as: present, partially present or not present. Partners should agree what each ‘assessment category’ means before evaluating indicators. For example, does ‘present’ mean that it is documented in some way, that the responsible manager confirms its presence, or that several staff members agree it is present?

The example questions and indicators presented in the following section are categorised by the different elements of the **security risk management framework** presented previously in section 2.1. The questions and

indicators are only indicative, however, and should be amended in line with the circumstances of each partnership.



**TOOL 3:** Joint SRM review questionnaire and worksheet template to answer questions and assess indicators. The tool can also be downloaded in editable format from [www.gisf.ngo](http://www.gisf.ngo)

The following chapter works through the joint SRM review questionnaire section by section, with explanations and some additional questions that organisations may choose to discuss.

### Preliminary security risk management questions for partners

Partners that may not be in a position to complete the full review, perhaps because they are still in the early stages of the partnership, may choose to initially explore the following preliminary questions.

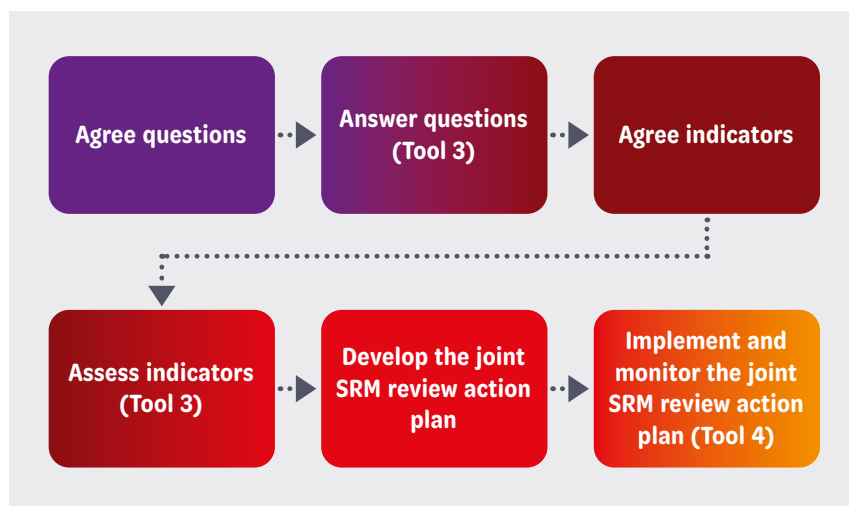
| Preliminary security risk management questions for partners |   |
|---|---|
| Duty of care  | <ul style="list-style-type: none"><li>• What are the legal and moral duty of care obligations of each partner to each other?</li></ul>  |
| Governance and accountability                               | <ul style="list-style-type: none"><li>• Have both partners inputted into key decision-making opportunities (e.g., meetings) regarding the programme, project, partnership and/or security?</li><li>• Do both partners have suitable security risk management structures (including roles and responsibilities) in place to enable the partnership objectives to be met?</li><li>• Does the partnership agreement include mention of security risks and their management?</li></ul>  |
| Risk transfer   | <ul style="list-style-type: none"><li>• How are the partners perceived by the stakeholders that each partner regularly engages with and relies on in order to operate?</li><li>• How does the vulnerability of each organisation and its staff to existing threats change as a result of the partnership? Does an organisation's perceived identity play a role?</li><li>• Are there any new threats that emerge as a result of the partnership?</li><li>• Does the partnership change the likelihood or impact of a particular threat? If yes, is this positive or negative?</li></ul> |
| Policies and principles                                     | <ul style="list-style-type: none"><li>• Are the mandate, mission, values and principles of each organisation understood by both partners, and are both organisations comfortable with each other's work and approach to operations and security (e.g., do both partners agree to each other's position regarding adherence to humanitarian principles)?</li></ul>   |

### Preliminary security risk management questions for partners *continued*

|   |  |
|---|--|
| Operations and programmes                     | <ul style="list-style-type: none"><li>• What are the security needs and expectations of each partner?</li><li>• Do the partners have an agreed system in place to identify and monitor security risks faced by staff?</li><li>• Do the partners agree on who is responsible for managing identified risks, and how these people should be managed and funded?</li><li>• Is there a system in place to make both partners aware of security risks and changes in the risk environment?</li><li>• Does each partner have enough resources (funding, time, and staff) to manage security risks?</li></ul> |
| Inclusive security risk management approaches | <ul style="list-style-type: none"><li>• Does the security risk management approach of both organisations consider how staff members' identity can affect their vulnerability to threats?</li><li>• How should sensitive identity topics, such as internal and external threats on the basis of sexual orientation or gender, be discussed by the partners? What are the comfort levels (accounting for cultural sensitivities)?</li><li>• How can partners support each other to step out of their comfort zones to ensure effective security risk management for all staff?</li></ul>                 |
| Internal threats and safeguarding             | <ul style="list-style-type: none"><li>• How will the partners manage security threats that may arise from within the partner organisations themselves (e.g., staff)?</li><li>• How are safeguarding concerns addressed within the partnership? Are there appropriate safeguarding reporting mechanisms in place for each partner's staff, programme beneficiaries and community members?</li></ul>   |
| Travel  | <ul style="list-style-type: none"><li>• How should security risks resulting from travel related to the partnership be managed?</li></ul>   |
| Awareness and capacity strengthening          | <ul style="list-style-type: none"><li>• How will partners identify security awareness and capacity strengthening needs and jointly meet these (both for personal safety and security risk management)?</li></ul>   |
| Incident monitoring                           | <ul style="list-style-type: none"><li>• How should the partners share incident information with each other, if at all?</li></ul>   |
| Crisis management                             | <ul style="list-style-type: none"><li>• How will the partners collaborate/coordinate in the event of a crisis or critical incident affecting either organisation in the location where the partnership is active?</li></ul>  |
| Security collaboration and networks           | <ul style="list-style-type: none"><li>• Are there platforms in the relevant context that discuss security issues?</li><li>• If yes, do both partners have access and an equal voice in these coordination platforms and networks in their operational areas, including security information sharing platforms?</li></ul>   |
| Compliance and effectiveness monitoring       | <ul style="list-style-type: none"><li>• How should both partners regularly review security risk management within the partnership?</li></ul>   |
| Resources                                     | <ul style="list-style-type: none"><li>• Have partners shared their respective resources on security risk management with each other?</li></ul>   |
| End of the partnership                        | <p>Will ending the partnership according to the contract (and financial timeline) have implications on the security of either partner? If yes, how should this be addressed?</p>   |



**Reminder:** When going through the review in the next sections, please follow the flowchart below.



### 2.3.1. Duty of care



**Duty of care** is a key element to address in partnerships in order to have a clear understanding of each partner's responsibilities and expectations with regard to staff care. It is also important to verify that both partners have a similar understanding of duty of care as not all partners may be familiar with the term.

#### An organisation's duty of care

Duty of care is the legal and moral obligation of an organisation to take all possible and reasonable measures to reduce the risk of harm to those working for, or on behalf of, the organisation. It applies in high risk contexts as well as low risk ones. While duty of care is usually strongly focused on legal obligations, partners should also explore their moral duty of care. This usually refers to every action (or omission) that goes beyond an organisation's legal obligations and aims to ensure the well-being of any individual affected by the organisation's activities.

Basic duty of care usually means:

- Knowing the risks faced by those the organisation is responsible for.
- Establishing mitigation measures to manage identified risks.

*continued*

### An organisation's duty of care *continued*

- Developing emergency plans.
- Ensuring staff understand the risks they face and the measures in place to manage them.
- Ensuring staff make informed decisions about the risks involved with their role.
- Providing appropriate support in the event of a security incident.

#### Example questions

**1.1.** What are the legal and moral duty of care obligations of each partner to each other, if any?

**1.2.** What are the legal and moral duty of care obligations of each partner to their respective staff, beneficiaries and affected communities?

**1.3.** Are the psycho-social needs of all staff considered and addressed, and what actions, if any, can either partner take to improve the care of implementing staff, e.g., insurance cover, psycho-social well-being?

**1.4.** Is duty of care – both legal and moral – understood by each partner, and is this understanding the same?

**1.5.** Will ending the partnership according to the contract (and financial timeline) have implications for the security of either partner? If yes, how should this be addressed?

#### Example indicators

**1.1.** Legal duty of care obligations are understood and being met by both partners.

**1.2.** Moral duty of care obligations have been discussed and agreed by both partners.



### Duty of care: Next steps and further information

To support this process, partners may also consider:

- Sharing their duty of care policies with each other and adding a paragraph to their duty of care policy on partnerships (if these policies exist).
- Jointly pulling together a list of service providers offering culturally and linguistically appropriate psycho-social support that is then shared with staff in both organisations.

#### Further information:

- *cinfo – Duty of Care Maturity Model Tool*
- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *EISF – Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*
- *EISF and 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. Governance and accountability



Good governance and accountable structures are essential for effective security risk management. Within partnership arrangements it is important to ensure both partners have security risk management structures in place, while being mindful of the diversity in practices and capacities between organisations.

Organisations benefit from determining early on in the partnership the **risk ownership** and responsibilities of each partner to ensure they have the right expectations of each other. Sharing responsibilities for security risk can be done in a strategic way and relies on assessing partners' risk profiles and ensuring complementarity.

**Security risk management arrangements will need to be adapted to match the type of partnership.**

#### Example questions

**2.1.** Do both partners have suitable security risk management structures in place to enable the partnership objectives to be met?

**2.2.** Do both partners have a clear understanding of roles and responsibilities relating to security risk management with regards to the partnership and implementation of programmes? For example, do both organisations have a security focal point who can be the main point of contact for partners on security issues?

**2.3.** How does each partner perceive **risk transfer** in the partnership (if at all)? What actions does each partner think they can take to move from risk transfer to **risk sharing**? (See box below for specific questions on risk transfer.)

**2.4.** Is there an agreed procedure to report concerns, and hold each partner accountable for failure to meet security risk management needs within the partnership?

**2.5.** What can both partners do to enhance their employees' **security culture**, particularly discussions and awareness of security within partnership arrangements?

**2.6.** Is there clarity on how security risks are linked to other risks, e.g., fiduciary risks, legal challenges, administrative barriers? Are colleagues working on these other types of risks aware of the security risk management approaches being implemented by partners?

**2.7.** Have both partners inputted into key decision-making opportunities (e.g., meetings) regarding the programme, project, partnership and/or security?

**2.8.** Does the partnership agreement include mention of security risks and their management?

#### Key questions to understand the security risks that can emerge from partnerships

To unpack the risks that may result from partnerships, organisations should ask themselves and each other:

- How are the partners perceived by the stakeholders that each partner regularly engages with and relies on in order to operate?
- Do organisational identity aspects impact the organisation and its staff's vulnerability to threats?
- Are there any new threats that emerge as a result of the partnership?
- Does the partnership change the likelihood or impact of a particular threat? If yes, is this positive or negative?
- When exploring mitigation measures and security strategies, can one organisation take particular actions to reduce the risk faced by their partner?

► See Part 4 to learn more about the role of advocacy



### Example indicators

**2.1.** A statement of accountability and governance pertaining to safety and security risk management within the partnership exists.

**2.2.** A reporting and accountability process (with defined content and frequency) exists for informing each partner of safety and security risk issues. This includes clarity on both partners' responsibilities with regards to security risk management within the partnership.

**2.3.** Both partners have a focal point explicitly assigned, with responsibility for governance of safety and security risks for the organisation and partnership.

### Governance and accountability: Next steps and further information

To support this process, partners may also consider:

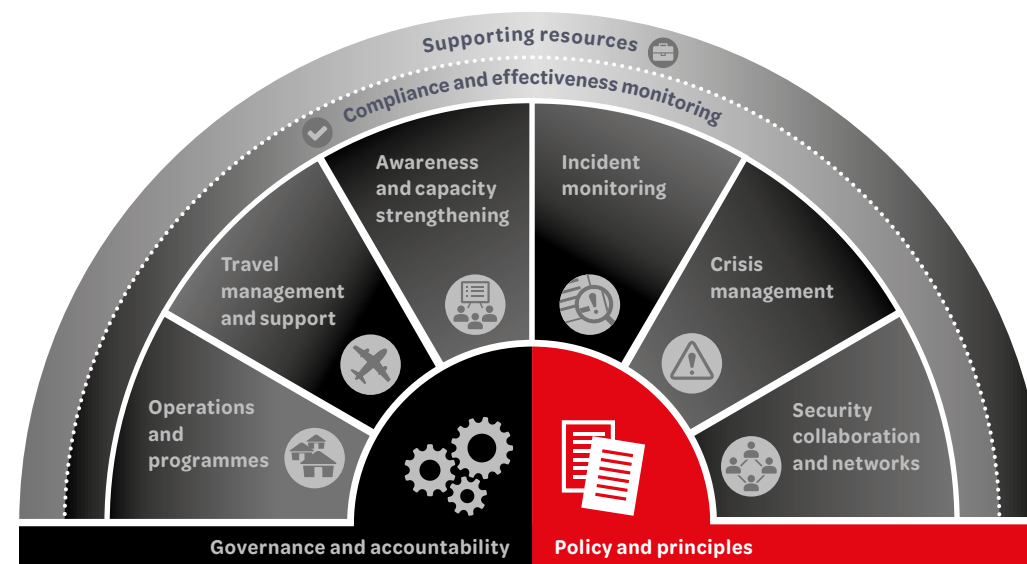
- Creating an organogram (with names / contacts / responsibilities) of staff with security responsibilities within the partnership.
- Taking actions to support a positive security culture among their staff (see, for example, '11 steps to a positive security culture' in EISF – Security Risk Management: a basic guide for smaller NGOs (p. 11)).
- Setting up a regular meeting with staff in both organisations working on different types of risks to regularly map the intersection and effects of the different types of risks facing both organisations.

### Further information:

- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *GISF – Security to Go*
- *Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships*



### 2.3.3. Policy and principles



Both partners should have an approach to security risk management that is based on an organisational security policy. The policy helps to inform staff of the principles and approaches the organisation takes to manage security risk and provides information on staff responsibilities for security risk management. Partners should compare each other's principles and approaches to managing security risk. Conversations around each partner's **risk attitude**, **risk habituation** and overall approach to security, including humanitarian principles, are particularly important.

► See section 1.5. Exploring security risk attitudes within the partnership



### TOOL 2: Risk attitude in partnerships

#### Example questions

**3.1.** Are the mandate, mission, values and principles of each organisation understood by both partners, and are both organisations comfortable with each other's work and approach to operations and security (e.g., do both partners agree to each other's position regarding adherence to humanitarian principles)?

**3.2.** Is there agreement by the partners on practical minimum security requirements that must be in place in each location or activity? (Note that

while these should apply to both partners, they must also be realistic and adapted to each organisation's capacity.)

**3.3.** How do the partners define and approach risk attitude, and is there agreement between the partners on what is an acceptable **risk threshold** for the partnership and programmes within it?

**3.4.** How do the partners perceive risk habituation and are there ways the partners can support each other in addressing it?

**3.5.** What are the links between risk attitude, programme criticality and security risk management capacity within the partnership?

**3.6.** Are the principles and objectives underlying the partnership agreed and understood between the partners?

#### Example indicators

**3.1.** Security risk management policies and their implementation (through plans, procedures, and/or guidelines) are appropriate to the local context and partnership circumstances, and accessible to all staff (i.e., available in relevant languages and formats).

