Addressing Gaps in Institutional Donor Policies on Safety and Security

NGO Perspectives on Meaningful Reform

Unpublished Working Draft - February 2025

Introduction

Despite recent commitments by member states on the protection of aid workers, the risks faced by those serving the world's most vulnerable populations continue to grow. 2024 became the deadliest year on record for aid workers, with 378 fatalities among nearly 700 victims (killed, injured, or kidnapped).[1] Rising threats – including indiscriminate bombing, targeted attacks, and restrictions on access – make security risk management (SRM) an increasingly vital component of humanitarian action.

Yet, support provided to NGOs to manage these risks through robust SRM has not kept pace. In 2019, GISF (then the European Interagency Security Forum, EISF) launched the **'At What Cost?' campaign**, which highlighted outdated funding structures for safety and security in the aid sector. Backed by 188 stakeholders across 38 countries, and reviewed by the UK Parliament's International Development Committee, the campaign led to a significant policy shift: DFID (now the FCDO) introduced a dedicated SRM budget line in its Rapid Response Facility template, setting a precedent for enabling policy changes.[2]

However, five years on, these improvements remain isolated. Scaling reforms across government donors and diverse operational contexts has proven challenging, leaving gaps in how SRM is prioritised and funded. This report examines these persistent gaps and provides actionable insights to strengthen donor engagement with SRM. Based on a survey[3] with 68 NGO participants—including safety and security staff, grant/business development staff, and programme managers from GISF member organisations—it offers a snapshot of the sector's current landscape and identifies opportunities for improving SRM funding and implementation.

Security risk management (SRM) enables organisations to identify, assess, and mitigate risks, ensuring safe access to crisis-affected populations, while ensuring duty of care. Effective SRM integrates security into programme planning, travel, incident response, and partnerships, and staff capacity-building, fostering practical, context-specific approaches.

[1] Data from the Aid Worker Security Database (AWSD): https://www.aidworkersecurity.org/

[2] Read more about the 'At What Cost?' campaign.

[3] This survey was conducted between 11 December 2024 and 17 January 2025. The survey is part of a broader GISF study reviewing institutional donors' grant terms, conditions, and contracts. The study seeks to examine: (1) Experiences with donor policies regarding safety and security; (2) Budgeting for safety and security in grant proposals; (3) Donor approaches to partner inclusion in security planning; (4) Recommendations for institutional donors to improve support. Survey questions available on request.

Key challenges and barriers faced by NGOs

1. Inconsistent and restrictive donor guidance and budgeting guidelines

Funding for SRM remains highly inconsistent across government donors, creating major obstacles for NGOs seeking to integrate security into programme design and adequately fund risk mitigation measures. While some donors (e.g. FCDO, ECHO) were noted by NGOs to have taken steps to improve guidance on incorporating SRM funding, the most donors lack any guidance or even specific reference to security.

- **Only 18% of respondents reported that safety and security measures are consistently included in donor requirements**.
- 43% said they are occasionally referenced, and 27% noted they are rarely or never mentioned.
- **Over half (54%) of respondents stated that donors do not provide clear instructions** on presenting safety and security in grant budgets.

The lack of clarity leaves NGOs to navigate a patchwork of inconsistent guidance, varying donor expectations, and unclear budgeting requirements. Where security is referenced, some donors request detailed justifications on security-related costs. Common requirements include:

- Security plans tied to project activities and geographic contexts
- Detailed risk assessments or threat analyses
- Cost breakdowns for security and safety measures.

However, NGOs note that providing justification is not always straightforward. Some donors request justifications at the proposal stage which can be difficult to meet without adequate guidance on allowable costs, while others request justifications at the audit stage, rather than engaging with organisations during the proposal process to ensure SRM is appropriately resourced. This disconnect creates additional administrative burden and uncertainty for organisations in the budgeting process:

> "Donors are very demanding on risk analysis but don't provide guidance about the means to finance it."
>
> "Some [donors] ask for justifications or breakdowns of costs that are hard to provide in the design phase of a project."
>
> "Specific SRM budget and expense justifications are usually demanded [by donors] later, at the audit stage, rather than supported during the proposal phase."

Restrictions and conditions for security costs

Even when security costs are acknowledged, they are often subject to restrictive conditions which limits NGOs' ability to allocate adequate funding for SRM. Common challenges include:

- Budget ceilings that cap allowable security expenses irrespective of the operational context.
- Restrictions on categorising SRM as a direct cost, forcing NGOs to absorb costs into general overhead or administrative budgets.
- Vague cost categories that make it difficult to allocate SRM funding transparently.

