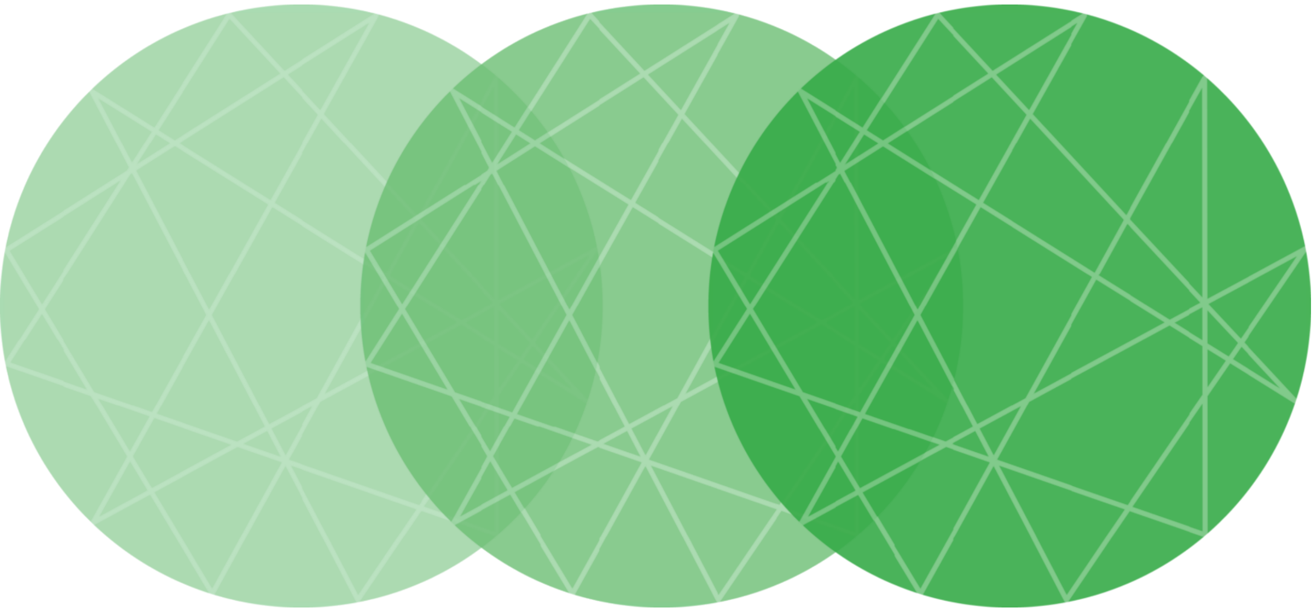
NGO Security Collaboration Guide

Published on 10 March 2022



The GISF NGO Security Collaboration Guide provides NGO security staff with advice and practical resources to support them in facilitating effective security collaboration with other organisations operating in the same context.

The guide highlights the different models and options for organisational collaboration, suggests how they can be established and maintained, and examines potential activities and support they can provide to humanitarian organisations.

Download a PDF version of the NGO Security Collaboration Guide (2MB)

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.

Home > NGO Security Collaboration Guide > Introduction

Introduction

≡

Most humanitarian and development non-governmental organisations (NGOs) appreciate the value of sharing information and collaborating with other organisations operating in the same space to improve their collective security.

In the past, organisations were wary about sharing security information, concerned it would place staff at greater risk, or expose weaknesses or mistakes in their security approach. Now, however, there is greater recognition that coordinating and collaborating on security issues is in everybody's best interest, and actively engaging with inter-agency security networks and forums has become an essential element in maintaining a successful presence in complex contexts with ever-increasing risks to staff.

We are also witnessing a significant growth in online or virtual NGO security networks at national, regional and global levels, increasing both accessibility and participation. Such networks offer huge opportunities for information sharing, discussion, and greater collaboration, but they are not without their unique challenges.

Security collaboration mechanisms offer particular value for smaller NGOs which are often constrained by limited budgets and minimal security capacity. The ability to access the security information and support provided by networks and forums enables smaller organisations to confront operational security challenges without the need for large formal security structures. However, regardless of size, all NGOs benefit from the collective support offered by security collaboration mechanisms.

Despite several successes, and even when the need for a mechanism to share security information and coordinate on security issues is widely recognised – and indeed demanded – by NGOs on the ground, it can be difficult to get initiatives up and running. Many successful initiatives have been largely dependent on the commitment and personalities of the individuals involved.

Even when a mechanism gets off the ground, maintaining it is equally challenging, especially given the high turnover of staff within the sector; when those who have been central to a mechanism's success move on, and others are unwilling to take up the task, the mechanism often ceases to exist.

During emergencies, or as a result of sudden deterioration in security, smaller organisations often look to security staff from the larger humanitarian NGOs to establish much-needed security networks or forums, and to facilitate the sharing of security information for the NGO community. While security personnel may be willing to support in this way, they are often time-constrained or have limited experience in establishing security collaboration mechanisms.