**3.2.** The partnership agreement includes a statement relating to a joint understanding and agreement of the risk threshold for partnership activities.

**3.3.** The partnership agreement does not contradict – but where possible reinforces – both partners' security policies (e.g., provisions around the use of armed escorts).

#### Policy and principles: Next steps

To support this process, partners may also consider:

- Sharing each organisation's mandate, mission, values, principles and security policies and discussing how they compare between partners (e.g., is there alignment or are there serious tensions?).
- Creating a list of red flags in terms of security risks and mitigation measures that should be discussed before being implemented, especially if these relate to principles and policies (for example, the use of armed escorts).
- Discussing risk attitudes and determining ways to report concerns when one partner's threshold is reached.
- Organising awareness-raising activities to ensure all staff understand the concepts of risk habituation and risk acceptance and can voice concerns.



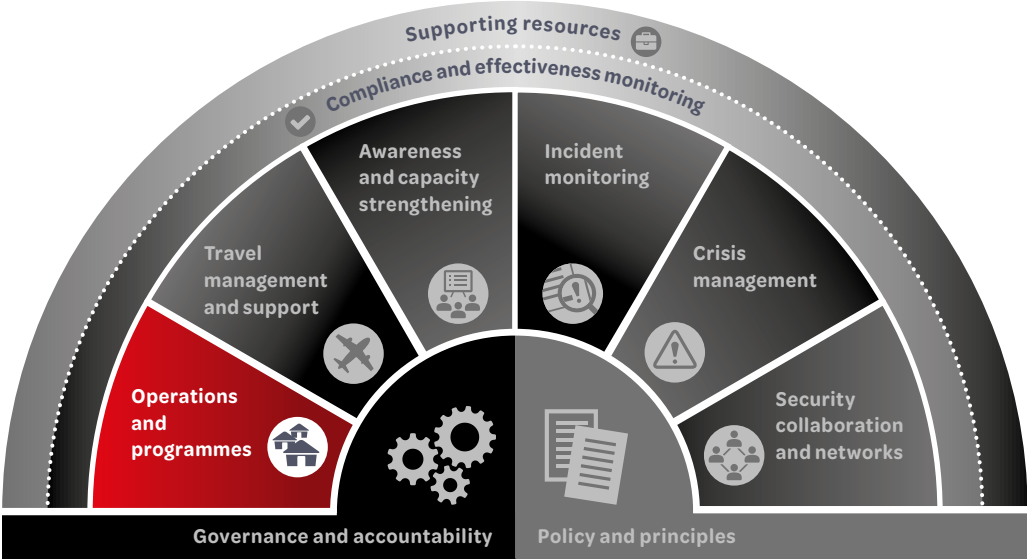
#### Policy and principles: Further information

##### Further information:

- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *EISF – Risk Thresholds in Humanitarian Assistance*



2.3.4. Operations and programmes



At the heart of many partnerships is the effective implementation of programmes. Partners should agree on the best way to manage security risks that arise from carrying out activities. Realistic plans, procedures and resources should be in place that support the analysis of the operating environment and the identification of security risks to staff and operations.

These will help with determining the most effective approaches and measures to manage security risks in the operating context.



Where possible, consider doing a **joint security risk assessment** for each operational context.

► See section 3.1. Jointly identify and address security risks



**TOOL 5:** Joint security risk assessment and management plan template

Effective security risk management involves collaboration with a diverse range of colleagues. Programme and finance staff should be involved, where appropriate, in conversations around identifying and mitigating risks, and to ensure that security risk management is included in partnership and project budgets.

► See section 3.2. Funding security risk management in partnerships



**TOOL 6:** Security risk management in partnerships budget template

Example questions

- 4.1. What are the security needs and expectations of each partner?
- 4.2. Do the partners have an agreed system in place to identify and monitor security risks faced by staff? (Is there alignment between both organisations' **security risk assessments** and security plans for the locations in which the implementing partner operates? What are the divergences, and why?)
- 4.3. Do the partners agree on who is responsible for managing identified risks, and how these should be managed and funded?
- 4.4. Is there a system in place to make both partners aware of changes in the risk environment?
- 4.5. Does each partner have enough resources (funding, time, and staff) to manage security risks?
- 4.6. Does the partnership/project budget include security-related budget lines and is this sufficient to meet the security needs of both partners? Is this funding flexible enough to cover overhead costs, allow adaptation in the event of changes in the context and security risks, or to use for capacity strengthening activities?
- 4.7. Who controls what is included in the partnership budget(s)? Can control be shifted so it is equally shared between partners?
- 4.8. How are safeguarding concerns addressed within the partnership? Are there appropriate safeguarding reporting mechanisms in place for each partner's staff, programme beneficiaries and community members?
- 4.9. How will the partners manage security **threats** that may arise from within the partner organisations themselves (e.g., staff)?

### Key questions for inclusive security risk management

To unpack the risks that may result from partnerships, organisations should ask themselves and each other:

- Does the security risk management approach of both organisations consider how staff members' identity can affect their vulnerability to threats?
- How should sensitive identity topics, such as internal and external threats on the basis of sexual orientation or gender, be discussed by the partners? What are the comfort levels (accounting for cultural sensitivities)?
- How can partners support each other to step out of their comfort levels to ensure effective security risk management for all staff?



### Example indicators

- 4.1. A joint security risk assessment** of operations, associated risks and impact on each partner has occurred, with a clear process in place for regularly updating the analysis. This assessment includes an analysis of internal risks and those that might be a result of the partnership itself.
- 4.2.** Explicit budget lines for meeting security requirements are present in the partnership budget, including capacity strengthening activities, and deemed sufficient to meet all resource requirements by both partners.
- 4.3.** Context-specific security strategies or approaches have been agreed between the partners and are articulated and communicated to all relevant parts of each organisation.
- 4.4.** Security risk management is actively promoted and supported by managers throughout the organisation, and is demonstrated by communications and reporting, workshop events, and/or other initiatives.
- 4.5.** The partners agree on how to prevent, prepare for and respond to incidents of sexual exploitation, abuse and harassment affecting their staff and beneficiaries within their organisations and the partnership.



### Operations and programmes: Next steps and further information

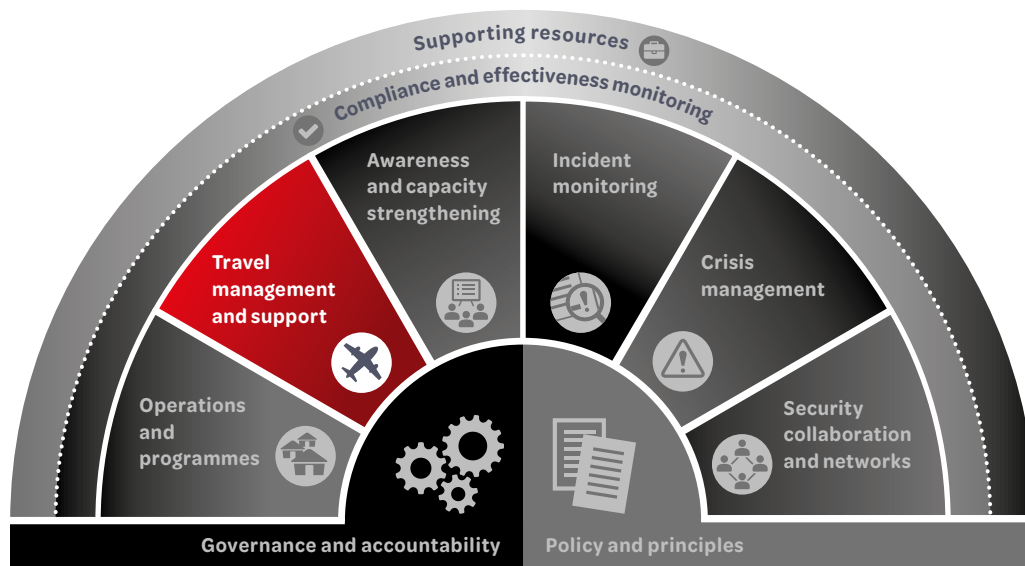
To support this process, partners may also consider:

- Mapping a standard day in the project locations together. This exercise can help identify questions around security issues.
- Jointly carrying out a security risk assessment.  
 See **TOOL 5**
- Jointly creating a list of security needs required for programme implementation, prioritising them and costing them.  
 See **TOOL 6**
- Review the programme/partnership budget and add security costs that may be missing.
- Share or, if appropriate, jointly create a security risk management plan.  
 See **TOOL 5**

### Further information:

- *GISF – Security to Go*
- *EISF – The Cost of Security Risk Management for NGOs*
- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *EISF – Managing the Security of Aid Workers with Diverse Profiles*
- *EISF – Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management*
- *ODI-GPR8 – Operational Security Management in Violent Environments*

### 2.3.5. Travel management and support



*'L/NGO staff often travel to riskier locations and have access to less secure vehicles or transportation means than INGO staff. This needs to be considered and addressed.'*

INGO Security Focal Point

In order to carry out programmes, staff may need to travel, for example, to visit project locations and attend meetings and events. In partnership arrangements, partner organisations may choose to visit each other's project location and/or offices. Therefore, both partners should agree on the best way to manage the risks that arise from travel, including movements in the project locations where these are relevant to the partnership, or travel that arises due to the partnership itself. Part of this means ensuring that communication and travel rules take into account local knowledge and language.



**The aid sector should move towards a culture of equal support for equal work. Distinction in support provided to international, national and local staff in either INGOs or L/NGOs needs to be appropriately justified (e.g., if there is a clear differentiation in risk profiles based on security risk assessments).**



### TOOL 5: Joint security risk assessment and management plan template

#### Example questions

- 5.1.** How should security risks resulting from travel related to the partnership be managed? What should be the minimum requirements for travel management and support arrangements (for field travel, overnight stay, travel communication procedures and other support)?
- 5.2.** Is equitable support on travel and stay provided to both organisations' staff in the project locations?
- 5.3.** Do the partners agree on the security policy and procedures that should be followed during partners' visits, and who holds **duty of care** for visiting staff?
- 5.4.** Does the partnership budget include insurance for travelling staff from both partner organisations?
- 5.5.** Are the diverse needs of travelling staff considered within travel procedures, e.g., heightened risk due to personal characteristics (gender, ethnicity, ability, etc.)?

#### Example indicators

- 5.1.** The partners agree on security arrangements and responsibilities for staff visits from both organisations to each other's offices and programme locations.
- 5.2.** Partners share with each other their security procedures for travelling staff for locations that are relevant to the partnership (e.g., these procedures can include information on roles and responsibilities, training and briefings, check-in procedures, travel monitoring, travel authorisations, and emergency procedures).
- 5.3.** The diverse security risks and needs of travelling staff are considered within travel procedures, e.g., heightened risk due to personal characteristics (gender, ethnicity, ability, etc.).

## Travel management and support: Next steps and further information

To support this process, partners may also consider:

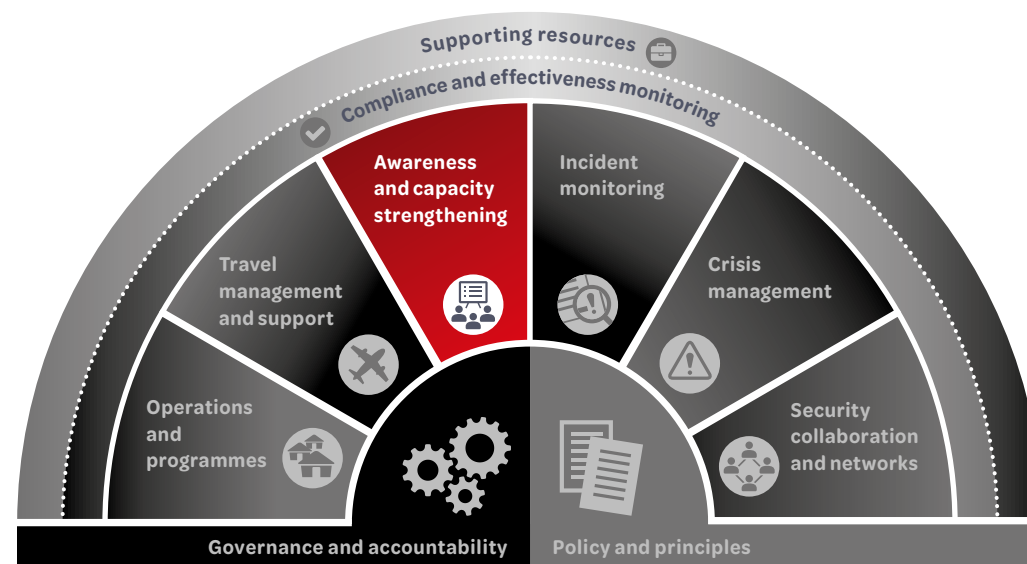
- Imagining a scenario in which staff from one organisation visit a partner organisation's offices or project location and assess which organisation has responsibility for planning the trip, ensuring security measures are in place during the trip, and responding in case an incident occurs.
- Discussing what travel will be necessary for both partners to carry out any relevant programmes and develop security procedures/requirements for each location (either jointly, or independently, as agreed by both partners).
- Consulting staff with diverse personal profiles on their experiences travelling and the risks both partners should consider to reduce the risks faced by staff due to their personal profiles (See 'Section 5.7. Travel' in EISF's research paper *Managing the Security of Aid Workers with Diverse Profiles*).
- Discussing minimum security measures for travel, such as security briefings, check-in procedures, vehicle maintenance, travel risk assessments, driver training, and confidential travel information management.



### Further information:

- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *EISF – Managing the Security of Aid Workers with Diverse Profiles (particularly, 'Section 5.7. Travel' and 'Chapter 2. Legal duty of care and anti-discrimination')*

## 2.3.6. Awareness and capacity strengthening



A core element that is often raised within partnership arrangements is capacity strengthening. Improving staff awareness of security risks and staff capacity to manage these risks is essential for both INGO and L/NGOs, as it ensures that staff in each partner organisation feel empowered to take ownership over security decisions and tools.



### Learning is a two-way process.

When entering into partnerships, organisations should consider each other's strengths and weaknesses and jointly explore ways to improve staff awareness of security risks and their capacity to manage them.



### Differences in approach should not be mistaken for lack of capacity.

Partners should agree on what is most needed in terms of capacity strengthening, and which format is the best to raise awareness (e.g., remote versus in-person training, staff communications, etc.). All capacity strengthening should be as sustainable as possible to support the long-term capacity of staff and organisations. Partners may also consider the

option to contract private training providers or external consultants to provide training to staff, where appropriate.

► See section 3.3. *Strengthening security risk management capacity in partnerships*

### Example questions

- 6.1.** How will partners identify security awareness and capacity strengthening needs and jointly meet these (both for personal safety and security risk management)?
- 6.2.** Is there agreement on what security risk management capacity gaps there are within both partners, and what each organisation can do to address them?
- 6.3.** Does the partnership budget include funding to support long-term capacity strengthening activities?
- 6.4.** Are partnership arrangements, particularly in relation to security risk management, shared with relevant new and existing staff in both partner organisations?
- 6.5.** Do implementing staff members have access to personal security training – particularly those working in the most high-risk locations?
- 6.6.** Is the security training provided to implementing staff in the right format to meet needs (e.g., remote versus face-to-face)?
- 6.7.** Does the training meet the long-term needs of staff by building on existing knowledge and skills and being as sustainable as possible?
- 6.8.** Is the approach to security risk management in the partnership designed to empower both partner organisations to address security needs independently?
- 6.9.** Are there opportunities for the long-term mentoring of security focal points within the partnership?

