# State of Practice: The Evolution of Security Risk Management in the Humanitarian Space

Humanitarian Outcomes | gisf

As a subject of humanitarian policy and practice, security risk management (SRM) has been an active and growing – yet largely understudied – area of operations. Only a small number of comprehensive, sector-wide analyses of SRM have been published over the past two decades, and none of them are recent enough to cover the significant developments of the past several years. This report discusses current capacities, issues, dilemmas, and challenges in humanitarian SRM, presenting them within the context of a sector that is continually adapting to meet needs in the face of evolving threats.

The research found that humanitarian organisations, individually and in coordination, have made significant advances in systematically enhancing the safety and security of their staff with proactive measures, leaving less to the realm of chance and intuition. While the institutionalisation of methods can go too far or be misapplied, overall, humanitarians have made progress in a challenging area that often deals with life-and-death stakes and the knowledge that risk can only be reduced – never eliminated.

Ultimately, the success or failure of SRM is not measured in the number of staff trained or procedures implemented, or even in security incidents encountered, but rather in how well the measures enabled effective humanitarian response to people in crisis.

The research project drew its findings from key informant interviews, an online survey, and country-based research in Colombia, Central African Republic, Ukraine, Iraq, and Ethiopia.

## Key findings

- Development of SRM systems and capacities has been significant but skewed
- New threats and shifting security conditions challenge humanitarian access and adaptability
- Deep disparity: Local and national organisations are unable to develop SRM within current partnership models
- Significant progress in SRM coordination, inputs, and training – and a need to expand their reach
- Challenges in access and cooperation with armed actors
- Individualising security: Steps made towards the person-centred approach in SRM

**These key findings are discussed in further detail in this summary brief.**

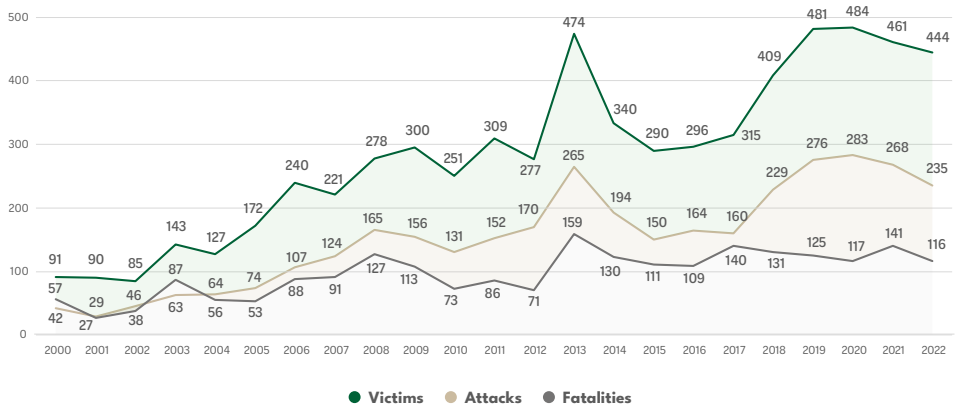
# Insecurity for aid workers

## Trends in casualty data

Humanitarian aid workers in conflict areas are more likely to die from violence than any other job-related cause. While the biggest risks are concentrated in a relatively small proportion of response settings, the toll remains alarmingly high.

Over 20 years of data on security incidents shows a long-term increase in the number of major violent attacks and victims, reflecting both the expanding international humanitarian sector and the proliferation and intensification of conflicts, where most humanitarian aid work takes place.