Many respondents expressed frustration with these limitations that obscure the true cost of delivering aid safely and fail to reflect the realities of high-risk environments. Operating in highly insecure contexts costs more, and arbitrary percentages of total programme budgets fail to account for the

distinct contexts, programmes, and organisational models in each operation. When donors and NGOs treat SRM as a general administrative cost rather than a critical enabling function within budgets, they risk the safe and sustainable delivery of aid and programme continuity.

> "Budget ceilings make it difficult to allocate sufficient resources for safety and security, especially in high-risk environments where costs are inherently higher."
>
> "We are often requested [by donors] to share security plans and reassurances that we can remotely manage any security challenges. But no costs can be budgeted for security without creating a burden on already challenging ceilings for management costs and without reducing the budget available for activities."

2. Barriers to partner inclusion

Many respondents emphasised the heightened security risks faced by local and national partners, particularly those operating in frontline, high-risk areas. These partners often lack the resources or capacity to implement robust SRM measures, leaving them disproportionately exposed. One respondent highlighted:

> "Donors should understand that partner organisations face unique risks that cannot be addressed with a one-size-fits-all approach."

While INGOs often act as intermediaries in transferring funds to national and local NGOs, **60% of INGO respondents face challenges in allocating security resources to their local and national partners due to donor restrictions or conditions.**

The most cited barriers included lack of donor clarity on allowable expenses (23%) and insufficient recognition of partner-specific SRM needs (21%) (Figure). Respondents noted that complex compliance requirements for partner-related SRM funding can make it difficult to channel resources effectively.

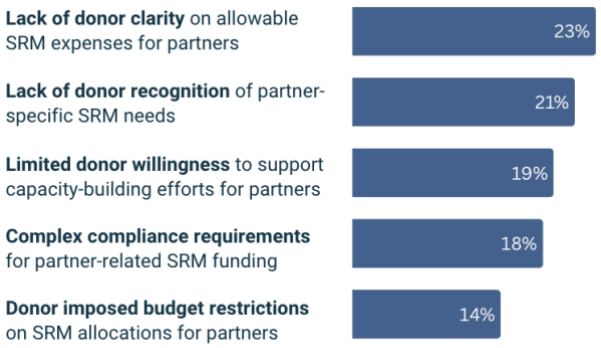

Figure. Challenges faced in allocating SRM resources to local and national partners

3. Donor expertise on safety and security

Donors' perceived lack of expertise and understanding of SRM and its operational realities was highlighted as a key contributing factor to the restrictive funding structures. Many described donors taking a "tick-box" approach to SRM, and *"looking for compliance with their needs, rather than asking for set-ups that actually improve security in complex conflict areas."*

Several noted that donor teams managing grants often lack the operational experience or contextual understanding needed to effectively assess or support SRM needs. While some larger donor agencies may have security teams and highly skilled security practitioners, they are not always connected with the desks that manage grants and engage with implementing partners. Many also pointed out that this gap in expertise leads to unrealistic expectations and approaches that are disconnected from field realities. One respondent noted:

> *"*Those in charge often have little or no experience in such environments and come with very technocratic solutions—**at times it's even dangerous**."
>
> "Donors should understand that for certain programmes, work is going to be more expensive because the security setup is going to be proportional to the level of insecurity."

Several respondents pointed out that donors rarely engage directly with local partners on SRM issues. This lack of engagement often results in mismatched priorities and an incomplete understanding of partner-specific risks. NGOs noted a greater need for donor staff to participate in inception conversations to develop a common understanding on risk exposure of national and international staff.

Respondents described significant variability in expertise and engagement, not only between donors but also within individual donor agencies. This inconsistency creates challenges for NGOs trying to navigate donor expectations and secure meaningful support for SRM. One participant observed:

> "There is no universal standard even within donor organisations. I have worked with some donor teams who were helpful, engaged and focused on the issue for a specific project, but that same organisation then showing no interest or meaningful engagement on another."

Donors' lack of expertise in SRM often limits their ability to collaborate effectively with security professionals and coordination bodies. Many respondents called for donors to engage with NGOs and networks to build their understanding of operational realities and improve their funding frameworks.