### Example indicators

- 6.1.** Security risk management capacity needs are agreed between the partners.
- 6.2.** There is a capacity strengthening learning and development strategy in place, with a clear implementation plan, and its aim is to improve the long-term capacity of partners.
- 6.3.** The organisation regularly shares resources and supports access to appropriate and context-specific opportunities for capacity strengthening.

learning and development opportunities in security risk management with partner organisations.

### Awareness and capacity strengthening: Next steps and further information

To support this process, partners may also consider:

- Identifying what training and capacity development opportunities each partner has access to, and how these could be shared between partners.
- Listing long-term training needs and ways each organisation can address them.
- Regularly sharing resources with each other (for example, helpful websites, tools, documents, lists of training providers, local contacts, etc.).

The following organisations and platforms provide training on personal security and security risk management:

- [INSSA website](#)
- [DisasterReady Platform](#)
- [UNDSS](#)
- [IFRC's Stay Safe training](#)
- [Kaya Connect](#)

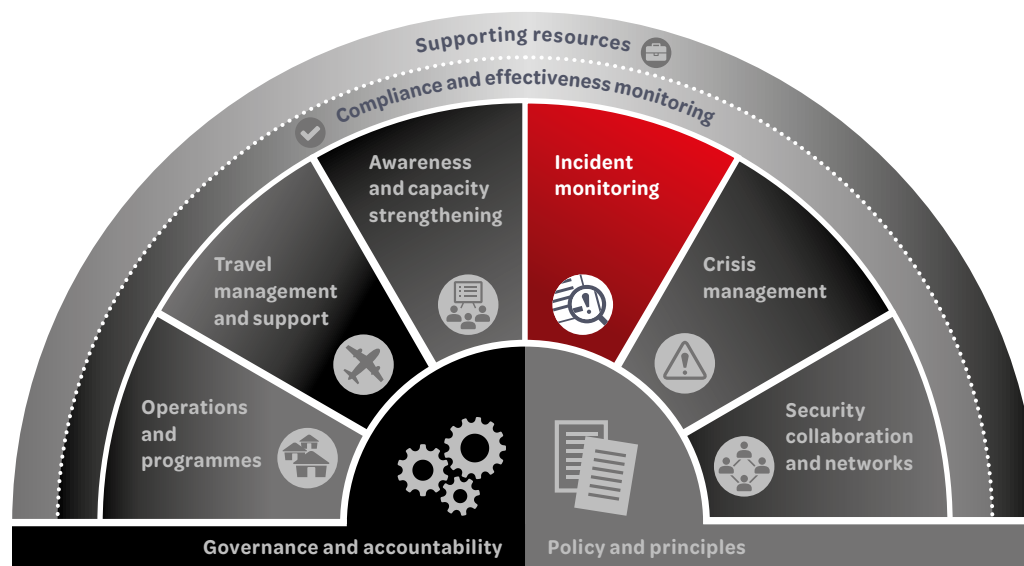
### Further information:

- [EISF – Security Management and Capacity Development: International agencies working with local partners](#)
- [EISF – Security Risk Management: a basic guide for smaller NGOs](#)





### 2.3.7. Incident monitoring



Incident reporting and monitoring is an essential part of security risk management as it allows for a greater understanding of the operating context and the security risks faced by organisations and their staff. This knowledge can be used to inform decision-making throughout an organisation, including operations, programmes, finance, advocacy and security risk management.

**All organisations experience security incidents. Partners that have strong reporting systems will have a greater understanding of the security risks their staff face and through this can reduce the likelihood of future incidents.**

Partnerships are strengthened when organisations share information on incidents which can affect each other and the partnership as a whole. A key challenge for incident reporting and sharing is a lack of trust, either within an organisation with staff afraid to report incidents, or between partner organisations who fear that sharing incident information might affect the partnership, their reputation and funding. To improve reporting within and between partners, strong and confidential reporting mechanisms must be established that address concerns around privacy and sanctions.



**Partners should be transparent with each other as well as with their staff about how information around reported incidents will be used and how its confidentiality will be maintained.**

► See section 1.4. Communicating and building trust in partnerships

#### Example questions

- 7.1.** How should the partners share incident information with each other?
- 7.2.** How can partners support each other's security incident information management? For example, incident reporting procedures, incident logging systems, and tools to analyse incident data and use it to inform decisions on security, programmes, operations, advocacy, finance, etc.
- 7.3.** What security incident data in the relevant location does each organisation have access to, either from its own operations or through its networks, that it can share with its partner on a regular basis?
- 7.4.** How can both partners address issues of under-reporting?
- 7.5.** Is there agreement on what types of incidents to report?
- 7.6.** How can partners support each other in strengthening the confidentiality of reporting mechanisms to protect staff and also to avoid information falling into the hands of hostile actors or authorities (e.g., technological solutions and good practice guidance)?

#### Example indicators

- 7.1.** A process for managing and sharing security information, including incident data, between partners for the operating context is in place and adhered to.
- 7.2.** There is agreement on how incident data is used to inform decision-making, including a clear policy on whether any punitive actions may result from the reporting and non-reporting of incidents.
- 7.3.** The organisation periodically reviews incidents affecting its staff to identify security incident trends and concerns and shares these with partner organisations.

## Incident monitoring: Next steps and further information

To support this process, partners may also consider:

- Sharing and jointly reviewing existing procedures and internal mechanisms to report incidents.
- Appointing a focal point for incident reporting.
- Establishing a way to share incident information with each other.
- Training staff on incident reporting, information management and confidentiality (see, for example, the DisasterReady mobile guides listed below).
- Discussing what kinds of incidents should be reported, and what effect certain types of incidents could have on the partnership.

The following platforms collect and openly share incident data from multiple organisations:

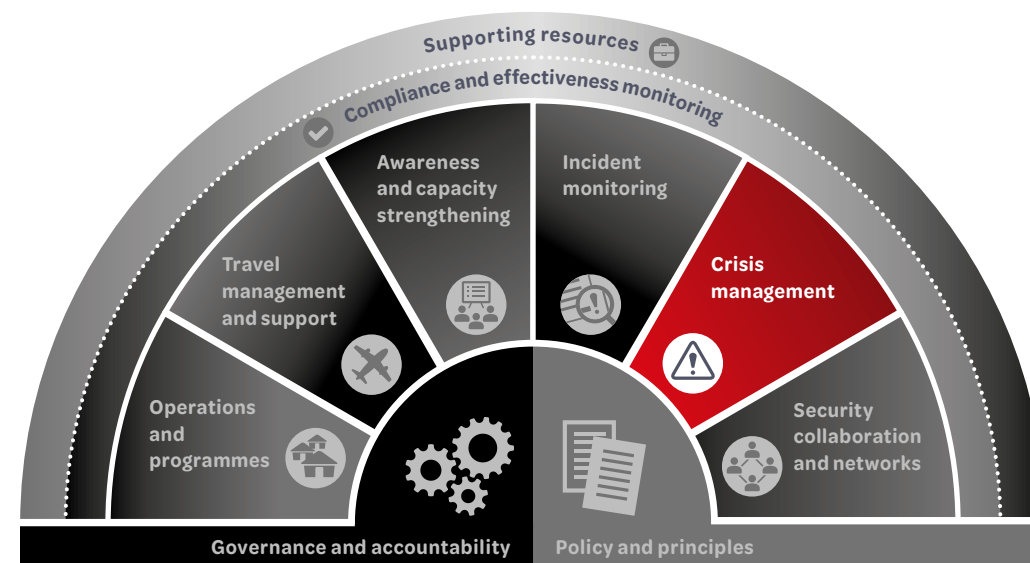
- [Aid Worker Security Database – Humanitarian Outcomes](#)
- [Aid in Danger project – Insecurity Insight](#)
- [INSO Key Data Dashboard](#)

### Further information and resources:

- [RedR UK, Insecurity Insight and EISF – Security Incident Information Management Handbook](#)
- [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. Crisis management



Organisations operating in high risk contexts are more likely to experience a severe incident that cannot be managed using normal organisational procedures. This type of incident (generally referred to as a 'crisis' or 'critical incident') could be, for example, a death, kidnapping, or the arrest of a staff member (as a result of external as well as internal **threats**). A crisis could also be an event that, due to its severity, has wider implications for the organisation. Organisations with mature security risk management systems will have a dedicated way to respond to a crisis (sometimes called a 'crisis management structure').

While crises are exceptional, partners should nonetheless be prepared for such an eventuality and agree in advance the best way to manage an incident of this severity. Partners should consider which organisation would be best placed to respond in the event of a crisis affecting the partnership, e.g., in terms of logistics, access and expertise.



**Crisis management is a complex issue that is only touched upon briefly in this guide. Partners are encouraged to consult additional resources on how to manage a crisis (see 'Further information' below).**



### Example questions

**8.1.** How will the partners collaborate/coordinate in the event of a crisis or critical incident affecting either organisation in the relevant location?

**8.2.** If a crisis or critical incident takes place and affects both partners, who should lead the crisis management response? What are the responsibilities and who has decision-making authority?

**8.3.** What support can each partner provide the other in the event either organisation experiences a critical incident in the partnership location?

**8.4.** Should partners include staff from each organisation in a rapid security information sharing system to ensure that staff in the affected location are well and accounted for in the event of a crisis or critical incident?

**8.5.** Are there post-incident assessment and de-briefing procedures in place within the partnership to understand and possibly mitigate further occurrences of incidents?

**8.6.** What access to insurance do both partners have in the event of a crisis or critical incident?

#### Rapid security information sharing system

In the event of a security incident or sudden change in the security context, organisations should have a process to quickly communicate news throughout an organisation – and in partnership arrangements between organisations – without overburdening any specific person. This is sometimes called a **security tree** process, which involves assigning each staff member a small number of other individuals they are responsible for calling in the event of an emergency. Alternatively, organisations may use mass messaging platforms, such as WhatsApp, to share security information to a large number of people quickly (any method of this kind must consider digital security concerns).

### Example indicators

**8.1.** Responsibilities and decision-making authority in the event of a crisis or critical incident affecting both partners are agreed, ideally in writing or visualised in some manner (e.g., a flowchart).

**8.2.** Partners have a crisis management structure and plan in place.

**8.3.** Partners have access to emergency support services (medical and non-medical) as part of each organisation's insurance cover.



### Crisis management: Next steps and further information

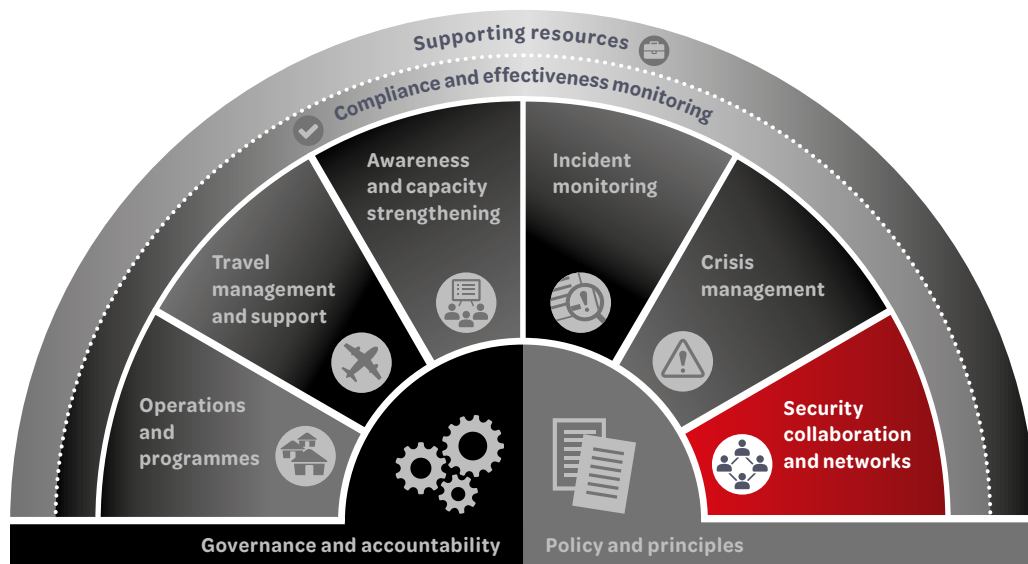
To support this process, partners may also consider:

- Agreeing on a communication system in the event of crisis.
- Creating a crisis management team including staff from both organisations, that can be activated in the event of a crisis.
- Running crisis simulation exercises.
- Discussing insurance options to prepare for a crisis or critical incident.
- Preparing for a crisis by consulting and sharing resources on how to effectively manage crises and critical incidents (see resource list below).

#### Further information:

- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *EISF – Crisis Management of Critical Incidents*
- *EISF – Managing Sexual Violence against Aid Workers*

### 2.3.9. Security collaboration and networks



Collaborating on security issues with other organisations operating in the same operational context not only strengthens an organisation's security risk management, but improves the collective security of all. Collaborations should extend beyond partner organisations and include active engagement with networks and information-sharing fora at different levels, including local or community-based, national, regional and international.



**Both partners should consider how they can support networks where security issues are discussed.**

#### Security collaboration example

The OCHA-led Humanitarian Access Working Group for northwest Syria includes various L/NNGOs, INGOs and international agencies and serves as a good example of successful collaboration on security risk management, with a positive impact on the security risk situation of organisations operating in the context. For example, the platform has enabled L/NNGOs to raise common issues of concern without having to expose their **vulnerabilities** as individual organisations to donors or partner organisations, fostering a more open and honest conversation while protecting L/NNGOs from any negative impact these conversations may have on their reputation and/or funding opportunities.

Partners should support each other in accessing the necessary security collaborations and networks that will help improve the security of their staff. Sometimes this requires advocacy with other organisations.

► See Part 4 to learn more about advocating on security risk management issues

#### Example questions

**9.1.** Are there platforms in the relevant context that discuss security issues? If yes, do both partners have access and an equal voice in these coordination platforms and networks in their operational areas, including security information sharing platforms?

**9.2.** What are the barriers and challenges that impede the active participation of both partners in inter-agency forums, meetings and discussions on security at the local, national, regional and international level?

**9.3.** What actions can either organisation take to facilitate the inclusion of their partner in these discussions?

**9.4.** What actions can either partner take individually and collectively to improve security collaboration with other organisations – both national and international – in the operational area?

#### Example indicators

**9.1.** Both partners actively participate in security risk management forums, platforms, meetings and consortia, and share safety and security information with others at the local, national, regional and/or international level.

**9.2.** Both organisations advocate for and facilitate the participation of their partners, where possible, in inter-agency forums, platforms, meetings and discussions in order to strengthen information-sharing and security collaboration. This includes sharing contact information with partners of relevant actors who can provide security risk management support.

