3.5 Security risk management in partnerships

In aid work, it is common for part or all of a programme to be designed and 'owned' by one organisation, but implemented in part or wholly by another. Working with and through other organisations or associations may be more cost-effective, programmatically sound or part of a deliberate strategy, such as to strengthen local capacities or reduce risk. The number of partnerships in the aid sector has increased in recent years, due in part to localisation and decolonisation efforts. This chapter examines equitable partnerships through a security lens. While it acknowledges the diversity of aid sector partnerships, and aims to be broadly applicable, it focuses on partnerships between international organisations and national and local actors.[41]

3.5.1 Principles and strategic considerations

A partnership is any formalised working relationship between two or more organisations to meet agreed objectives. Partnerships in the aid sector can vary in form, length, scope and degree of collaboration; they can be strategic and long-term, or project-based and short-term. They are often bilateral between international organisations and national actors (e.g. local NGOs and community-based groups), but can also be between several organisations (such as through consortia and umbrella grants), and between organisations and private companies, as well as between national NGOs. For some international organisations, implementing through local partners may be their core way of working, while for others it may only be an occasional departure from direct implementation by their own staff.

Partnership agreements or contracts tend to dictate the scope of these types of arrangement, with security responsibilities sometimes marked in agreements as falling under each individual legal entity. In some circumstances, agreements can dictate a cross-over of support, e.g. in the event of a critical incident. In many cases, however, responsibilities are unclear, and cooperation on security risk management is not spelled out, leading to wide variance in how these issues are handled.

[41] Some literature distinguishes between 'national' and 'local' organisations and actors. This GPR uses both terms interchangeably to refer to all types of organisations that operate solely in one country, whether in multiple locations or just one, including community-based groups.

The growing calls for 'localisation' within the aid sector have, unfortunately, not resulted in a commensurate discussion of security risk management and duty of care considerations in international–local partnership arrangements. This is often to the detriment of local actors, who often face the greatest risk of experiencing a severe security incident, but receive the least security support (both within their organisations and from their international partners).[42] Research has also shown that, in international–local partnerships, the risks most discussed and mitigated against are fiduciary, while security risks are often dealt with perfunctorily. While this seems to be changing, challenges remain.[43]

Whether and how partnership arrangements consider security risk management can often be a reflection of:

- how much each partner organisation internally considers and addresses security risks; and
- the circumstances and objectives of the partnership.

Organisations that lack knowledge or capacity, or where robust internal security risk management systems are not in place, may feel unable to have security discussions or extend support beyond their own organisation and staff, or may not have the organisational security culture to even consider doing so. Engagement can also differ within the same organisation due to varying capacities in security risk management across different offices and locations.

The intentionality or purpose of a partnership also affects how the partnership is viewed and managed, with consequences for how partners discuss the risks they face in carrying out their work. For example, research into local–international partnerships has shown that short-term, project-based partnership models are not conducive to security risk management discussions or support.[44]

[42] GISF (2020) *Partnerships and security risk management: from the local partner's perspective* (https://gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/); GISF and Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

[43] Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local–international partnerships (global report)* (https://humanitarianoutcomes.org/publications/ngos-risk2-partnerships); GISF and Humanitarian Outcomes (2024).

[44] GISF (2020).

3.5.2 Challenges

Partners face a number of challenges and obstacles when trying to engage in mutually beneficial security risk management.

Duty of care – legal and ethical considerations

As discussed in Chapter 1.1, ‘Key concepts and principles’, legal duty of care is generally understood to apply solely to an organisation’s own employees, rather than to those of partner organisations. Nevertheless, there exists an ethical duty to support partners in managing security risks and to share pertinent information, knowledge and good practice. Some international organisations are concerned that, by offering such support, they might inadvertently assume legal liability for the staff of their partners. Some security staff have been advised by legal counsel to refrain from engaging with partners on security matters for this reason.[45]

While the extent and nature of legal responsibility can vary significantly depending on the jurisdiction and specific circumstances, these concerns may be exaggerated. As with individuals,[46] an organisation’s legal responsibility towards a partner may depend on the ‘degree of control’ it exerts over the partner’s decision-making processes.

While it is good practice to consider the relevant legal instruments and their implications on security risk management within partnerships, ignoring the issue altogether is an ethical failing that could, potentially, lead to legal consequences. In general, it is beneficial for every organisation that enters into partnerships regularly to establish a policy on what kind of support the organisation will provide or expect from its partners. In addition to making clear where responsibility sits, the support provided to partners on security should aim to remain collaborative, without dictating one particular approach over another, and keep decision-making clearly within each organisation. In this respect, it is important to also be cognisant of how power imbalances and financial incentives can make ‘support and advice’ appear like direction. In some jurisdictions, a legal

[45] GISF and Humanitarian Outcomes (2024).