**Figure 1:** Major attacks affecting aid workers and total numbers of victims and fatalities by year, 2000-2022




## Emerging threats and changing security landscapes

While insecurity is highly context-specific and does not follow global trends, humanitarian security professionals have noticed some general shifts, borne out by global incident data, that influence their current work and priorities.

| | |
|---|---|
| **Complex threat environments** | The increasing complexity of operational environments (conflicts and unstable settings, marked by weak or absent rule of law and multiple armed actors) is straining aid organisations' capacity to measure and manage risks. |
| **Digital risks** | The rise in digital risks, including mis/disinformation, cybercrime, and the phenomenon of globalised risk, is a growing cause for concern, with examples of hostility online quickly morphing into real-life threats. |
| **Crime and criminal economies** | Crime was one of the most prevalent threats reported by security staff interviewed at all levels, with humanitarians also grappling with the challenge of engaging with criminal actors who control access to places and populations. |
| **Collateral violence in major wars** | In recent years, humanitarian efforts have faced an escalating risk stemming from major warfare and associated collateral violence. |
| **The Wagner Group's presence in Africa** | International actors, like Wagner Group, are having a significant impact on the operational environment in which humanitarians work, with both improvements and challenges in security dynamics. |
| **Mixed extremes and transitional contexts** | Across the countries studied, organisations struggle to adapt to changing security and crisis conditions, whether deteriorating or improving. |

# The development of security risk management in humanitarian action

The humanitarian sector has made substantial advances in building SRM systems and capacities, especially in the past 10 years, including a shift away from reactive and restrictive security measures to active, 'enabling' risk management. This impressive progress has been lopsided, however, mainly benefiting international actors.

## The current state of SRM structures and capacities

Virtually every international aid organisation consulted had well-developed security risk management systems. This stands in contrast to local/national organisations, where SRM capacities are still under-supported and underdeveloped.

Priorities for improvement for both international and national/local organisations were:

- **Staff capacity in SRM**
- **Risk assessment**
- **Contingency planning and development**

Within international organisations, discrepancies continue to exist between what SRM support is provided to staff. International staff were more likely to receive SRM support – including security briefings, training, medical insurance, life insurance and post-incident care – than their national colleagues.

## Risk assessment and analysis

Assessing risks is a cornerstone of SRM and among the top SRM priorities for consulted organisations. Security risk assessments are now an increasingly standardised process in the sector. The research, however, uncovered three prominent issues worthy of further discussion:

**Do formalised risk assessments narrow the field of vision?**

Risk assessments that focus on the most likely risks may neglect to consider risks that, while remote, will have a major impact.

**Reliance on outsourced analysis**

There is a trend towards greater reliance on outsourced risk analysis, which may not always be fit for purpose.

**Siloisation of risk assessment processes**

Many organisations still treat security risk assessments as an isolated activity that only security focal points feed into.

## Funding for security

Disparities among different aid actors remain with regard to funding for SRM.

**International organisations**

Donors are receptive to funding security-related costs, particularly in high-risk contexts.

Within organisations, however, SRM is sometimes not introduced into the programme planning phase early enough, and security costs risk being cut from budgets.

**Local and national organisations**

Insufficient and sporadic (project-based) funding for security means a lack of the inputs needed to develop and implement SRM.

International actors' requirements and funding scarcity incentivise local/national NGOs to prioritise programmatic and administrative spending.

**Donors**

Major humanitarian funding agencies have improved in their ability and willingness to support SRM and facilitate flexible budgeting.

By not directly funding local actors, donors play a big part in the inability of local/national NGOs to resource their SRM needs.

# Local actors and national-international partnerships

Despite the international community's stated aims for localisation, the relative level of SRM development suggests that local/national organisations are about 20 years behind their international counterparts in terms of security systems. The discrepancy is especially problematic since local actors are assuming more of the risk as frontline providers.

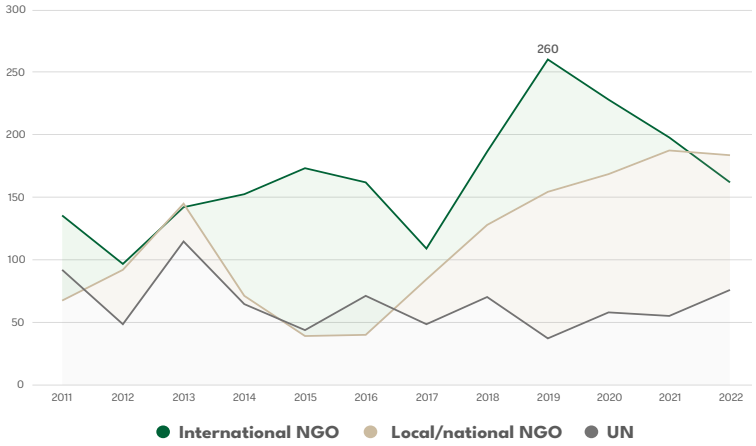
## Local actors are at greatest risk with the least security support

The number of casualties experienced by national and local organisations has increased steadily over the past seven years and, in 2022, surpassed that of international NGOs (whose own casualty numbers have declined since 2019).