#### Example coordination platforms that discuss security

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



## Security collaboration and networks: Next steps and further information

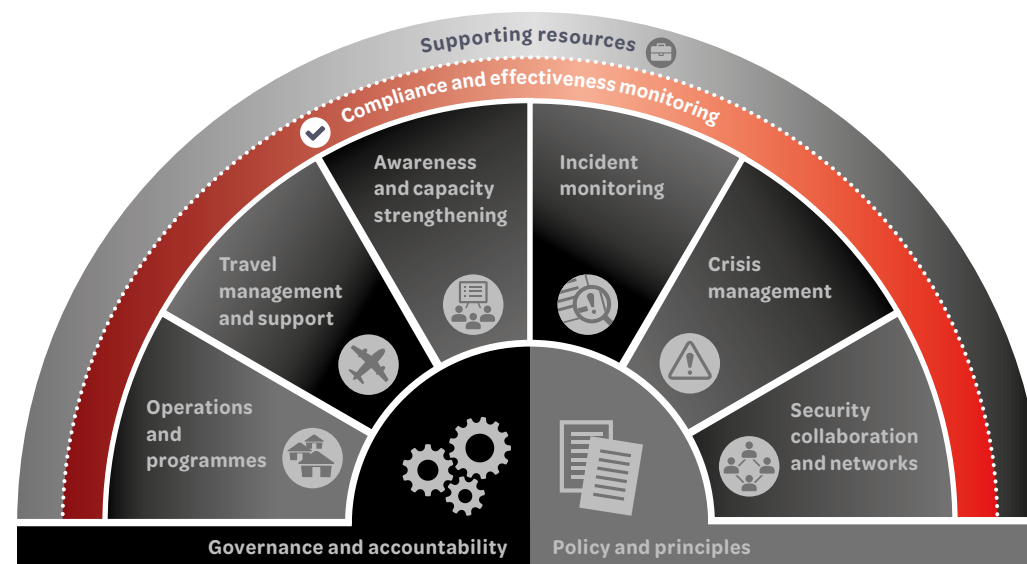
To support this process, partners may also consider:

- Introducing their partners to relevant security collaboration platforms.
- Discussing and addressing barriers to the active participation of both partners in existing platforms.
- Contacting security collaboration platforms and identifying a focal point within their organisation responsible for regularly engaging with these platforms.
- Creating security collaboration networks where these are absent and inviting a variety of different organisations to participate.

### Further information:

- *RedR UK, Insecurity Insight and EISF – Security Incident Information Management Handbook*
- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *GISF – Partnerships and Security Risk Management: from the local partner's perspective*

## 2.3.10. Compliance and effectiveness monitoring



*'Compliance is about maintaining the organisation's security approach (ensuring long-term viability and sustainability), as well as monitoring this approach.'*

INGO Security Focal Point

Organisations should regularly monitor and review their **security risk management framework** to ensure that staff are complying with procedures and that the organisation's approach to security remains fit for purpose. In partnership arrangements, this also involves ensuring that each partner is meeting its agreed responsibilities in relation to security risk management as part of the partnership.

### Example questions

**10.1.** How should both partners regularly review security risk management within the partnership?

**10.2.** What level of compliance and effectiveness monitoring in relation to security risk management within each organisation and/or the partnership is agreeable to both partners?

**10.3.** How much information relating to lessons learned, reviews, security audits, and post-incident analysis relating to the context, the partnership, or a particular project, are the partners willing to share with each other?

**10.4.** Does the compliance process overburden any of the partners unreasonably?

**10.5.** Are expectations around compliance and effectiveness monitoring in line with capacity? Does this monitoring complement monitoring related to the partnership carried out by other departments, such as finance?

**10.6.** Are there existing partnership management processes for monitoring and review that security risk management could be integrated into?

**10.7.** What actions can both partners take to establish and enforce a strong disciplinary culture within their organisations towards non-compliance with security policies and minimum requirements?

#### Example indicators

**10.1.** Outcomes of lessons learned, reviews, post-incident analysis, and security audits relating to the context, the partnership or the project/programme, are shared between and discussed by both partners.

**10.2.** Persons responsible for monitoring safety and security system implementation and compliance (both within each organisation and within the partnership) are properly trained, were involved in the **joint SRM review**, and have these responsibilities explicitly stated in their job descriptions.

**10.3.** Employee performance management systems make explicit reference to safety and security responsibilities, and compliance with the organisation's policies.

#### Compliance and effectiveness monitoring: Next steps and further information

To support this process, partners may also consider:

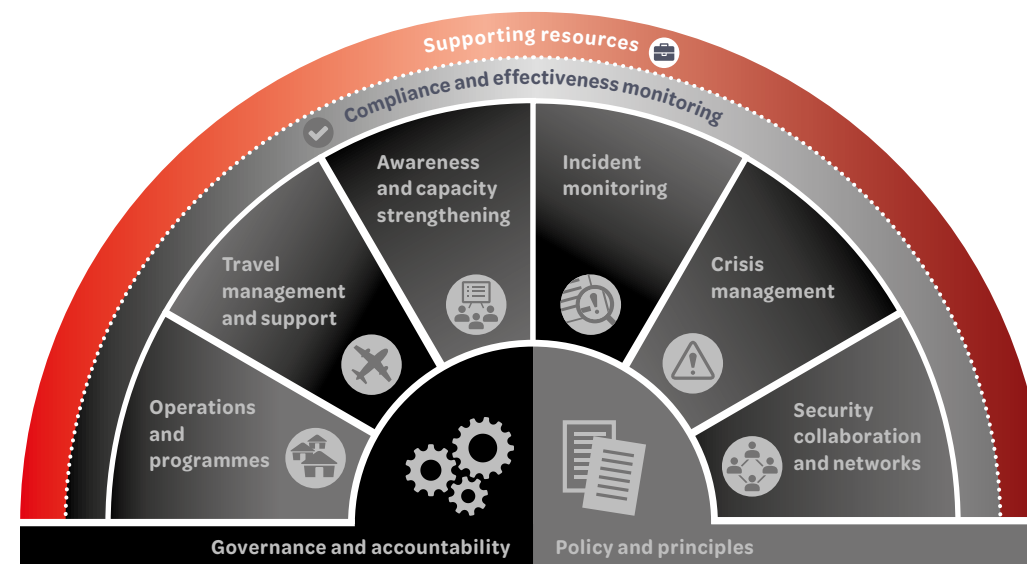
- Creating a compliance checklist (for example, 'Tool 3 – Document review checklist' in EISF's guide *Security Audits*).
- Using existing compliance mechanisms that partners may already be using for other partnerships to avoid duplication of efforts/reporting.

#### Further information:

- [EISF – Security Audits](#)
- [EISF – Security Risk Management: a basic guide for smaller NGOs](#)



## 2.3.11. Supporting resources



**'INGOs have a responsibility to support their L/NGO partners with security risk management.'**

L/NGO Security Focal Point

All staff should have access to guidance, tools and other resources to support them in their efforts to manage security risks as part of their work. Most resources on security risk management are available for free online and in multiple languages (*see the Further information box later in this section*).



**Both partners should proactively share security risk management resources within the partnership.**

Partners should increase all of their staff members' access to supporting resources by making resources available offline, in non-written formats, and translated into relevant languages.

#### Example questions

**11.1.** Are supporting resources on security risk management available and accessible to all staff, and if not, what actions can be taken to improve accessibility?

**11.2.** Have partners shared their respective resources on security risk management with each other?

**11.3.** What other resources would the partners benefit from to help them manage security risks?

#### Example indicators

**11.1.** Resources on security risk management that meet the needs of all relevant partner staff are regularly shared in a format that is accessible to them.

**11.2.** Partners make available a range of guidance, tools and templates as part of a security library to assist each other in managing security risks.

#### Supporting resources: Next steps and further information

To support this process, partners may also consider:

- Sharing security resources with each other and discussing them to ensure understanding.
- Adapting resources to make them more accessible (e.g., visualisation of decision-making processes, translations into relevant languages, etc.).

#### Further information:

- *EISF – Security Risk Management: a basic guide for smaller NGOs (available in Spanish and French. An Arabic translation will be available in 2021)*
- *GISF Library webpage*
- *GISF Training hub*
- *DisasterReady resources and training (available in multiple languages)*



## 2.4. Develop and implement a joint SRM review action plan

After completing the questionnaire and assessing indicators, the final step in the **joint SRM review** is to address partial or absent indicators, which can be done by developing and implementing a **joint SRM review action plan**. Both organisations should implement the joint action plan and agree on a timeframe for regular monitoring.

The aim of this action plan is to improve the coordination between partners around the security risk management system within the partnership (it is therefore a ‘partnership management tool’, not a ‘security risk management tool’).



**Indicators that were deemed present in the assessment exercise do not need to be included in the action plan.**

This guide presents a **joint SRM review action plan template** that can support partners in listing the status of each indicator, roles and responsibilities, key objectives, and the timeframe for implementation. Partners can adapt the template to help them discuss and monitor actions taken as part of the joint SRM review.



#### TOOL 4: Joint SRM review action plan template

#### The joint SRM review action plan vs a security risk management plan

The ‘joint SRM review action plan’ presented in this guide refers specifically to a checklist of tasks that both partners agree to implement as part of the joint SRM review process introduced in this guide.

Within each organisation there may be a separate ‘risk management plan’ (sometimes referred to as a ‘security risk management plan’, ‘security management plan’ or ‘security plan’), which refers specifically to actions to be taken by an organisation to manage identified security risks (for example, how to manage the risk of theft or detention).

► See section 3.1. Jointly identify and address security risks





## Jointly identify and address SRM needs, gaps and challenges

### 3.1. Jointly identify and address security risks

Sharing responsibility for security risks means that partners jointly explore the different types of security risks they are exposed to and the impact these can have on both organisations and their staff. It also means that they jointly identify and implement actions to manage security risks.



**Sharing responsibility for security risks is at the heart of having an equitable approach to security risk management within a partnership.**

To share risks, partners first need to have a common understanding of the risks affecting them and the partnership. This discussion should explore each partner's perceptions of the security risks they face and their attitude to it. The conversation should enable both organisations to explain what they understand by 'likelihood' and 'impact' in practice, to ensure they have a similar understanding of how to characterise the levels of risks they face. Once this is done, partners can then discuss what they perceive as an acceptable level of risk.



#### TOOL 2: Risk attitude in partnerships

Partners should also understand and jointly address issues arising from the transfer of security risk within the partnership. A security risk faced by one partner can easily affect the other partner and the partnership as a whole. By jointly identifying risks and agreeing on how to address them, partners combine their capacity and knowledge to reduce the likelihood of an incident happening and improve each other's ability to handle an incident should it take place.

For example, while implementing a project as part of the partnership, an implementing L/NNGO may face the risk of a road traffic accident. An

incident of this kind will not only affect the L/NNGO's staff directly, but also affect the partnership's budget, the ability of both partners to meet their programme objectives, and both partners' reputation. To mitigate the risk of a road traffic accident, the L/NNGO can, for example, help its INGO partner understand the likelihood of a road traffic incident happening and why the risk may be high (e.g., unsafe roads, unsafe vehicles). In turn, the INGO can, for example, support the L/NNGO's drivers in accessing safe driving training or provide additional funding for the L/NNGOs to buy more appropriate vehicles.

Carrying out a joint security risk assessment is essential for partners to understand each other's support needs and to implement adequate mitigation measures. The joint security risk assessment can be done at a global level to consider general risks resulting from the partnership, or at the country level to consider context-specific risks. This joint assessment can then be used to develop a joint security risk management plan to mitigate against identified risks. This guide presents a joint security risk assessment and management plan template to support partners in carrying out this exercise.



#### TOOL 5: Joint security risk assessment and management plan template

A joint security risk assessment and the broader 'joint SRM review' may, furthermore, highlight broader SRM needs, gaps and challenges, such as those related to funding and capacity. These challenges are discussed in more depth in the following sections.



#### Further information

- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *GISF – Security to Go*

### 3.2. Funding security risk management in partnerships

Security risk management costs should be considered at the earliest opportunity, ideally before programme activities commence, to ensure that both partners have the funding they need to carry out project activities safely and securely.

Funding security risk management is essential to allow staff to safely and securely reach the communities they seek to assist. Unfortunately,

L/NGO staff often face barriers that make it difficult for them to ask for additional funding in partnership arrangements, and security-related budget lines are the most likely to be left out when there is pressure to cut costs. INGO partners can address some of these challenges by initiating conversations around funding security risk management with L/NGOs rather than waiting for a funding request to come through.



**Partners should support each other in identifying, asking for, and openly discussing SRM funding needs, as this is a condition of good programming and meeting organisational duty of care obligations.**

Security risk management costs include any expense related to reducing the potential for harm or loss to the organisation and its workforce or compensating for actual harm or loss. Example costs may include:

- Developing and implementing policies and procedures;
- Salaries of security focal points;
- Security training and awareness-raising activities;
- Carrying out **security risk assessments**;
- Responding to incidents, including programme suspension or closure;
- Insurance;
- Equipment to support security, including communications;
- Provision of physical security, including gates, locks, etc;
- Employee welfare and psycho-social support services.

**TOOLS 3 & 4:** Joint SRM review questionnaire and worksheet template and joint SRM review action plan template can help partners consider funding gaps and identify ways to cover SRM costs more broadly within the partnership

**TOOL 5:** Joint security risk assessment and management plan template can be used as a basis for costing security risk management within a partnership in relation to identified security risks



**If funding is insufficient to adequately manage the security risks that staff are exposed to, partners should reconsider the project or programme in line with their agreed risk threshold.**

Previous research by GISF has found that most international donors are open to the inclusion of security risk management costs in project budgets. It is imperative that partnership project proposals include the required budget to manage security risks and that this is evidenced through context-specific **security risk assessments**. Proposal writers should know the relevant donor's policy position on security risk management funding, as well as their own organisation's and the partner's security risk management needs, so that the assessed security risk management activities are appropriately resourced.



#### **TOOL 6:** Security risk management in partnerships budget template

If including security costs in proposals is problematic, grant managers, programme staff and organisational leaders should advocate with donors for the inclusion of security costs.

► See section 4.2.3. *Security risk management advocacy and funding*



#### **Further information**

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

### **3.3. Strengthening security risk management capacity in partnerships**



**'All staff need to know how they should manage security risks within their role.'**

#### **Security Focal Point**

GISF's research has shown that there is a widespread misperception that knowledge and expertise on security risk management – and many other aspects of aid delivery – are held at the INGO level. 'Capacity building' for L/NGO staff is often perceived as a default necessity and may follow the model of one- to two-day security trainings or briefings. While each L/NGO will be different, this view does not represent the capacities of many L/NGOs in the aid sector.



Research has shown that L/NNGOs demonstrate extensive competencies in:

- Establishing and maintaining acceptance, e.g., preserving quality and long-term relationships with beneficiaries;
- Coordination and negotiation;
- Analysing and understanding the local context (including community dynamics, local conflicts, and politics);
- Engaging with and understanding affected people, their needs and aspirations.

International partners should not assume that an L/NNGO lacks security thinking and actions just because it does not have written rules or the same approach to security risk management. Similarly, just because L/NNGOs have a good understanding of the local context, it cannot be assumed they do not experience security risks or that they have the capacity needed to manage them. Conversely, L/NNGOs should not assume that INGOs have all the necessary capacity, knowledge or resources to effectively manage security risks. INGOs often rely on local knowledge and ways of working to securely operate in high-risk contexts.