[46] An organisation’s legal responsibility towards an individual can be relative to the ‘degree of control’ the organisation has over that individual’s circumstances. For example, an organisation that is hosting a visit from a non-employee in a particular country, and that has full control over where the visitor is staying, their travel arrangements and general itinerary, will likely have a de facto legal duty of care to that individual, whether or not a contractual agreement is in place. See Kemp, E. and Merkelbach, M. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications.* EISF (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

entity may be held liable if it were to emerge that an agreement was harmful to one party, even if both agreed to it. This is a particular concern as implementing partners may feel pressured to take on more security risks than they are comfortable with in order to gain contracts. To address this, partners can prioritise building trust with each other and developing strong communication around these issues.

Risk transfer

Sometimes, international NGOs partner with local actors in order to reduce the risks faced by their own staff. Risk transfer, in these circumstances, becomes a component of an operational risk management strategy where an organisation seeks someone else to carry out certain activities in a highly insecure context in order to reduce the risks to their own staff. This classical definition of 'risk transfer' has been the subject of much discussion in recent years and efforts are under way to address the inherent ethical duty of care failings that it can raise – especially where there is no clear assessment that indicates that local organisation staff are at lower risk than international organisation staff.

While it is sometimes easier for local actors to maintain access in volatile environments than international organisations, this should be properly assessed and agreed by both partners. International and local actors may face different risks and challenges in different contexts, including risks that they may transfer or create for each other through the partnership. In fact, by entering into a partnership, organisations automatically transfer risk, both intentionally and unintentionally. For example, in partnering with an international organisation to implement a high-profile programme, a community-based group may experience heightened risk due to the additional attention it can receive, including from local authorities and communities.

With this understanding, risk transfer is best understood as 'the formation or transformation of risks (increasing or decreasing) for one actor, caused by the presence or actions of another'.[47] This can extend beyond international–local partnerships, and includes relationships with donors and other actors, such as community-based organisations.

Good practice encourages partners to reflect on the impact a partnership can have on each other's exposure to particular threats and each organisation's capacity to address the risks before entering into a partnership arrangement.

[47] GISF (2021) *Partnerships and security risk management: a joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Funding gaps

National organisations consistently receive insufficient, sporadic and project-based funding, which makes it difficult for them to develop the back-end systems and inputs needed to manage security risks effectively.[48] In the face of general funding scarcity and an extremely competitive funding environment, partnership budgets can fail to include security-specific budget lines or adequate core costs, while local actors can be incentivised to prioritise programme costs over security-related expenses when entering into partnership arrangements. Local partners may also feel compelled to accept higher levels of risk to secure funding. Knowing this, it is good practice for international organisations to systematically ensure that security funding exists for partners' budgets, either for assessed security costs or as a standard percentage of the overall funding provided.

Communication and trust challenges

There are many obstacles to communicating about security within partnerships, but the primary one is the failure to hold any discussion on security in the first instance. Communication around security issues too often defaults to due diligence checks of implementing partners or as one element of a broader 'capacity-strengthening' package driven by an international partner. Security focal points from both organisations may not be adequately involved in these initial discussions.

Security can be a sensitive topic and implementing actors may be disincentivised to speak honestly about their security challenges and any support needed out of fear of financial and reputational repercussions. Funding partners may fear legal liability if broaching the subject, as discussed above. Security discussions are also prone to challenges owing to a lack of common vocabulary; differences in understandings of security, risk and risk appetite; and power imbalances. Time is required to build and maintain trusting relationships, which short-term and project-based funding can further undermine.

3.5.3 Practical considerations

A strategic and policy-led approach to partnerships makes it easier for organisations to adopt an equitable security risk management approach. This aims to shift security-related conversations within the partnership from one-sided due diligence checks and 'risk transfer' to collaborative discussions on how to 'share risk', directly involving security focal points and relevant programme staff from all partners.

[48] GISF (2020); GISF and Humanitarian Outcomes (2024).

GISF's *Partnerships and security risk management* guide offers a roadmap for implementing this approach, which is summarised in the following sections of this chapter.[49]

Before entering into partnership: a strategic approach and initial discussions

While there are many positive examples of informal collaboration between security focal points in partnerships arrangements, they are often not sustainable in practice. Without a clear strategic approach to why and when an organisation may seek partners, or how it will address security risk management within partnerships, security arrangements can be subject to individual staff members' preferences and biases, with any positive outcomes at risk of being lost when staff change roles.