Virtually every national organisation we spoke to had a very keen sense of the risks it was running and the value of SRM staff and institutional capacities, but simply could not afford them. A pervasive and stubborn funding model prevents them from building core organisational capacities.

In most partnerships, collaboration on SRM is neither close nor comprehensive and often is limited to a superficial one-sided review of SRM systems and the designation of a security focal point.

**Figure 2:** Number of aid worker victims by type of organisation, 2011–2022




## Is liability risk preventing collaboration on security?

Security professionals in international organisations generally agree that, whether or not there is a formal legal responsibility toward the staff of their partner organisations, there is an ethical or moral duty of care. However, there is a growing concern that if any formal duty of care relationship is acknowledged or implied, an international partner could be liable for any harm that may come to local partners.

**Ethical duty of care**

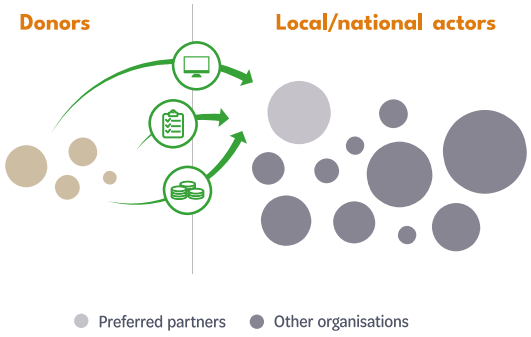
- Confusion and uncertainty for international organisation security staff on how to support partners in practice.
- Ad hoc security engagement between partners at operational levels.

**Fear of liability**

- Leadership teams directing operational teams to not collaborate more closely with local partners on security.
- Keeping partners at arm's length - transfer of risk without mitigation capacity.
- Failure to capitalise on the comparative advantages of the partnership.

## Overlapping and uncoordinated partnership arrangements

A small number of well-established and capable local/national NGOs (often the only local actors that have SRM systems already in place) tend to become the preferred partners of multiple international agencies. This results in these local/national NGOs being forced to juggle multiple, uncoordinated due diligence requirements and SRM workstreams set by their international partners.



# Security coordination

While some critical gaps remain, SRM coordination at both the global and local levels has increased and become more systematised, and its value is seldom questioned.

## Informal coordination

The rise of digital communication platforms has been both a boon and a risk to security coordination. Social media and messaging apps have allowed humanitarian security staff to receive and relay nearly instantaneous information, and to curate a variety of information sources and contacts to suit their purposes. These digital tools, however, also carry risks of:


## The coordination coverage gap

According to the gaps and needs expressed by study participants, the biggest challenge for SRM coordination in the humanitarian space would seem to be achieving it at the necessary scale. Local/national NGOs are underrepresented in many of the existing coordination mechanisms that are designed and led by international actors. In major crises, the humanitarian actors, particularly at the local level, can be so numerous and disparate that no single internationally-led mechanism can cover and serve them all. There is an evident need for supporting additional, context-specific local coordination platforms that could link to the international coordination bodies.

## Formal coordination

The following are some of the major mechanisms through which formal coordination on humanitarian SRM is taking place.

### UNSMS

- UN agencies are coordinated under UNSMS.
- UNDSS was created to support and coordinate the SRM of various UN organisations.

### INSO

- INSO is the main SRM coordination mechanism at the country level.
- In the countries where it has presence, INSO serves as one of the primary links between NGOs and the UN on security matters.
- Its proponents far outnumber its detractors, but the research team heard some repeated criticisms of the platform.