Partners should begin by identifying existing capacity within the partnership and agree on the capacity areas that need strengthening. An overview of needs and gaps can be determined using the **joint SRM review**.

► See Part 2. Carry out a joint review of security risk management

For long-term partnerships, more detailed approaches to strengthening security risk management capacity are advisable. A number of tools exist that can support these efforts.



### Further information

- Cinfo's *Duty of Care Maturity Model Tool* can support organisations in measuring their maturity against key areas related to meeting **duty of care** and improving security risk management.
- Annex 1 in EISF's *Security Management and Capacity Development: International agencies working with local partners* presents a simplified partner security level assessment tool.

In discussions around capacity strengthening, partners should aim for complementarity of different approaches to security risk management, building on what is already in place and effective in managing security risks. Part of this conversation involves discussing what opportunities for development already exist.



*'Some of our partners...are already receiving capacity building from other actors – discussing that helps avoid duplication of resources. It might also flag up where there could be shared interests among a group of actors to work together on a specific piece of work (e.g. collective training).'*

INGO Security Focal Point



**Security risk management capacity strengthening efforts should be as sustainable as possible and outlast the partnership itself.**

Capacity strengthening activities may include:

- Providing information and resources on security and making sure these are accessible to the staff who need them (e.g., consider if they need to be translated or provided in a non-written format).
- Providing security training that meets the needs of staff, whether this is training by L/NNGOs for their international partners on the local context and effective security strategies, or INGOs providing L/NNGO staff with context-appropriate security training (including supporting L/NNGO staff's access to regional or national inter-agency personal security training courses).
- Adopting a 'training of trainers approach' (ToTs) to ensure that trained staff have the capacity to pass on the acquired knowledge and resources.
- Embedding expertise into the partner organisations. For example, seconding staff from one partner organisation to the other, to encourage the in-depth sharing of information, knowledge and ways of working.
- Developing formal mentoring schemes between security focal points in both organisations or with mentors outside of the partnership (see INSSA, for example, in further resources below).
- Collaborating with other organisations, both international and local, to share resources to support security capacity strengthening, including the provision of inter-agency security training directly or through third-party providers, for example, independent consultants or security training providers.



**It is important for partners to monitor and evaluate capacity strengthening efforts in the short and long-term. This can be done through the regular review of the **joint SRM review action plan**.**



#### TOOL 4: Joint SRM review action plan template

##### Adapting capacity strengthening activities due to external factors

Environmental, safety and security factors can make the provision of capacity strengthening activities challenging. Approaches need to be flexible and adapt to quickly changing circumstances. Organisations should be creative and cater to the needs of the most vulnerable staff.

##### The challenge of staff poaching

An unfortunate side effect of capacity strengthening efforts can be that local staff members become more attractive to organisations, usually INGOs, that can offer a higher salary. It can be challenging for L/NNGOs to compete with INGOs as employers, particularly if they lack core funding, and this can affect their ability to retain a strong central team.

This issue requires discussion between partners and is a topic of discussion within the broader **localisation** agenda. The Charter4Change, which has been endorsed by several hundred organisations, expects signatories to identify and implement fair compensation (such as paying a recruitment fee) to a local organisation if they contract their staff member in a humanitarian setting.



#### Further information

- *EISF – Security Management and Capacity Development: International agencies working with local partners (particularly Annex 1)*
- *EISF – Security Risk Management: a basic guide for smaller NGOs*
- *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*
- *GISF website – training hub*
- *ICRC – Safer Access Framework*

The following platforms provide free personal security and security risk management training:

- *INSSA website*
- *DisasterReady Platform*
- *UNDSS*
- *IFRC's Stay Safe training*
- *Kaya Connect*

To measure an organisation's maturity in security risk management from a duty of care perspective see:

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

# 4

## Advocate for change: strengthening security in the aid sector through partnerships

### 4.1. Joint advocacy



*'A voice that represents many actors, that is echoed by many, and that is clear and evidence based, is a powerful voice that can effectively influence third parties and targets.'*

ICVA – NGO Fora Advocacy Guide

Advocacy is about influencing change. While working in partnership, organisations may identify security-related issues that are beyond their ability to address as individual organisations or within the partnership. For these types of challenges, partners should consider engaging in collective advocacy efforts to influence change within the broader aid sector.

Security-related advocacy aims may include:

- Positioning security risk management as a central consideration in all programmatic discussions, rather than it being treated as an 'add on';
- Ensuring that security focal points are included in high-level and strategic debates;
- Ensuring greater inclusion of security risk management in **localisation** agenda discussions;
- Ensuring donors meet the security risk management funding needs of both partner organisations;
- Ensuring greater access for both partners to security resources, collaborations and networks.

Partner organisations are particularly well-placed to engage in advocacy efforts as they can tackle these challenges together and build on each other's strengths to influence change.

Partners can develop a joint advocacy strategy by identifying common goals, objectives, targets, messages, allies and opportunities. This can be done in a formal manner (following the guidelines shared in Figure 5

overleaf), or more informally by:

1. Jointly identifying what changes the partners want to see;
2. Making allies, within each organisation, within the partnership, and outside the partnership;
3. Speaking up together, building on knowledge and evidence gathered.



**It is imperative that advocacy staff and security focal points work together in both partner organisations so that any advocacy efforts build on the knowledge and expertise of security experts.**

### Separate advocacy efforts

While partnerships offer organisations a unique opportunity to engage in joint advocacy, partner organisations can benefit from also engaging in separate advocacy efforts.

INGOs, for example, are often better positioned with donors and as members of international advocacy groups to advocate on behalf of L/NNGOs. INGOs should use their influence to promote better security for L/NNGOs, for example, by advocating with donors for adequate security budgets for local and national organisations.



**INGOs have a responsibility to use their position to advocate on behalf of L/NNGOs.**

L/NNGOs, on the other hand, can engage in their own advocacy efforts, for example, to change their relationships with their international partners when these partners are not responsive to the needs of the L/NNGO.



**L/NNGOs should develop an advocacy agenda independently or with other L/NNGOs to advocate for change when international actors, including their INGO partners, are not responsive to their needs.**

Figure 5: Advocacy strategy: key steps and questions



Adapted from ICVA's NGO Fora Advocacy Guide

## 4.2. Security risk management and advocacy efforts

This section provides examples of how organisations can engage in advocacy related to security, and highlights challenges that could be addressed through security-related advocacy.

### 4.2.1. Protecting aid workers against targeted attacks

By working together, aid organisations can draw attention to the security risks faced by their staff and call for the greater protection of aid workers. The '**Not A Target**' movement is one example of this type of effort (activities related to this movement on social media are using the hashtag #NotATarget).

The collaboration between humanitarian organisations – and in particular between international and local actors – in these efforts is essential. Much of the work to highlight attacks faced by healthcare workers relies on evidence from local sources. Reports by the Syrian Network for Human Rights, for example, document attacks against civilians, healthcare professionals and others. This evidence allows the organisation and its partners to advocate for the greater protection of civilians and other non-combatants, including healthcare workers, in Syria.



**Evidence of security risks can play an important role in messaging and help with meeting advocacy objectives.**

The collection of security incident information affecting staff from multiple organisations, even if not originally intended for advocacy purposes, can also help organisations identify trends and present evidence of security-related challenges, which can lead to collective advocacy efforts. For example, the Safeguarding Health in Conflict Coalition uses data on security incidents reported by multiple organisations to advocate for greater protection of healthcare workers in conflict environments. For these types of efforts, pooled incident data from multiple organisations is important.

Partners can also jointly engage in advocacy in the event of a serious incident. For example, in August 2020, seven staff members from the NGO ACTED were tragically killed in Niger. This incident led ACTED to launch a global call to action to improve the protection of aid workers. The call to action was joined by 63 other organisations, and resulted in high-level conversations within the French government and the United Nations on compliance with international humanitarian law and the need to improve aid worker protection.



### 4.2.2. Security risk management advocacy and the localisation agenda

International and local organisations may also consider engaging in advocacy to improve understanding and efforts to address security-related challenges within partnerships. The Grand Bargain and **localisation** agenda have focused extensively on shifting decision-making power to L/NNGOs within the humanitarian space. This shift has been supported by noteworthy initiatives such as the Charter4Change and the Alliance for Empowering Partnership (A4EP). This shift, however, has not resulted in greater dialogue on the security needs of L/NNGOs within the localisation agenda or the aid sector more broadly. This is a significant and telling gap.

Advocacy teams that are working on the localisation agenda in both partner organisations should collaborate with their security focal points to advocate for greater consideration and dialogue around the security risks faced by L/NNGOs. For example, the greater inclusion of security risk management in localisation-focused tools, such as the Localisation Performance Measurement Framework produced by NEAR (Network for Empowered Aid Response), would be a positive step.

### 4.2.3. Security risk management advocacy and funding

Organisations require sufficient and dedicated funding to manage security risks. However, funding is increasingly competitive for organisations, particularly L/NNGOs, and can often fall short of what is actually required. To obtain sufficient security funding, organisations may need to engage in advocacy efforts that target their partners or donors, either as individual organisations or through collective advocacy.

Organisations that fear raising concerns with donors and partners around funding gaps related to security risk management may find it easier to engage in collective advocacy campaigns with other NGOs. L/NNGOs, for example, could use platforms such as NEAR to advocate that their INGO partners ensure they have adequate security funding.



**Where INGOs themselves struggle with security funding, they should aim to include support for security risk management for themselves and their L/NNGO partners in any advocacy strategy they have towards donors.**

A key element of an effective advocacy strategy of this kind is being clear on the security funding needs and gaps of both partners. Security focal

points can play an important role in this type of advocacy by providing examples to their advocacy colleagues of any security challenges that can arise due to existing security funding gaps.

► See section 3.2. Funding security risk management in partnerships

#### Example The ‘At What Cost’ campaign

In July 2019, GISF (then EISF) launched a campaign called ‘At What Cost?’ to raise awareness of inadequate funding for security within the aid sector. The campaign’s open letter challenged the practice within the aid sector of allocating an arbitrary percentage for security costs in budgets – a practice that fails to recognise the diversity in contexts, operations, organisations, and risks that aid organisations face. The letter pushed for the inclusion of dedicated, explicit budget lines for staff safety and security, with key messages targeted at different groups:

*‘EISF...calls upon the aid sector to reignite the conversation about security risk management funding so that staff safety and security is not side-lined in budgets. To aid workers at all levels, we ask you to question how the true cost of your safety is included in programme budgets. To security managers, we call on you to lobby your organisations to include safety and security as a direct budget line. To donors, we call on you to coordinate with non-governmental organisations to reform funding processes for security risk management.’*

EISF Open Letter to Non-Governmental and Donor Organisations

This open letter was signed by almost 200 stakeholders working in 38 countries around the world. By calling on donors, security managers and all aid workers to be more aware and to push for adequate funding for security, the letter succeeded in raising awareness and bringing about concrete change. Following the campaign, the UK’s Department for International Development (DFID, replaced in September 2020 by the Foreign, Commonwealth and Development Office) announced that they would update the template and guidance for their Rapid Response Facility to include a specific line for security risk management.





## Further information

- *Oxfam and the Open University – ‘Make Change Happen’ course*
- *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 and EISF – Security Incident Information Management Handbook (particularly ‘Section 4.5 Using security incident information for strategic advocacy’)*
- *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*

Organisations and initiatives engaged in localisation work include:

- *NEAR*
- *Charter4Change resources*
- *A4EP*

# 5 Tools

- **Tool 1**  
**Good communication in partnerships**
- **Tool 2**  
**Risk attitude in partnerships**
- **Tool 3**  
**Joint SRM review questionnaire and worksheet template**
- **Tool 4**  
**Joint SRM review action plan template**
- **Tool 5**  
**Joint security risk assessment and management plan template**
- **Tool 6**  
**Security risk management in partnerships budget template**





## Tool 1

### Good communication in partnerships

This tool presents guidance on how to evaluate the quality of communications within partnership arrangements.

There are often misunderstandings between partners around security risks and contexts. Differences in communication cultures and language barriers are particularly challenging for meaningful and in-depth discussions around security risks, e.g., oral versus written cultures, lack of face-to-face engagement. Security-focused staff also often use jargon, with many concepts difficult to translate into different languages.

Partners should regularly review the quality of their communication and identify the main obstacles to their exchange. Partners can use this tool as an individual exercise to improve communication, or as a joint evaluation tool to compare different approaches to communication and to address any misunderstandings.

#### Exercise: Assess the quality of your communication (for example, e-mail, letter, phone call, face-to-face meeting)

1. Is the communication clear?
2. Does the communication avoid the use of jargon and acronyms?
3. Is the communication transparent about motivations and aims (i.e., is it clear why you are communicating and what you hope to get from the communication)?
4. Is the communication channel and method appropriate for the recipient?
5. Is the communication culturally sensitive, positive, respectful and based on the notion of equity (i.e., avoiding negative, top-down and demanding language)?
6. Does the communication show compassion for the particular circumstances of the recipient individual and organisation as a whole?
7. Is the communication relevant for all recipients, and if not, how can this be addressed (e.g., some staff may feel it is unnecessary to be involved in security discussions when they do not have security responsibilities or operate in low-risk areas)?

#### Evaluation: Review communication within the partnership more generally

1. Is trust evident in communications between partners?
2. Is information shared proactively between the partners?
3. Do the partners seek feedback from each other regularly, both formally and informally, including on how effective communication has been between them?
4. Are the communication outputs necessary or are they excessive?
5. Do the partners take responsibility for what has been said or done?
6. Is communication consistent? (In frequency, nature and in expectations from each partner.)
7. Are the right people receiving the communication? If not, why not? Address any cultural or language barriers.
8. Can an interlocutor be brought in to strengthen communication between the partners?
9. Can the partners jointly address digital security concerns which may cause staff to avoid using particular communication platforms (i.e., in some contexts, e-mails and phone calls may be intercepted by government actors)?
10. Where the security of certain types of communication is a concern, are alternative forms of communication (such as face to face) provided to all staff?

► See section 1.4. for further guidance on good communication



## Tool 2

### Risk attitude in partnerships

This tool allows partners to explore and develop a mutual understanding of risk attitude and acceptance. The tool should be used to develop an ongoing discussion for partners and should be reviewed on a regular basis.