Organisations that have developed policies around entering into partnership agreements and their responsibilities to their partners, as well as clearly stated security agreements, benefit from more strategic and better-balanced partnership arrangements that are more conducive to constructive security risk management discussions and mutual support. This strategic approach increases the likelihood that both partners benefit from the partnership, and reduces the likelihood of inadvertent and unaddressed risk transfer.

In practice, this includes ensuring that security considerations from focal points are incorporated in the strategic documentation of partnerships and related policies. Initial discussions can be incorporated into due diligence processes. If approached well, these discussions provide an opportunity for partners to collaboratively address concerns about risk transfer, assess security capacity and preparedness, and explore ways to support each other on security-related issues.

Case example: Beyond one-sided due diligence processes

One international NGO has started bringing its local security staff into the identification and contracting processes of local implementing partners. This has enabled the organisation to discuss security issues at the beginning of a partnership, and resulted in security becoming more than a due diligence 'systems review' within the partnership.

[49] GISF (2021).

During this phase, partners should aim to assess how risk is being transferred between organisations and jointly find ways to address any challenges that arise – including identity-related risks stemming from external perceptions of the organisation and its staff. For example, if it emerges that a local community has negative perceptions about certain work an implementing partner is expected to do for its funding partner, the partners can discuss mitigating measures. This could involve reducing the visibility of those programme activities or modifying the project to enhance the security of implementing staff. See Table 3 for some key questions.

Beginning the partnership: agreeing on a security risk management approach

Soon after entering into a partnership or, if feasible and appropriate, before finalising the contract, organisations should aim to agree on how each partner can support the other on security-related issues arising in the partnership and in programme implementation.

GISF's *Partnerships and security risk management* guide provides a list of questions that can support these conversations and offers some ideas on the joint management of security risks between partners. A summary of key questions is in Table 3.

Table 3 Preliminary security risk management questions

Area	Questions
Duty of care	• What are the respective legal and ethical duty of care obligations of each partner? • Are these clearly explained in partnership documentation?
Governance and accountability	• Have both partners contributed to key decision-making opportunities regarding the programme, project, partnership and/or security? • Do both partners have suitable security risk management structures (including roles and responsibilities) in place to enable the partnership objectives to be met? • Does the partnership agreement include mention of security risks and their management? • Can the partners support each other, for example through the recruitment of dedicated security staff?

Area	Questions
Risk transfer	• How is each partner perceived by relevant stakeholders? • Could the organisational identity of one partner impact the other partner? • Does the partnership result in any new threats to either organisation? • Does the partnership change the impact or likelihood of any threat? If yes, is this positive or negative? • When exploring mitigation measures, can one organisation take particular actions to reduce the risk faced by their partner? • In conflict environments, how does the partnership interact with the dynamics of the conflict, and can steps be taken to be more conflict-sensitive?
Policies and principles	• 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 parties agree with each other's position on humanitarian principles and safeguarding)?
Operations and programmes	• What are the security needs and expectations of each partner? • Do the partners have an agreed system in place to identify and monitor security risks faced by staff? • Do partners have security focal points who can speak to each other on security issues? • Do the partners agree on who is responsible for managing identified risks and how these positions should be managed and funded? • Is there a system in place to make both partners aware of security risks and changes in the risk environment (physical and online)? • Does each partner have enough resources (e.g. funding, time and staff) to manage security risks?
Inclusive security risk management approaches	• 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 zones to ensure effective security risk management for all staff?

Area	Questions
Internal threats and safeguarding	● How will the partners manage security threats that may arise from within their own organisations? ● How are safeguarding concerns addressed within the partnership? ● Are appropriate safeguarding reporting mechanisms in place?
Travel	● How should security risks resulting from travel related to the partnership be managed?
Awareness and capacity sharing	● How will partners identify security awareness and capacity-strengthening needs and jointly meet these (both for personal safety and security risk management)? ● Can security staff from one partner provide advice, mentoring and technical support to security focal points in the other organisation, if this is needed? ● Can partner staff access appropriate security training (internal and external to the partner organisations)?
Incident monitoring	● How should the partners share incident information with each other, if at all?
Incident and crisis management	● 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?
Staff care	● Do both partners have access to relevant insurance policies? If not, can either partner support the other in accessing relevant insurance? ● Do both partners have staff care policies and procedures in place, including medical, mental health and post-incident support? ● Can partners support each other with relevant staff care resources and activities (including making changes within the partnership to improve staff wellbeing, such as reducing workloads, flexible work hours and reducing administrative expectations)?
Security collaboration and networks	● Are there platforms in the relevant context that discuss security issues? If yes, do both partners have access and an equal voice in these platforms and networks in their operational areas, including security information-sharing platforms? ● Can access to existing coordination mechanisms be improved for either partner?