### GISF

- GISF is a platform for global-level dialogue and collaboration, guidance, original research, and practical tools and templates on SRM.
- While GISF membership is restricted to organisations operating in more than one country, research outputs and some events are open to all actors.

### SAVING LIVES TOGETHER (SLT)

- SLT is a framework for how the UN and NGOs can collaborate on security and foster greater coordination.
- The objectives and functions of SLT remain widely misunderstood, and a lack of common understanding has resulted in SLT being a frequent source of frustration for both UN and international NGO staff.

### PLSOs

- Operating at the country level, PLSOs are funded by USAID to support the operational security of its implementing partners.
- PLSOs have had a mixed reception from some humanitarian NGOs.

### INSSA

- INSSA is a platform that focuses on technical SRM skills development for individuals and accreditation standards for humanitarian SRM professionals.

# Advancements in SRM inputs

The research shows that there has been immense progress in the development of tools, standard operating procedures, and training resources over the past decade, particularly within international organisations.

## Incident monitoring

Security incident monitoring has become much more widespread in the last decade, as indicated by 72% of survey respondents reporting having a global incident reporting system in place in their organisation, including most of the local/national NGO respondents. Despite the clear advancements in this area, interviewees identified three main challenges:

**Lack of systematic recording of incidents affecting implementing partners and contractors.**

**A need to improve the quality of reporting.**

**Underreporting of incidents.**

## Staff care and mental health support

The research team recorded many different examples of mental health and wellbeing risks but found few examples of commensurate mitigation systems. Staff care and mental health support is, however, an acknowledged area of concern that different organisations are increasingly exploring how best to address.

## Training

The past decade has also seen significant advancements in security training in the aid sector, both in terms of personal safety and security courses for general aid workers, as well as SRM training and skills development for security professionals. Following the lockdowns brought about by the COVID-19 pandemic, there has also been an explosion of online courses on security. However, the following challenges remain:

**Disparities**
Local/national staff are much less likely to receive personal safety and security training, especially if they work for a local organisation.

**Access**
Lack of locally accessible and language-appropriate security training.

**Effectiveness**
Widespread absence of hard evidence on the effectiveness of different types of personal security training.

**Sustainability**
Concerns that HEAT courses have come to be seen as the gold standard in security training, while not being financially or logistically accessible to those most at risk.

**Quality**
Wide variance between good quality and context-appropriate HEAT courses (in-house and external) and lesser quality, more opportunistic courses.

**Relevance**
Tendency towards "cookiecutter" course design, which lacks tailoring towards specific contexts, programmes, organisations, and individuals.

Many of these challenges are not new or surprising, and a number of training providers and international organisations indicated efforts towards addressing some of these concerns.

# Humanitarian access challenges and the role of SRM

## Limited international footprint

In some conflict environments, such as Myanmar, Syria, Ukraine, and Yemen, international organisations have effectively abdicated their presence to local/national organisations and informal groups in large parts of the country due to insecurity. In these and other contexts, humanitarian access has been severely constrained by security threats, often compounded – or even exceeded – by governmental constraints. This has created significant challenges in reaching affected people, leaving many areas inaccessible to international organisations. Our research team found that in Ukraine, aid operations witnessed the emergence of a two-tiered system of humanitarian security culture:


## Civil-military and deconfliction challenges

Deconfliction – the process of coordinating with military actors to avoid harm to humanitarian operations and civilians – is a critical activity in conflict zones. Despite serious, concerted efforts to build mechanisms like the Humanitarian Notification System for Deconfliction (HNS4D), trust remains low, and participation is far from universal, due to the perception among many NGO staffers that to do so creates more danger than it mitigates.

In addition, the weaknesses in coordinating mechanisms supporting dialogue between humanitarian and military actors in conflict contexts (civil-military coordination) have also contributed to overall coordination challenges for NGOs. UN Humanitarian Civil-Military Coordination (UN-CMCoord), led by OCHA, struggles with a lack of resources and sometimes a disconnect between official civil-military guidance and on-the-ground realities. There is limited attention to how SRM for aid workers fits into the discussions, and in some contexts a lack of clarity as to which UN body – OCHA or UNDSS – the NGOs should coordinate with on these issues.