#### Step 1: Define what likelihood and impact mean

How severe a risk is will depend on how likely it is that the event will occur, and if it did occur, how severe the impact would be. Partners should discuss what they understand by 'likelihood' and 'impact' in practice by defining each of the impact and likelihood categories (listed below). This discussion will enable both partners to compare the risks based on a similar understanding, e.g., one partner may consider 'unlikely' to be once per month, whereas the other partner may define it as once per year. When defining what each category of 'impact' means, partners should consider personnel, equipment and the relevant programme(s).

| Likelihood |                   | Definitions  |
|------------|-------------------|--|
| 1          | Very Unlikely     | For example:<br>More than – once per decade<br>Less than – once per year   |
| 2          | Unlikely          |  |
| 3          | Moderately Likely |  |
| 4          | Likely            |  |
| 5          | Very Likely       |  |
| Impact     |                   | Definitions  |
| 1          | Negligible        | For example:<br>Personnel – minor injuries to one staff member<br>Equipment – loss of non-essential equipment<br>Programme – temporary loss of access due to seasonal weather challenges |
| 2          | Minor             |  |
| 3          | Moderate          |  |
| 4          | Severe            |  |
| 5          | Critical          |  |

Step 2: Develop a matrix to agree on acceptable levels of risk

Partners can use a matrix, which compares the likelihood of an incident with its impact (sometimes numerically calculated as Likelihood x Impact), to identify, for each partner, where the level of acceptable risk lies within the partnership. Acceptable risk levels should be highlighted in green. The matrix below serves only as an example and each organisation/ partnership will have different levels of risk acceptance and should therefore adapt the assessment of risk acceptance to meet their needs.

| LIKELIHOOD            | IMPACT         |            |              |            |              |
|-----------------------|----------------|------------|--------------|------------|--------------|
|                       | Negligible = 1 | Minor = 2  | Moderate = 3 | Severe = 4 | Critical = 5 |
| Very Likely = 5       | (1x5) = 5      | (5x2) = 10 | 15           | 20         | 25           |
| Likely = 4            | 4              | 8          | 12           | 16         | 20           |
| Moderately Likely = 3 | 3              | 6          | 9            | 12         | 15           |
| Unlikely = 2          | 2              | 4          | 6            | 8          | 10           |
| Very Unlikely = 1     | 1              | 2          | 3            | 4          | 5            |

Beyond focusing on the resulting number, partners are encouraged to think whether the risk is low/medium/high and make an assessment on that basis.



Tool 3  
Joint SRM review questionnaire and worksheet template

This template provides a list of example questions followed by example indicators that partners can jointly answer and assess. Indicators can be assessed for the partnership as a whole, or when appropriate, by each partner organisation using a three-tier assessment system: present, partially present and not present. The purpose of this tool is to encourage an honest and open conversation between partners about security risk management capacities, resources, gaps and needs within each organisation and the partnership as a whole. This tool includes some of the questions and indicators presented in Part 2 of this guide.

This is NOT a ‘security risk management tool’ but a ‘partnership management tool’. This is also NOT a tool to evaluate the strengths or weaknesses of a partner organisation’s security risk management system.

Please note that this is only an example list of questions and indicators and the template should be adapted by the partners to include questions and indicators that are relevant to their specific needs and situation.

► For additional questions and indicators, please refer to Part 2 of this guide



| Part 1: Duty of care |  |                |            |                      |                    |
|----------------------|--|----------------|------------|----------------------|--------------------|
| Ref no.              | Question   | Answer         |            |                      | Notes              |
| 1.1.                 | What are the legal and moral duty of care obligations of each partner to each other, if any?   | L/NNGO         |            |                      |                    |
|                      |  | INGO           |            |                      |                    |
| 1.2.                 | What are the legal and moral duty of care obligations of each partner to their respective staff, beneficiaries and affected communities?   | L/NNGO         |            |                      |                    |
|                      |  | INGO           |            |                      |                    |
| 1.3.                 | Are the psycho-social needs of all staff considered and addressed, and what actions, if any, can the either partner take to improve the care of implementing staff, e.g., insurance cover, psycho-social well-being? | L/NNGO         |            |                      |                    |
|                      |  | INGO           |            |                      |                    |
| Ref no.              | Assessment indicator   | Partnership    | L/NNGO     | INGO                 | Notes and evidence |
| 1.1.                 | Legal duty of care obligations are understood and being met by both partners.  | <i>Not met</i> | <i>Met</i> | <i>Partially met</i> |                    |
| 1.2.                 | Moral duty of care obligations have been discussed and agreed by both partners.  |                |            |                      |                    |

| Part 2: Governance and accountability |   |                |            |                      |                    |
|---------------------------------------|---|----------------|------------|----------------------|--------------------|
| Ref no.                               | Question  | Answer         |            |                      | Notes              |
| 2.1.                                  | Do both partners have suitable security risk management structures in place to enable the partnership objectives to be met?   | L/NNGO         |            |                      |                    |
|                                       |   | INGO           |            |                      |                    |
| 2.2.                                  | Do both partners have a clear understanding of roles and responsibilities relating to security risk management with regards to the partnership and implementation of programmes? For example, do both organisations have a security focal point who can be the main point of contact for partners on security issues? | L/NNGO         |            |                      |                    |
|                                       |   | INGO           |            |                      |                    |
| 2.3.                                  | How does each partner perceive risk transfer in the partnership (if at all)? What actions do each partner think they can take to move from risk transfer to risk sharing?   | L/NNGO         |            |                      |                    |
|                                       |   | INGO           |            |                      |                    |
| Ref no.                               | Assessment indicator  | Partnership    | L/NNGO     | INGO                 | Notes and evidence |
| 2.1.                                  | A statement of accountability and governance pertaining to safety and security risk management within the partnership exists.   | <i>Not met</i> | <i>Met</i> | <i>Partially met</i> |                    |
| 2.2.                                  | A reporting and accountability process (with defined content and frequency) exists for informing each partner of safety and security risk issues. This includes clarity on both partners' responsibilities with regards to security risk management within the partnership.   |                |            |                      |                    |
| 2.3.                                  | Both partners have a focal point explicitly assigned, with responsibility for governance of safety and security risks for the organisation and partnership.   |                |            |                      |                    |

## Part 3: Policy and principles

| Ref no. | Question  | Answer      |        |               | Notes              |
|---------|---|-------------|--------|---------------|--------------------|
| 3.1.    | Are the mandate, mission, values and principles of each organisation understood by both partners, and are both organisations comfortable with each other's work and approach to operations and security (e.g., do both partners agree to each other's position regarding adherence to humanitarian principles)? | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 3.2.    | Is there agreement by the partners on practical minimum security requirements that must be in place in each location or activity? (Please note that while these should apply to both partners, they must also be realistic and adapted to each organisation's capacity.)  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 3.3.    | How do the partners define and approach risk attitude, and is there agreement between the partners on what is an acceptable risk threshold for the partnership and programmes within it?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| Ref no. | Assessment indicator  | Partnership | L/NNGO | INGO          | Notes and evidence |
| 3.1.    | Security risk management policies and their implementation (through plans, procedures, and/or guidelines) are appropriate to the local context and partnership circumstances, and accessible to all staff (i.e., available in relevant languages and formats).  | Not met     | Met    | Partially met |                    |
| 3.2.    | The partnership agreement includes a statement relating to a joint understanding and agreement of the risk threshold for partnership activities.  |             |        |               |                    |
| 3.3.    | The partnership agreement does not contradict – but where possible reinforces – both partners' security policies (e.g., provisions around the use of armed escorts).  |             |        |               |                    |

## Part 4: Operations and programmes

| Ref no. | Question  | Answer      |        |               | Notes              |
|---------|---|-------------|--------|---------------|--------------------|
| 4.1.    | What are the security needs and expectations of each partner?   | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 4.2.    | Do the partners have an agreed system in place to identify and monitor security risks faced by staff? (Is there alignment between both organisations' security risk assessments and security plans for the locations in which the implementing partner operates? What are the divergences, and why are they different?) | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 4.3.    | Do the partners agree on who is responsible for managing identified risks, and how these should be managed and funded?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| Ref no. | Assessment indicator  | Partnership | L/NNGO | INGO          | Notes and evidence |
| 4.1.    | A joint security risk assessment of operations, associated risks and overlap/impact on each partner has occurred, with a clear process in place for regularly updating the analysis. This assessment includes an analysis of internal risks and those that might be a result of the partnership itself.                 | Not met     | Met    | Partially met |                    |
| 4.2.    | Explicit budget lines for meeting security requirements are present in the partnership budget, including capacity strengthening activities, and deemed sufficient to meet all resource requirements by both partners.   |             |        |               |                    |
| 4.3.    | Context-specific security strategies or approaches have been agreed between the partners and are articulated and communicated to all relevant parts of each organisation.   |             |        |               |                    |



## Part 5: Travel management and support

| Ref no. | Question  | Answer         | Notes      |                      |                    |
|---------|---|----------------|------------|----------------------|--------------------|
| 5.1.    | How should security risks resulting from travel related to the partnership be managed? What should be the minimum requirements for travel management and support arrangements (for field travel, overnight stay, travel communication procedures and other support)? For example, security briefings, check-in procedures, vehicle maintenance, travel risk assessments, driver training, confidential travel information management. | L/NNGO         |            |                      |                    |
|         |   | INGO           |            |                      |                    |
| 5.2.    | Is equitable support on travel and stay provided to both organisation's staff in the project locations?   | L/NNGO         |            |                      |                    |
|         |   | INGO           |            |                      |                    |
| 5.3.    | Do the partners agree on the security policy and procedures that should be followed during partners' visits, and who holds duty of care for visiting staff?   | L/NNGO         |            |                      |                    |
|         |   | INGO           |            |                      |                    |
| Ref no. | Assessment indicator  | Partnership    | L/NNGO     | INGO                 | Notes and evidence |
| 5.1.    | The partners agree on security arrangements and responsibilities for staff visits from both organisations to each other's offices and programme locations.  | <i>Not met</i> | <i>Met</i> | <i>Partially met</i> |                    |
| 5.2.    | Partners share with each other their security procedures for travelling staff for locations that are relevant to the partnership (e.g., these procedures can include information on roles and responsibilities, training and briefings, check-in procedures, travel monitoring, travel authorisations, and emergency procedures).   |                |            |                      |                    |
| 5.3.    | The diverse security risks and needs of travelling staff are considered within travel procedures, e.g., heightened risk due to personal characteristics (gender, ethnicity, ability, etc.).   |                |            |                      |                    |

## Part 6: Awareness and capacity strengthening

| Ref no. | Question   | Answer         | Notes      |                      |                    |
|---------|--|----------------|------------|----------------------|--------------------|
| 6.1.    | How will partners identify security awareness and capacity strengthening needs and jointly meet these (both for personal safety and security risk management)?   | L/NNGO         |            |                      |                    |
|         |  | INGO           |            |                      |                    |
| 6.2.    | Is there agreement on what security risk management capacity gaps there are within both partners, and what each organisation can do to address them?   | L/NNGO         |            |                      |                    |
|         |  | INGO           |            |                      |                    |
| 6.3.    | Does the partnership budget include funding to support long-term capacity strengthening activities?  | L/NNGO         |            |                      |                    |
|         |  | INGO           |            |                      |                    |
| Ref no. | Assessment indicator   | Partnership    | L/NNGO     | INGO                 | Notes and evidence |
| 6.1.    | Security risk management capacity needs are agreed between the partners.   | <i>Not met</i> | <i>Met</i> | <i>Partially met</i> |                    |
| 6.2.    | There is a capacity strengthening learning and development strategy in place, with a clear implementation plan, and its aim is to improve the long-term capacity of partners.  |                |            |                      |                    |
| 6.3.    | The organisation regularly shares resources and supports access to appropriate and context-specific opportunities for capacity strengthening, learning and development opportunities in security risk management with partner organisations. |                |            |                      |                    |

| Part 7: Incident monitoring |  |                |            |                      |                    |
|-----------------------------|--|----------------|------------|----------------------|--------------------|
| Ref no.                     | Question   | Answer         |            |                      | Notes              |
| 7.1.                        | How should the partners share incident information with each other, if at all?   | L/NNGO         |            |                      |                    |
|                             |  | INGO           |            |                      |                    |
| 7.2.                        | How can partners support each other's security incident information management? For example, incident reporting procedures, incident logging systems, and tools to analyse incident data and use it to inform decisions on security, programmes, operations, advocacy, finance, etc. | L/NNGO         |            |                      |                    |
|                             |  | INGO           |            |                      |                    |
| 7.3.                        | What security incident data in the relevant location does each organisation have access to, either from its own operations or through its networks, that it can share with its partner on a regular basis?   | L/NNGO         |            |                      |                    |
|                             |  | INGO           |            |                      |                    |
| Ref no.                     | Assessment indicator   | Partnership    | L/NNGO     | INGO                 | Notes and evidence |
| 7.1.                        | A process for managing and sharing security information, including incident data, between partners for the operating context is in place and adhered to.   | <i>Not met</i> | <i>Met</i> | <i>Partially met</i> |                    |
| 7.2.                        | There is agreement on how incident data is used to inform decision-making, including a clear policy on whether any punitive actions may result from the reporting and non-reporting of incidents.  |                |            |                      |                    |
| 7.3.                        | The organisation periodically reviews incidents affecting its staff to identify security incident trends and concerns and shares these with partner organisations.   |                |            |                      |                    |

| Part 8: Crisis management |   |                |            |                      |                    |
|---------------------------|---|----------------|------------|----------------------|--------------------|
| Ref no.                   | Question  | Answer         |            |                      | Notes              |
| 8.1.                      | How will the partners collaborate/coordinate in the event of a crisis or critical incident affecting either organisation in the location where the partnership is active?                             | L/NNGO         |            |                      |                    |
|                           |   | INGO           |            |                      |                    |
| 8.2.                      | If a crisis or critical incident takes place and affects both partners, who should lead the crisis management response? What are the responsibilities and who has decision-making authority?          | L/NNGO         |            |                      |                    |
|                           |   | INGO           |            |                      |                    |
| 8.3.                      | What support can each partner provide the other in the event either organisation experiences a critical incident in the partnership location?   | L/NNGO         |            |                      |                    |
|                           |   | INGO           |            |                      |                    |
| Ref no.                   | Assessment indicator  | Partnership    | L/NNGO     | INGO                 | Notes and evidence |
| 8.1.                      | Responsibilities and decision-making authority in the event of a crisis or critical incident affecting both partners are agreed, ideally in writing or visualised in some manner (e.g., a flowchart). | <i>Not met</i> | <i>Met</i> | <i>Partially met</i> |                    |
| 8.2.                      | Partners have a crisis management structure and plan in place.  |                |            |                      |                    |
| 8.3.                      | Partners have access to emergency support services (medical and non-medical) as part of each organisation's insurance cover.  |                |            |                      |                    |

## Part 9: Security collaborations and networks

| Ref no. | Question  | Answer      |        |               | Notes              |
|---------|---|-------------|--------|---------------|--------------------|
| 9.1.    | Are there platforms in the relevant context that discuss security issues? If yes, do both partners have access and an equal voice in these coordination platforms and networks in their operational areas, including security information sharing platforms?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 9.2.    | What are the barriers and challenges that impede the active participation of both partners in inter-agency forums, meetings and discussions on security at the local, national, regional and international level?   | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 9.3.    | What actions can either organisation take to facilitate the inclusion of their partner in these discussions?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| Ref no. | Assessment indicator  | Partnership | L/NNGO | INGO          | Notes and evidence |
| 9.1.    | Both partners actively participate in security risk management forums, platforms, meetings and consortia, and share safety and security information with others at the local, national, regional and/or international level.  | Not met     | Met    | Partially met |                    |
| 9.2.    | Both organisations advocate for and facilitate the participation of their partners, where possible, in inter-agency forums, platforms, meetings and discussions in order to strengthen information-sharing and security collaboration. This includes sharing contact information with partners of relevant actors who can provide security risk management support. |             |        |               |                    |

## Part 10: Compliance and effectiveness monitoring

| Ref no. | Question  | Answer      |        |               | Notes              |
|---------|---|-------------|--------|---------------|--------------------|
| 10.1.   | How should both partners regularly review security risk management within the partnership?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 10.2.   | What level of compliance and effectiveness monitoring in relation to security risk management within each organisation and/or the partnership is agreeable to both partners?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 10.3.   | How much information relating to lessons learned, reviews, security audits, and post-incident analysis relating to the context, the partnership, or a particular project, are the partners willing to share with each other?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| Ref no. | Assessment indicator  | Partnership | L/NNGO | INGO          | Notes and evidence |
| 10.1.   | Outcomes of lessons learned, reviews, post-incident analysis, and security audits relating to the context, the partnership or the project/programme, are shared between and discussed by both partners.   | Not met     | Met    | Partially met |                    |
| 10.2.   | Persons responsible for monitoring safety and security system implementation and compliance (both within each organisation and within the partnership) are properly trained, were involved in the joint security risk management assessment, and have these responsibilities explicitly stated in their job descriptions. |             |        |               |                    |
| 10.3.   | Employee performance management systems make explicit reference to safety and security responsibilities, and compliance with the organisation's policies.   |             |        |               |                    |

## Part 11: Supporting resources

| Ref no. | Question  | Answer      |        |               | Notes              |
|---------|---|-------------|--------|---------------|--------------------|
| 11.1.   | Are supporting resources on security risk management available and accessible to both partner organisations' staff, and if not, what actions can be taken to improve accessibility? | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 11.2.   | Have partners shared their respective resources on security risk management with each other?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| 11.3.   | What other resources would the partners benefit from to help them manage security risks?  | L/NNGO      |        |               |                    |
|         |   | INGO        |        |               |                    |
| Ref no. | Assessment indicator  | Partnership | L/NNGO | INGO          | Notes and evidence |
| 11.1.   | Resources on security risk management that meet the needs of all relevant partner staff are regularly shared in a format that is accessible to them.                                | Not met     | Met    | Partially met |                    |
| 11.2.   | Partners make available a range of guidance, tools and templates as part of a security library to assist each other in managing security risks.                                     |             |        |               |                    |



## Tool 4

## Joint SRM review action plan template

This action plan template serves to help partners agree on actions needed to address gaps identified during the assessment of security risk management indicators. Indicators that were deemed present in the assessment exercise do not need to be included in the action plan.