Area	Questions
Compliance and effectiveness monitoring	• How should both partners review security risk management measures during the partnership?
Resources	• Have partners shared their respective resources on security risk management with each other? • Can access to existing resources be improved for either partner?
End of the partnership	• 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?

Adapted from GISF (2021) *Partnerships and security risk management: a joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Finally, for a partnership to be equitable, it is crucial that both parties have a clear understanding of each other's attitudes to and tolerance of risk. Partners benefit from openly discussing each other's risk appetites and finding ways to align where there are strong differences – which can be quite stark in many of the contexts in which humanitarian programmes are carried out. Each partner's attitude towards risk should ideally be discussed at the beginning of a partnership and regularly revisited throughout the life of the partnership (which could match the schedule of partnership milestones). In some instances, it may be that agreement on risk thresholds cannot be reached or risks appropriately mitigated, and this can inform more strategic discussions on whether the partnership should go ahead or programmatic work should be modified.

▶ *See Chapter 1.1 for more on risk thresholds and programme criticality.*

During partnerships: identifying and addressing needs, gaps and challenges

Strengthening communication and operationalising principles

Proactive efforts can be made to improve communication between partners. This can mean ensuring that the right people are in the communication chain (which should typically include the designated security focal points of each partner); that the frequency and method of communication is the most appropriate and convenient for both partners; that communication is transparent, honest and clear; and that staff adhere to key principles that aim to address and overcome inherent biases and build trust.

Partnership principles

In order to make partnerships more equitable, effective and secure, staff working on establishing and maintaining partnerships can consider some basic good practice principles:

- Equity – partners have equal rights, regardless of any power imbalances.
- Transparency – there is open and honest interaction between partners.
- Mutual benefit – both partners should benefit from the partnership, ideally beyond simply meeting the partnership objectives.
- Complementarity – partners each bring their own strengths and weaknesses to a partnership, complement each other and recognise that diversity can be an asset.
- Results-oriented – actions expected from partners should be realistic and focused on results.
- Responsibility – partners should take responsibility for their actions and avoid overcommitting or overpromising.

Source: GISF (2021) *Partnerships and security risk management: A joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Case example: Risk sharing in practice

A local Nigerian NGO approached its two international NGO partners for funding for the recruitment of a security officer. In addition to agreeing to provide funding for two new security roles in the local NGO, the international partners' security staff supported the recruitment process and provided the new recruits with inductions, bi-weekly support and monthly catch-up meetings. When discussing the benefits and challenges, international NGO security staff involved in the process agreed that buy-in from all partners was essential and ensured that ownership over security roles and decisions remained with each organisation. They agreed that, to share risk effectively, a key challenge is ensuring that international NGO security staff have the capacity to build relationships and provide the appropriate level of mentoring to local NGO security focal points.

Source: Christian Blind Mission (CBM) and Sight Savers International (SSI) (2022) *Sharing risk – a good practice example in the INGO sector* (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

Joint risk assessments and adapted security plans

Although still uncommon within the aid sector, joint risk assessments of programme activities provide both partners with a clear picture of the likely risks, and allow the implementing partner (and its staff) to voice concerns before carrying out the work. A joint risk assessment also allows for greater discussion on possible mitigation measures and ways in which each partner can support the other in meeting security needs and programmatic objectives. This process allows for clearer discussions around risk ownership and responsibilities within the partnership, as well as setting clear expectations from the start about what each organisation can bring to the partnership. A joint periodic review of the evolving risk picture is also advisable. The exercise can be an opportunity for partners to benefit from exposure to each other's perspectives and helps identify where adaptions may need to be made. For example, this could include reconciling one organisation's emphasis on documentation and written policies with another's reliance on verbal communication.

Depending on the circumstances, this joint risk assessment can culminate in shared security protocols. At the very least, these risk assessments should aim to inform each organisation's security plans and procedures. Regular communication between partners can help in addressing security concerns promptly.