4. Impact on funding and implementation

The consequences of inconsistent guidance, restrictive conditions, and the perceived lack of understanding of SRM costs and operational realities has resulted in critical gaps in security funding across the NGO sector:

- **70% of respondents reported encountering situations where their organisations were forced to initiate projects with insufficient SRM measures in place** due to donor restrictions limiting adequate funding.
- The most frequently cited restrictions were donor-imposed budget ceilings, restrictions on categorising SRM as direct costs, and unclear donor guidelines on allowable security expenses.

These funding constraints have direct implications on aid operations, compromising staff safety, programme continuity, and the sustainability of humanitarian action in high-risk contexts. They place additional strain on NGOs, many of whom are operating in settings where violations of IHL are rampant and heightening aid worker exposure to the most resource-intensive and complex risks, including explosive weapons, remote violence, and systemic detention.[4]

The inability to allocate sufficient resources for essential SRM measures forces NGOs to confront challenging dilemmas, whether prioritising programme delivery at the expense of staff safety and sustainability; diverting unrestricted funds from other critical areas and reducing programme flexibility; or relying on ad hoc funding sources and creating inconsistent security measures across different programmes.

[4] ACLED (2024). Conflict Index: December 2024, Global conflicts double over the past five years; Insecurity Insight. (2025). Hovering Threats: The challenges of armed drones in humanitarian contexts.

Restrictive donor policies have a stark impact on local and national NGOs, who often bear the highest security risks operating at the frontlines of crises. A 2024 global survey of more than 700 frontline workers highlights the extent of these challenges: [5]

- More than a quarter of frontline staff face serious safety and security threats on a daily basis.
- Fewer than 50% of staff in local and national NGOs have access to security plans, infrastructure, or risk monitoring resources.

Key recommendations to donors

1. Flexibility and clarity in guidelines and budgeting

- Categorise SRM as a direct programmatic cost rather than an administrative expense, ensuring resources can be allocated based on operational realities.
- Provide flexibility in budgeting to accommodate the dynamic nature of high-risk environments, such as allowing lump-sum allocations that can be adjusted as risks evolve.
- Move away from one-size-fits-all approaches and recognise the unique risks and operational realities of different contexts and organisations.
- Establish clear and standardised guidelines on SRM requirements.
- Include specific instructions in funding calls on how to present SRM costs, including the requirement for safety and security plans, budget allocations, and clear explanations of allowable costs.

2. Improve supportive funding practices for local and national partners

- Streamline compliance requirements to make SRM funding more accessible to partner organisations.
- Allow flexibility in channelling funds directly to local partners or through INGOs to cover security costs.
- Prioritise capacity-building initiatives for local and national partners to strengthen their ability to manage unique security risks.

3. Strengthen donor expertise and engagement on safety and security

- Develop internal donor capacity by providing staff with training on SRM and strengthen links between donors' grant-making functions and existing security knowledge and expertise.
- Increase direct collaboration with NGOs, security professionals, and security networks like GISF to enhance understanding of SRM challenges and best practices.
- Encourage active engagement with implementing organisations to build partnerships that improve funding models and address practical SRM needs.

4. Adopt and scale successful models

- Expand the use of proven models, such as the UK's Rapid Response Facility budget template[6], across donors' funding instruments.
- Integrate SRM into all aspects of programme planning, including requirements for security plans and specific budget allocations for safety and security.
- Standardise SRM practices across donors to ensure consistency and equity in how SRM is incorporated into funding frameworks.

[5] Greenway, L. Joshi, N., Jha, R., Ahimbisibwe, L., & Tanner, L. (2024). Research study: The status of frontline humanitarian workers. Humanitarian Aid International.

[6] Annex B. Budget template: https://www.gov.uk/guidance/humanitarian-response-funding

Conclusion

Donors play a critical role in ensuring the safety and security of aid workers. Small but significant changes—such as recognising SRM as a direct programmatic cost, providing clear and consistent guidelines, and adopting flexible budgeting frameworks—can greatly enhance the availability and effectiveness of resources for security. By engaging more deeply with implementing organisations to co-develop practical solutions that reflect the rapidly evolving and increasingly complex humanitarian landscape, donors can help protect aid workers and enable the sustainable delivery of life-saving assistance to those in need.

About GISF

The Global Interagency Security Forum (GISF) is a member-led NGO forum that works to strengthen the safety and security of aid workers globally. GISF achieves this by shaping global policy, driving collaboration among key stakeholders, and providing practical tools and resources that empower humanitarian organisations to effectively manage security risks. With a focus on supporting both international and local NGOs, GISF bridges the gap between operational realities and high-level policy discussions, ensuring aid workers can deliver life-saving assistance in even the most challenging environments.