The joint SRM review action plan is a tool to help partners implement the joint SRM review process presented in this guide and is, therefore, a partnership management tool. This is NOT a tool to manage actual security risks.

## Part 1: Duty of care

|                  |             |   |
|------------------|-------------|---|
| Reference no.    |             | Insert indicator reference number   |
| Indicators       |             | Insert indicator  |
| Assessment       | Partnership | Present   |
|                  | L/NNGO      | Partially present   |
|                  | INGO        | Not present   |
| Priority         |             | Urgent/ Intermediate/ Not urgent  |
| Actions required |             | Detail actions required to address gap.<br>Consider if there is sufficient funding to implement relevant actions. |
| Responsible      |             | Identify an individual or department within the relevant partner organisation responsible for this action.        |
| Timeline         |             | Set a realistic timeline.   |
| Date of review   |             | Agree on a date when progress is reviewed by both partners.   |

**Part 2: Governance and accountability**

|                  |  |                             |
|------------------|--|-----------------------------|
| Reference no.    | For example: 2.2   |                             |
| Indicators       | For example: A reporting and accountability process (with defined content and frequency) exists for informing each partner of safety and security risk issues.   |                             |
| Assessment       | Partnership  | For example: Present        |
|                  | L/NGO  | For example: Not present    |
|                  | INGO   | For example: Not applicable |
| Priority         | For example: Urgent  |                             |
| Actions required | For example: Agree and develop a process as part of the partnership security working group. Does not require additional funding or other resources. Consider if there is sufficient funding to implement relevant actions. |                             |
| Responsible      | For example: Partnership security working group (insert names)   |                             |
| Timeline         | For example: By 15 February 2022   |                             |
| Date of review   | For example: March 2022 monthly meeting  |                             |

**Part 3: Policy and principles****Part 4: Operations and programmes****Part 5: Travel management and support****Part 6: Awareness and capacity strengthening****Part 7: Incident monitoring****Part 8: Crisis management****Part 9: Security collaborations and networks****Part 10: Compliance and effectiveness monitoring****Part 11: Supporting resources****Tool 5****Joint security risk assessment and management plan template**

This joint security risk assessment and management plan template allows partners to jointly determine the risks they are exposed to, how each organisation may be affected by the partnership, and assess the ways in which identified threats can be mitigated for each partner. The tool should be used to develop an ongoing discussion for partners and should be reviewed on a regular basis.



Please note that this is an example template and each partnership may assess security risks differently. This tool is different from the 'joint SRM review' detailed in this guide. The joint security risk assessment and management template is about identifying and managing actual security risks and therefore a 'security risk management tool', whereas the 'joint SRM review' and associated tools are about exploring SRM more broadly within partnership arrangements and therefore a 'partnership management tool'.

**Step 1: Assess the risks**

- 1.1. Identify the threats.
- 1.2. Consider threats external to the organisations (e.g., abduction, robbery), threats internal to each organisation and threats internal to the partnership (e.g., harassment, fraud).
- 1.3. Discuss how the threat affects each partner. What are the similarities and differences?
- 1.4. Discuss how the vulnerabilities to the threats are different for each partner and whether these are affected by the relationship between the partners (e.g., when international staff of a particular ethnicity are seconded into the local organisation).
- 1.5. Discuss how the impacts of the threats are different for each partner and whether these are affected by the partnership, for example, changes



in local community perceptions because of the partnership (e.g., political affiliations, wealth).

1.6. Using an agreed risk matrix, rate the likelihood and impact and identify whether the level or risk is acceptable to either or both parties.

Note: The downloadable tool is an Excel spreadsheet. It is segmented here for ease of understanding.

| Ref no. | Threat  | Actor       | Vulnerability  | Impact of threat on partners  | Inherent risk        |              |                     | Acceptable risk?<br>Yes/No |
|---------|---|-------------|--|---|----------------------|--------------|---------------------|----------------------------|
|         |   |             |  |   | Likelihood (1-5)     | Impact (1-5) | Risk rating (L x I) |                            |
| E.g: 1a | For example: Road traffic accident in the programme location. | Partnership | The partnership increases the exposure to the threat as it increases the need for implementing staff to travel to new programme location.          | A road traffic accident would affect the safety and well-being of staff, due to injury. It may affect the partnership by delaying and/or impeding the effective delivery of programmes. A road traffic accident may also affect the reputation of the partnership and the partners. | Moderately likely: 3 | Low: 1       | 3                   | Yes                        |
| 1b      |   | L/NNGO      | The exposure of L/NNGO staff is high as they implement the programme and are more likely to travel with untrained drivers or use public transport. | The impact on the L/NNGO would be higher as a road traffic accident would affect implementing personnel, L/NNGO vehicles, as well as be most closely associated with the L/NNGO with regards to legal and reputational issues.  | Moderately likely: 3 | Moderate: 3  | 9                   | Yes                        |
| 1c      |   | INGO        | The exposure of INGO staff is low as they do not travel to the programme unless it is a planned visit.   | The INGO may be impacted indirectly by the accident if it affects the delivery of the programme, the reputation of the partnership/partners, and has budget-related implications that the INGO has responsibility for.  | Very unlikely: 1     | Moderate: 3  | 3                   | Yes                        |

## Step 2: Identify mitigating measures

**2.1.** Identify the risks that cause particular concern to the partnership and/or either partner.

**2.2.** Identify mitigating measures for each risk, including the role of each partner in mitigating the risk.

**2.3.** Identify additional resources and/or inputs that may be required for sustainable/long-term mitigation (e.g., communication equipment, training).

**2.4.** Calculate the residual risk

| Ref no. | Acceptable risk?<br>Yes/No | Mitigation measures<br><br>Consider the roles of each actor to mitigate risks (L/NNGO, INGO, or collectively through the partnership)  | Resources required<br><br>Insert any resources required, for example, personnel, equipment, training. | Residual risk       |                |                     | Acceptable risk?<br>Yes/No | Ongoing Security Risk Management Plan<br><br>• Summarise steps to be taken to implement the mitigation measures and create a security risk management plan<br>• Identify regular monitoring points<br>• Identify key indicators of change for threats |
|---------|----------------------------|--|---|---------------------|----------------|---------------------|----------------------------|---|
|         |                            |  |   | Likelihood (1-5)    | Impact (1-5)   | Risk rating (L x I) |                            |   |
| 1b      | No                         | L/NNGO: Restrict travel on public transport where possible. Train the drivers who transport staff.<br><br>INGO: share safe driving resources with L/NNGO.                              | Personnel<br>Training   | Very unlikely:<br>1 | Moderate:<br>2 | 2                   | Yes                        | Map use of public transport.<br><br>Communicate with staff on travel restrictions.<br><br>Identify trainers for safe driving.<br><br>Undertake training.  |
| 1c      | No                         | INGO: Have formal rules for INGO staff that restrict travel on public transport. Train the drivers who transport staff.<br><br>L/NNGO: Share information on high risk roads with INGO. | Personnel<br>Training   | Very unlikely:<br>1 | Moderate:<br>2 | 2                   | Yes                        |   |

## Step 3: Security risk management plan

**3.1.** Summarise steps to be taken to implement the mitigation measures and create a security risk management plan.

**3.2.** Identify regular monitoring points.

**3.3.** Identify key indicators of change for threats.

| Ref no. | Ongoing security risk management plan  | Indicators of change   | Monitoring                    |
|---------|--|--|-------------------------------|
| 1b      | Map use of public transport.<br><br>Communicate with staff on travel restrictions.<br><br>Identify trainers for safe driving.<br><br>Undertake training. | Increase in road traffic accidents.<br><br>Evidence of non-compliance – e.g., use of public transport. | Who:<br><br>When:<br><br>How: |



**Tool 6**  
**Security risk management in  
partnerships budget template**

This is a joint security risk management expense portfolio template. The template includes examples of security risk management costs that each partner should consider including in a partnership budget. Where necessary, the last two columns allow partners to calculate how much funding is specifically focused on security risk management where costs may be shared by other departments (e.g., salaries of managers who have some security responsibilities).

This tool was adapted from the Risk Management Expense Portfolio (RMEP) Tool in EISF's paper 'The Cost of Security Risk Management for NGOs'. Please consult the RMEP tool for more NGO security risk management expense examples.

| Ref no. | Category                           | Partner | Expense Description  | Units | Cost per unit | Total                   | % of budget line allocated to security risk management | Security risk management total                                   |
|---------|------------------------------------|---------|--|-------|---------------|-------------------------|--|--|
|         | Salaries                           | INGO    | For example, partnership security focal point.   |       |               | = units x cost per unit |  | = total x % of budget line allocated to security risk management |
|         |                                    | L/NGO   | For example, head office and field-based safety and security focal points, managers with security risk management responsibilities.      |       |               |                         |  |  |
|         | Admin & Logistics                  | INGO    | Expenses related to supporting security risk management within a partnership, e.g., travel to partner field sites.                       |       |               |                         |  |  |
|         |                                    | L/NGO   | For example, travel and accommodation for security focal points.   |       |               |                         |  |  |
|         | Training, Learning and Development | INGO    | For example, support to partnership capacity strengthening efforts, e.g., translation.   |       |               |                         |  |  |
|         |                                    | L/NGO   | For example, staff training days on security (including HEAT, driver training, first aid training) and related travel and accommodation. |       |               |                         |  |  |

continued

Security risk management in partnerships budget template *continued*

| Ref no. | Category                                      | Partner | Expense Description   | Units | Cost per unit | Total                   | % of budget line allocated to security risk management | Security risk management total                                   |
|---------|---|---------|---|-------|---------------|-------------------------|--|--|
|         | <b>Information &amp; Knowledge Management</b> | INGO    | <i>For example, costs associated with conducting the joint security risk management assessment.</i>   |       |               | = units x cost per unit |  | = total x % of budget line allocated to security risk management |
|         |   | L/NNGO  | <i>For example, expenses related to carrying out risk assessments, developing security plans and procedures and monitoring staff compliance.</i>                  |       |               |                         |  |  |
|         | <b>Access</b>                                 | INGO    | <i>For example, advocacy with key stakeholders to improve partner security.</i>   |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, community engagement activities.</i>  |       |               |                         |  |  |
|         | <b>Facilities Management</b>                  | INGO    | <i>Usually not applicable for INGO when the L/NNGO is the implementing partner.</i>   |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, building lease, alarm system, safe room construction and maintenance.</i>   |       |               |                         |  |  |
|         | <b>Communications Assets</b>                  | INGO    | <i>For example, translation services to improve accessibility to security-related communications.</i>   |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, communications equipment, Internet.</i>   |       |               |                         |  |  |
|         | <b>Medical Assets</b>                         | INGO    | <i>Usually not applicable for INGO when the L/NNGO is the implementing partner.</i>   |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, first aid kits.</i>   |       |               |                         |  |  |
|         | <b>Transport Assets</b>                       | INGO    | <i>Usually not applicable for INGO when the L/NNGO is the implementing partner.</i>   |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, vehicles with adequate safety standards, drivers.</i>   |       |               |                         |  |  |
|         | <b>Crisis Management Assets</b>               | INGO    | <i>For example, the cost of managing a crisis, such as travel for international staff, if partners agree that the INGO will be involved in crisis management.</i> |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, hibernation and relocation supplies.</i>  |       |               |                         |  |  |
|         | <b>Insurance</b>                              | INGO    | <i>For example, insurance cover for staff involved in the partnership.</i>  |       |               |                         |  |  |
|         |   | L/NNGO  | <i>For example, medical relocation, personal accident insurance.</i>  |       |               |                         |  |  |
|         | <b>General contingency</b>                    | INGO    | <i>Usually not applicable for INGO when the L/NNGO is the implementing partner.</i>   |       |               |                         |  |  |
|         |   | L/NNGO  | <i>Unrestricted funds that may be immediately available in the event of an unforeseen crisis or incident.</i>   |       |               |                         |  |  |



# Glossary

**Bias:** the unfair inclination or prejudice for (or against) a particular group, on the basis of race, ethnicity, and other identity aspects, including nationality. There are four main dimensions of bias:

1. **Structural:** the maintenance of biased policies and practices by multiple institutions, which manifests itself in inequalities in power, opportunities, access, treatment, and policy impacts and outcomes, whether intentional or not.
2. **Institutional:** policies and practices that reinforce prejudice as a result of the systematic unequal distribution of resources, power and opportunity in an organisation.
3. **Interpersonal:** acts and micro-aggressions between individuals on the basis of prejudice.
4. **Internalised:** subtle and overt messages by individuals that reinforce negative beliefs, stereotypes, and self-hatred.

**Duty of care:** The legal and moral obligation of an organisation to take all possible and reasonable measures to reduce the risk of harm to those working for, or on behalf of, the organisation.

**International non-governmental organisation (INGO):** An NGO with operational reach beyond one country or sub-region.

**(Joint) security risk assessment:** A process through which organisations identify the different security and safety threats that could affect their staff, assets and programmes, and analyses threats according to likelihood and impact to determine the degree of risk involved. A joint security risk assessment is carried out together by partners and also analyses the threats that may arise due to the partnership itself.