Partners should be prepared for crises and critical incidents and ideally agree in advance the best way to manage them. Partners can consider which organisation would be best placed to respond in the event of a crisis or critical incident (e.g. logistics, access and expertise). Any support provided in these circumstances will usually need to be decided at a strategic level considering relevant legal and financial implications. However, being risk averse in this regard may not necessarily be the best option, as the reputational cost of not providing support during such an event (where an intervention would be beneficial and not cause more harm than good) may be more damaging than the possibility of legal liability. One international organisation that has recognised this has taken proactive steps to support their local partners with obtaining relevant insurance – something that can be very challenging for local organisations to obtain on their own.

Case example: Security risk management in partnerships

One international organisation has implemented several initiatives to better address security risk management issues and needs when working with partners. These include:

- Increasing the involvement of security staff in engagement with partners from the earliest discussions.
- Raising awareness among security staff of what partnership means and how to work together for common outcomes in a safe way.
- Creating (and sometimes co-creating) and sharing guidance, including tools.
- Offering a training 'menu' to partners.
- Increasing the number of partner staff in the organisation's own security training sessions.
- Supporting partners in managing incidents (in the form of technical advice).

Capacity sharing

Partners bring their own knowledge and strengths to a partnership and a discussion of these, as well as weaknesses and gaps, can lay the foundations of a stronger and mutually beneficial arrangement. Differences in approach should not be considered a lack of capacity. Partners should aim to agree on what is most needed in terms of support, for instance security training, and which formats work best. One international organisation created an online website that its partners can access for training on particular topics, including security-related content. Other organisations have promoted online platforms and training with their partners. Some international organisations have developed specific security training for their local partners, while others invite them to participate in the training they provide their own staff. It is important that all capacity-strengthening is relevant and beneficial to each partner, jointly agreed as needed, and sustainable so that it can support the long-term capacity of staff and organisations.

▶ *See Chapter 5.2 for more information on security training.*

Funding

Partners should aim to discuss security costs as early as possible, including the funding needed to strengthen back-end security systems. Partnership budgets should aim to contain security-related budget lines as a rule, while partners can ensure alignment of security cost requirements with assessed security risks. Longer-term funding needs should also be considered and discussed within the partnership, such as funding for training and medical and malicious act insurance coverage for staff most at risk. International partners can advocate with donors for adequate funding for their implementing partners, while donors themselves can demand greater consideration of the security needs of downstream partners.

▶ *See Chapter 3.3 for more information on funding security.*

Resource sharing

Partners benefit from proactively sharing security risk management resources and information within a partnership. Implementing partners may have greater insight into local security conditions, which they can share, while international partners may have greater access to coordination and information-sharing mechanisms, which they can facilitate access to. While this is often done informally, security resources should ideally be shared actively and regularly, be available online and offline (in a variety of formats where possible) and translated into relevant languages. Partners can support each other in engaging in security networks and information-sharing forums at local, national, regional and international levels.

Case example: Security coordination mechanisms

Local actors are significantly under-represented in coordination mechanisms led by international aid actors. Often, local actors are unfamiliar with the mechanisms or do not participate due to obstacles such as location and language. Organisations like INSO are taking steps to address this, offering membership to national registered NGOs and thereby allowing these actors free access to networking, information sharing and training. However, unregistered local humanitarian actors still face significant challenges in joining networks.

Advocacy and partnerships

Partnerships present opportunities as well as risks when it comes to advocacy. Common advocacy efforts between partners can result in an amplified voice, which can be useful for advocacy around security risk management (e.g. international partners advocating with donor governments for greater security funding for local actors). However, advocacy by one organisation can present security risks for its partners, for instance where a local government holds local partners in the country responsible for an international partner's advocacy efforts towards it. It is good practice to consider the impact that advocacy efforts can have outside the organisation, especially on partners, before moving forward. One international organisation in Myanmar has actively discussed advocacy messages with its implementing partners before going ahead in order to ensure that its partners are not only aware but also can discuss the possible consequences of the advocacy and any mitigation measures needed.

▶ *To learn more, see Chapter 2.2 on advocacy and security.*

Further information

Research and discussion

CBM and SSI (2022) *Sharing risk – a good practice example in the INGO sector* (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

EISF (2012) *Security management and capacity development: international agencies working with local partners* (https://gisfprod.wpengine.com/resource/international-agencies-working-with-local-partners/).

GISF (2020) *Partnerships and security risk management: from the local partner's perspective* (www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/).

GISF and Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local-International partnerships (global report)* (www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships).

Kemp, E. and Merkelbach, M. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications.* EISF (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

Guidance and resources

GISF (2021) *Partnerships and Security Risk Management: a joint action guide for local and international aid organisations* (www.gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Global Database of Humanitarian Organisations (GDHO) (n.d.) (https://humanitarianoutcomes.org/projects/gdho).