## Collective access initiatives and the missing link with SRM

OCHA serves as the focal point for humanitarian access and in recent years has sought to formalise and strengthen this role, providing a 'minimum package of services on access', including leading country-based collaborative efforts on advocacy, practical tactics, and negotiations in humanitarian access groups. These efforts are largely valued by humanitarian actors, who give particular praise for OCHA's leadership in this area of work in some settings, notably Haiti and Ukraine.

However, these access working groups do not exist in all contexts, and where they do, the research found a lack of engagement with SRM personnel. This divide between SRM and access activities is sometimes mirrored in individual organisations, where there can be tension rather than cooperation between SRM teams and programme personnel working on access initiatives. Better integration between SRM strategies and work on access could improve both.

## Access and acceptance

Another way of looking at access is as a series of efforts toward – and ultimately a measure of – acceptance. NGOs that have had a longstanding presence in a community all credit their integration in the area and the trust built up with communities and authorities over time as the key to their continued access in challenging locations. For many, acceptance continues to be a primary focus of their SRM approach. But in some conflict environments, where one or more of the belligerents do not consider the humanitarian organisations as neutral actors and will not accord humanitarian staff their protected status under international humanitarian law, acceptance strategies are insufficient to gain secure access. A broader discussion currently taking place in the humanitarian sector concerns whether solidarity-based approaches with oppressed populations are more appropriate in contexts like Myanmar and Ukraine, rather than acceptance based on the humanitarian principles of neutrality and impartiality.

# SRM and the individual

Many practitioners spoke of the need for diversity and inclusion in SRM, in two respects: firstly, as it relates to how identity characteristics affect the risks of individual aid workers, and secondly, to diversify the profiles of security staff themselves.

## People in SRM roles

One of the major trends identified by the research team and interviewees was a growing diversity in the profiles of the professionals employed in SRM positions. Overall, there appear to be more of the following profiles and skill sets of security staff than in previous years:

- Humanitarian backgrounds
- Individuals from the Global South
- Women
- Individuals with soft skills

## Person-centred approach to security

The emerging consensus in SRM thinking is that an aid worker's personal security is impacted by the interplay between where the aid worker is working, their role and organisation, and who they are (intersectional identity characteristics, such as age, gender, religion, ethnicity, and nationality). Thought leaders in SRM have advocated in recent years for a 'person-centred approach' to security, which aims to incorporate identity-based risks within organisational SRM approaches.

**At its core, a person-centred approach is about putting in place appropriate risk mitigation measures to match individual risk levels, not reducing opportunities for staff due to their individual risk profiles.**

Many security staff in this study knew of the approach and endorsed it but remain uncertain as to how to address it within their organisation's SRM structure. Some of the key discussions underway in this space are outlined here.

### Individualised risk assessments

- Individualised risk assessments are a key method in implementing a person-centred approach especially when done for staff in advance of travel, but an unrealistic expectation for organisations with frequent staff deployments and large in-country teams.

### Information sharing

- Some organisations have taken the path of informing staff of risks more generally (for example, by providing information about risks to LGBTQI staff in particular countries) and encouraging staff to raise concerns if they want to.
- Adopting a detailed informed consent process, which provides sufficient information to allow individuals to make informed personal security decisions, would allow an organisation to employ a person-centred approach and also support the organisation in meeting its duty of care obligations.

### Concerns over discrimination

- Many security professionals said they struggle with a thorny question: when is engaging with security-related identity issues a form of 'support' and when is it 'discriminatory'.
- However, conversely a 'don't ask, don't tell' approach, increases the risk that security decisions around personal vulnerability are random and based on individual decision maker's beliefs and biases.

### Benefits of institutionalisation

- An institutional and systematic approach can reduce the risk of discrimination and inequity, and foster a culture of openness and discussion about differentiated risks.

### Practical examples of a person-centred approach to security

- Incorporating identity risk in training, risk assessments, risk mitigation measures, and travel guidance documents.
- General communication about identity-based risks and organisational support available.