**Joint security risk management review (the ‘joint SRM review’):**

An approach or process through which partners jointly explore security concepts, their security approaches, and identify what both partners need to do and have in place to strengthen security risk management within the partnership. This is done by completing a questionnaire, agreeing on key indicators and assessing their presence.

**Joint security risk management review action plan (the ‘joint SRM review action plan’):** A detailed to-do list for partners to jointly address gaps in the indicators identified through the joint SRM review process.

**(Joint) security risk management plan:** Sometimes referred to as a ‘security plan’. This is a key document – usually at country level – that outlines the security and safety measures and procedures in place, and the roles and responsibilities all staff have in managing identified risks. A joint security risk management plan is a security plan that is developed and implemented by partner organisations together.

**Localisation:** ‘The process of recognising, respecting and strengthening the independence of leadership and decision making by [local and] national actors in humanitarian action, in order to better address the needs of affected populations.’<sup>1</sup>

**Local non-governmental organisation (LNGO):** An NGO that operates mainly in one distinct geographical area of a country. Its staff are mainly from the communities the NGO serves. Local NGOs are typically larger than community-based organisations (CBOs) and civil society organisations (CSOs) and have a more formal and developed structure.

**Local/national non-governmental organisation (L/NNGO):** A local or national NGO whose operations take place in their home country.

**National non-governmental organisation (NNGO):** An NGO that operates in several parts of a country. Its staff may be transferred to work in areas other than their area of origin.

**Partner:** One member of a formalised (contractual) partnership between aid organisations – usually international-local/national partnerships.

**Partnership:** Any formalised (contractual) relationship between aid organisations, usually international-local/national partnerships. Partnerships in the aid sector can vary in form, length, scope and degree of collaboration.

**Residual risk:** The risk that remains after mitigation measures have been put in place.

**Risk:** How a threat could affect the organisation, its staff, assets, reputation or programmes, considering specific vulnerabilities.

**Risk acceptance:** A process that results in a conscious decision that is understood and accepted by the organisation on the amount of residual risk that an organisation is willing to take.

**Risk attitude:** The organisation’s approach to assessing and eventually pursuing, retaining, taking or turning away from risk.

<sup>1</sup> IFRC definition, retrieved from <https://media.ifrc.org/ifrc/document/ifrc-policy-brief-localization/>



**Risk habituation:** A usually unconscious process of accustoming oneself to the presence of risks resulting from constant exposure to danger, and therefore decreasing one's conscious response to them. Risk habituation is a challenge that both INGO and L/NGO staff can face after prolonged periods of time in one location.

**Risk ownership:** When a person or entity has accountability and authority to manage a risk.

**Risk sharing:** Organisations share responsibility for security risks that affect them.

**Risk transfer:** The formation or transformation of risks (increasing or decreasing) for one actor caused by the presence or action of another, whether intentionally or unintentionally.

**Risk threshold:** The threshold of acceptable risk is reached when, following the implementation of mitigation measures, the residual/current risk level is not supported by an organisation's stated risk attitude.

**Safety:** Freedom from risk or harm resulting from unintentional or accidental acts, events or hazards.

**Security:** Freedom from risk or harm resulting from intentional acts of violence, aggression and/or criminal acts against agency staff, assets or property.

**Security culture:** The culture of an organisation can be defined as 'the way we do things around here'. Every organisation has a culture towards security, safety and risks in general.

**Security tree:** This is a process to quickly communicate news throughout an organisation without overburdening any specific person. The security tree process involves assigning each staff member a small number of other individuals they are responsible for calling in an emergency event.

**Security risk:** Physical or psychological risks arising from acts of war, violence, crime and other hazards.

**Security risk management:** The attempt to reduce exposure to the most serious risks (including contextual, programmatic and institutional risks) by identifying, monitoring and tackling key risk factors. It also involves balancing risk and opportunity, or one set of risks against another. Risk management should be seen as an enabling process, not simply a precautionary one.

**Security risk management framework:** A set of policies, protocols, plans, mechanisms and responsibilities that supports the reduction of security risks to staff.

**Threat:** Any safety- or security-related or other form of challenge to the organisation, its staff, assets, reputation or programme that exists in the context where the organisation operates.

**Vulnerability:** The organisation's exposure to a threat. It will vary depending on the nature of the organisation, how it works, what programmes it undertakes, the characteristics of its staff, and its ability to manage risks.



# References

(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'. Available from: <https://a4ep.net/?cat=17>

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

Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs*. European Interagency Security Forum (EISF). Retrieved from: <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). Retrieved from: <https://gisf.ngo/resource/crisis-management-of-critical-incidents/>

Charter4Change (n.d.). 'Resources'. Available from: <https://charter4change.org/resources/>

cinfo (n.d.). 'Duty of Care Maturity Model Tool', cinfo. Retrieved from: <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). Retrieved from: <https://gisf.ngo/resource/security-to-go/>

DisasterReady (n.d.): [https://get.disasterready.org/?gclid=Cj0KCQiAgomBBhDXARIsAFNyUqPRVm\\_69sS6omcjFq5CmlpTLNLdpl8ppnlibqLHMfMxaAYe994pikMaAkKaEALw\\_wcB](https://get.disasterready.org/?gclid=Cj0KCQiAgomBBhDXARIsAFNyUqPRVm_69sS6omcjFq5CmlpTLNLdpl8ppnlibqLHMfMxaAYe994pikMaAkKaEALw_wcB)

EISF (2019). *Managing Sexual Violence against Aid Workers: prevention, preparedness, response and aftercare*. European Interagency Security Forum (EISF). Retrieved from: <https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>

EISF and cinfo (2018). *Duty of Care Maturity Model*. EISF and cinfo. Retrieved from: [https://www.cinfo.ch/sites/default/files/matrix\\_web\\_pdf.pdf](https://www.cinfo.ch/sites/default/files/matrix_web_pdf.pdf)

EISF (2018). *Managing the Security of Aid Workers with Diverse Profiles*. European Interagency Security Forum (EISF). Retrieved from: <https://gisf.ngo/resource/managing-the-security-of-aid-workerswith-diverse-profiles/>

Fairbanks, A. (2018). *Duty of Care under Swiss law: How to improve your safety and security risk management processes*. EISF and cinfo. Retrieved from: [https://www.cinfo.ch/sites/default/files/duty\\_of\\_care\\_eisf.pdf](https://www.cinfo.ch/sites/default/files/duty_of_care_eisf.pdf)

Fast, L. and Bennett, C. (2020). *From the ground up: it's about time for local humanitarian action*. Humanitarian Practice Group (HPG). Retrieved from: <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). Retrieved from: <https://ngocoordination.org/system/files/documents/resources/near-localisation-performance-measurement-framework.pdf>

Finucane, C. (2013). *Security Audits*. European Interagency Security Forum (EISF). Retrieved from: <https://gisf.ngo/resource/security-audits/>

Finucane, C. (2013). *The Cost of Security Risk Management for NGOs*. European Interagency Security Forum (EISF). Retrieved from: <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)*. Retrieved from: <https://gisf.ngo/an-open-letter-to-non-governmental-and-donor-organisations-from-the-european-interagency-security-forum/>

GISF (2020). *Partnerships and Security Risk Management: from the local partner's perspective*. Global Interagency Security Forum (GISF). Retrieved from: <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. Retrieved from: <https://static1.squarespace.com/static/58256bc615d5db852592fe40/t/5d93782768d49710fa7a8349/1569945640280/Partnership+conditions+principles+practices.pdf>

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

- Humanitarian Leadership Academic (n.d.). 'Kaya Connect'. Available from: <https://kayaconnect.org/>
- Humanitarian Outcomes (n.d.). 'Aid Worker Security Database'. Available from: <https://aidworkersecurity.org/>
- IFRC (n.d.). 'Learning Platform'. Available from: <https://www.ifrc.org/en/get-involved/learning-education-training/learning-platform1/>
- IFRC (2018). *IFRC Policy Brief: Localization – what it means and how to achieve it*. IFRC. Retrieved from: <https://media.ifrc.org/ifrc/document/ifrc-policy-brief-localization/>
- INSSA (n.d.): <https://inssa.org/>
- Insecurity Insight (n.d.). 'Aid in Danger'. Available from: <http://www.insecurityinsight.org/aidindanger/>
- International NGO Safety Organisation (INSO) (n.d.). 'INSO Key Data Dashboard'. Available from: <https://ngosafety.org/keydata-dashboard/>
- Kemp, E. and Merkelbach, M. (2016). *Duty of Care: a review of the Dennis v. Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF). Retrieved from: <https://gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/>
- McManus, S. and Tennyson, R. (2008). *Talking the Walk: A Communication Manual for Partnership Practitioners*. International Business Leaders Forum on behalf of The Partnering Initiative. Retrieved from: <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). Retrieved from: <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). Retrieved from: <https://gisf.ngo/blogs/developing-a-covid-19-secure-heat-course/>
- Persaud, C. (2012). *Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management*. European Interagency Security Forum (EISF). Retrieved from: <https://gisf.ngo/resource/gender-and-security/>

- Race Forward (2015). *Race Reporting Guide*. Race Forward. Retrieved from: [https://www.raceforward.org/sites/default/files/Race%20Reporting%20Guide%20by%20Race%20Forward\\_V1.1.pdf](https://www.raceforward.org/sites/default/files/Race%20Reporting%20Guide%20by%20Race%20Forward_V1.1.pdf)
- RedR UK, Insecurity Insight and EISF (2017). *Security Incident Information Management Handbook*. Retrieved from: <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). Retrieved from: <https://gisf.ngo/resource/international-agencies-working-with-local-partners/>
- Stoddard, A., Czwarno, M. and Hamsik, L. (2019). *NGOs and Risk: Managing Uncertainty in Local-International Partnerships*. Global Report. Humanitarian Outcomes/Interaction. Retrieved from: <https://www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships>
- Sweeney, A. (2019). 'Reflections on GISF's 'At What Cost?' Campaign', *European Interagency Security Forum (EISF)*. Retrieved from: <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*. Retrieved from: <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. Retrieved from: <https://thepartneringinitiative.org/the-partnering-cycle-and-partnering-principles/>
- UNDSS (n.d.). 'Training'. Available from: <https://training.dss.un.org/>
- van Brabant, K. (2010). *GPR8 – Operational Security Management in Violent Environments, Revised Edition*. Overseas Development Institute (ODI). Retrieved from: <https://odi.hpn.org/resources/operational-security-management-in-violent-environments-revised-edition/>
- Whiting, C. (2016). *NGO Fora Advocacy Guide: Delivering Joint Advocacy*. ICVA. Retrieved from: [https://www.icvanetwork.org/system/files/versions/NGO\\_Fora\\_Advocacy\\_Guide\\_English\\_July2017.pdf](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*. Retrieved from: <https://reliefweb.int/report/world/toolkit-responding-violence-against-humanitarian-action-policy-level>



## Other GISF publications

Available at [www.gisf.ngo](http://www.gisf.ngo)

If you are interested in contributing to upcoming research projects or want to suggest topics for future research, please contact [gisf-research@gisf.ngo](mailto:gisf-research@gisf.ngo).

In 2020, EISF (European Interagency Security Forum) became GISF (Global Interagency Security Forum), reflecting the extension of its network.

You can access all the resources mentioned in this guide on GISF's new website:

[www.gisf.ngo](http://www.gisf.ngo)

### Research papers and reports

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

October 2020

Moutard, L. – GISF

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

October 2018

Fairbanks, A. – cinfo and EISF

#### Managing the Security of Aid Workers with Diverse Profiles

September 2018

Jones, E. et al. – EISF

#### Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management – 2nd edition

December 2016

Vazquez Llorente, R. and Wall, I. (eds.)

#### Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance

August 2014

Hodgson, L. et al. Edited by Vazquez, R.

#### The Future of Humanitarian Security in Fragile Contexts

March 2014

Armstrong, J. Supported by the EISF Secretariat

#### The Cost of Security Risk Management for NGOs

February 2013

Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

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

December 2012

Singh, I. and EISF Secretariat

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

September 2012 – Sp. and Fr. versions available

Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

#### Engaging Private Security Providers: A Guideline for Non-Governmental Organisations

December 2011 – Fr. version available

Glaser, M. Supported by the EISF Secretariat (eds.)

#### Risk Thresholds in Humanitarian Assistance

October 2010

Kingston, M. and Behn O.

#### Abduction Management

May 2010

Buth, P. Supported by the EISF Secretariat (eds.)

#### Crisis Management of Critical Incidents

April 2010

Buth, P. Supported by the EISF Secretariat (eds.)

#### The Information Management Challenge

March 2010

Ayre, R. Supported by the EISF Secretariat (eds.)

#### Joint NGO Safety and Security Training

January 2010

Kingston, M. Supported by the EISF Training Working Group

#### Humanitarian Risk Initiatives: 2009 Index Report

December 2009

Finucane, C. Edited by Kingston, M.

### Articles

#### Managing security-related information: a closer look at incident reporting systems and software

December 2018

de Palacios, G.

#### Digital Security for LGBTQI Aid Workers: Awareness and Response

December 2017

Kumar, M.

#### Demystifying Security Risk Management

February 2017, (in PEAR Insights Magazine) Fairbanks, A.

#### Duty of Care: A Review of the Dennis v Norwegian Refugee Council Ruling and its Implications

September 2016

Kemp, E. and Merkelbach, M. Edited by Fairbanks, A.

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

July 2015, (in Humanitarian Exchange, Issue 64)

Reilly, L. and Vazquez Llorente, R.

#### Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them

March 2012

Van Brabant, K.

#### Managing Aid Agency Security in an Evolving World: The Larger Challenge

December 2010

Van Brabant, K.

**Whose Risk Is it Anyway? Linking Operational Risk Thresholds and Organisational Risk Management**

June 2010 (in *Humanitarian Exchange*, Issue 47)

Behn, O. and Kingston, M.

**Risk Transfer through Hardening Mentalities?**

November 2009

Behn, O. and Kingston, M.

**Guides**

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

October 2020 – Fr. and Sp. versions available Davis, J. et al.

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

March 2019

EISF

**Abduction and Kidnap Risk Management**

November 2017 EISF

**Security Incident Information Management Handbook**

September 2017 Insecurity Insight, RedR UK, EISF

**Security Risk Management: a basic guide for smaller NGOs**

June 2017 Bickley, S.

**Office Opening**

March 2015 – Fr. version available Source8

**Security Audits**

September 2013 – Sp. and Fr. versions available Finucane C. Edited by French, E. and Vazquez Llorente, R. (Sp. and Fr.) – EISF Secretariat

**Managing the Message: Communication and Media Management in a Crisis**

September 2013 – Fr. version available Davidson, S. Edited by French, E. – EISF Secretariat

**Family First: Liaison and Support During a Crisis**

February 2013 – Fr. version available Davidson, S. Edited by French, E. – EISF Secretariat

**Office Closure**

February 2013

Safer Edge. Edited by French, E. and Reilly, L. –

EISF Secretariat



gisf



## **Global Interagency Security Forum**

GISF Executive Director

M: +44 (0) 77 6099 2239

E: [gisf-director@gisf.ngo](mailto:gisf-director@gisf.ngo)

GISF Research Advisor

M: +44 (0) 77 6099 2240

E: [gisf-research@gisf.ngo](mailto:gisf-research@gisf.ngo)

**[www.gisf.ngo](http://www.gisf.ngo)**

First published April 2021