# Conclusion and recommendations

Humanitarian Outcomes | gisf

The considerable progress made by aid organisations in managing security risks is demonstrated by their continued work in high-risk crisis contexts and is widely acknowledged by humanitarian practitioners. To build on the progress made, the next phase of efforts needs to focus on extending SRM capacities and competencies to the wider humanitarian space. Working to bridge the significant gap between international and local NGOs, adapting to evolving security threats, becoming more forward-looking and fostering a person-centred approach in SRM practices will better protect those committed to delivering aid in increasingly challenging environments.

## Adapting to new threats and risks

- **Maintain updated and responsive risk assessment processes,** ensuring SRM systems and personnel lead in the process of identifying and adapting to changing local conditions and risk levels.
- **Explore developing in-house discussion exercises in 'horizon scanning',** where groups brainstorm about improbable yet impactful events to motivate innovative thinking and organisational resilience.
- **Widen the scope of inputs for risk assessment and context analysis,** bringing together staff from different departments, and from all levels of the organisation, to get a better understanding of the context.
- **Identify the appropriate skill sets and focal points for assessing emerging threats and risks,** including misinformation and cybersecurity threats, and clarify organisational responsibilities between SRM, IT, and communications staff.

## Localising SRM through more ethical and equitable partnerships

- **Incentivise international organisations to share, rather than transfer, security risks with national and local partners.** This can be achieved by more donors requiring grantees to show evidence of collaborative SRM planning and support for any downstream partners.
- **Include SRM staff in project design with partners** to ensure security considerations are built into programme activities before contracts are signed.
- **Practise the principles of good partnership –** equity, transparency, mutual benefit, complementarity, and responsibility – to aid in the organisational mindset shift from 'risk transfer' to 'risk sharing'.
- **Implement previous fair funding recommendations** on providing adequate overheads, including security costs in programme budgets, and building flexibility and force majeure clauses into contracts.

## Supporting coordination and filling coverage gaps

- **Support existing national and local coordination platforms** to incorporate and develop capacity for SRM, and/or support new local initiatives to coordinate around SRM. This is in recognition that international bodies cannot accommodate the SRM coordination needs of all local actors in the space, and there are benefits to locally-led entities to augment and link to existing coordination platforms.
- **Reset and recommit to the SLT framework** in the form of a new statement of intent between NGOs and UN stakeholders that clarifies the framework and sets goals for more effective leadership and communication at country level.
- **Leverage informal digital platforms while mitigating risks** to acknowledge the benefits and widespread use of digital platforms for SRM information sharing, but with guidelines to manage risks of disinformation and fragmented information channels.

## Refining and extending existing SRM components

- **Support and enhance incident monitoring systems for local and national organisations** for more systematic tracking of security incidents.
- **Improve training accessibility and relevance for local and national staff and organisations**, preferably through pooling resources for continuous, relevant training opportunities in local languages that can accommodate large numbers of the local aid workers who need training most.
- **Do more to address staff wellbeing and mental health**, through culturally appropriate mental health support and a supportive work environment.

## Using SRM to help enhance, not hinder, improved humanitarian access

- **Integrate SRM into access initiatives** to ensure the inclusion of risk mitigation strategies and SRM expertise in ongoing access initiatives and negotiations, and avert the growing siloisation of access and security within and across organisations. This requires reinforcing that SRM is about enhancing, not inhibiting, programme delivery and is not an end in itself.
- **Address weaknesses in deconfliction** through a collective strategy for engaging with governments on issues of trust and accountability.

## Propagating the person-centred approach

- **Institutionalise the consideration of identity-based risks within SRM systems,** making this a more widespread and commonplace approach to risk management and mitigation than is currently the case.
- **Create an organisational culture supportive of a wide variety of identities and personal risk profiles,** thus fostering an environment that supports diverse identities.
- **Further diversify the profiles of SRM staff,** ensuring a diverse pool of security experts with a balance of skills and understanding in SRM and humanitarian programming and principles.