For local and national NGOs (L/NNGOs), access to security collaboration mechanisms is an additional challenge. Already pushed to deliver assistance under increasing risks, often without adequate resources to do so, many collaboration mechanisms are only accessible to security staff from international NGOs (INGOs). Even where L/NNGOs can participate, language, technical barriers, and, in some cases, power imbalances make it difficult for them to access security information or discuss their concerns. Enabling better access to security collaboration mechanisms is a critical part of the 'localisation' agenda which commits to improving support to, and strengthening the capacity of, local and national aid organisations.*

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

About this guide

This guide provides NGO security staff with advice, tips, and practical resources to support them in facilitating effective security collaboration with other organisations operating in the same context. The guide is also applicable to security collaboration and coordination mechanisms at the regional and global levels. The guide is intended for use as a reference rather than providing a prescriptive framework for NGO security collaboration.

The guide explains the overarching principles of security collaboration, highlights different models and options to be considered, suggests how such collaborative efforts can be established and maintained, and examines potential activities and support they can provide to humanitarian organisations.

Why collaborate?

Collaboration means acting together in the interests of a common goal. The goal is not collaboration itself, but the results it can produce. NGOs are diverse organisations, with different mandates, values, and approaches. However, organisations do not operate in a vacuum – what affects one NGO will almost certainly affect others. By working together, NGOs are more informed, more effective, and have a stronger voice on issues of concern across all aspects of providing humanitarian assistance, including security.

What is security collaboration?

In its simplest form, security collaboration is when NGOs come together to share relevant information and work in partnership to address common concerns regarding the security of their staff, programmes, and organisations.

Although responsibility for the security of staff and programmes will always remain with the respective NGO, actively sharing information and looking for opportunities to support each other improves our ability to provide sustained assistance in the most challenging of security contexts.

The creation of NGO-focused and managed security collaboration mechanisms provides a platform through which a diverse group of NGOs can exchange different perspectives and information on security incidents, share expertise and capacity and, if necessary, establish common and complementary positions in regard to security and access challenges.

Security collaboration

Security collaboration between NGOs in the humanitarian sector is when organisations are willing to act together to address common concerns regarding security and access, to share information on incidents and risks within the operating environment, and to strengthen their collective capacity to minimise risks to their staff, programmes, and organisations.

Acknowledgements

The NGO Security Collaboration Guide was authored by Shaun Bickley (**Tricky Locations**) with input from Lisa Reilly (GISF Executive Director).

The author and GISF would like to thank the following individuals and organisations who took the time to share information and resources, and contributed to the development of this guide: Caelum Moffatt (International NGO Safety Organisation), Chris Allen (Norwegian Refugee Council), Chris Williams (CARE International), Christina Wille (Insecurity Insight), Dieudonne Leroy (GOAL), Gerardo Calix (Catholic Relief Services), Gonzalo de Palacios (Oxfam International), Iván Pelaez (Save the Children), James Moulton (World Food Programme), Jeff Saayman (Danish Refugee Council), Joana Costa (Kvinna till Kvinna), John Murray (Relief International), José Luis Barreiro (International Humanitarian NGO Forum in Colombia), Kelsey Hoppe (Safer Edge), María Isabel León Jiménez (Save the Children), María Paula Martínez (Save the Children), Mayra Arana (Save the Children), Mohammad Ismail (Norwegian Church Aid), Nathanael Jarrett (Danish Refugee Council), Neil Elliot (Relief International), Sam Sherman (Danish Refugee Council), Scott Richards (Foreign, Commonwealth & Development Office), Soman Moodley (Lebanon Humanitarian INGO Forum), Sophia Guirguis (Libya INGO Forum), Stuart Fraser (Danish Refugee Council), and Zakaria Nadirashvilli (World Vision International).

1. Security groups, networks and forums

There is no standard model for inter-agency security collaboration; mechanisms exist in many different forms. Mechanisms range from small groups of interested NGO security staff sharing security information informally via Skype or WhatsApp, to hosted or stand-alone structures which have dedicated staffing, enabling them to provide a broad range of security services to the NGO community including security information, analysis, technical assistance and training.

Although collaboration mechanisms have diverse structures providing different services and activities, the majority can be categorised into one of five broad models:

- Peer-to-Peer Security Groups
- Interagency Security Networks
- Security Consortiums or Partnerships
- NGO-Managed Security Forums
- NGO Security Platforms

While some mechanisms have been very successful in certain contexts, similar approaches tried elsewhere have been less effective. Therefore any mechanism will need to be adapted to the operational context, specific security needs of the NGOs on the ground, and available resources. The different security collaboration models are examined in the table below.

	Peer-to-Peer Security Group	Inter-agency Security Network	Security Consortium/ Partnership	NGO-managed Security Forum	NGO Security Platform
KEY FEATURES	• Informal/ad hoc group. • Often exist as virtual/online groups. • Individual security staff take the lead, initiating the group and hosting meetings. • Hosting responsibilities may change on a revolving basis. • Main activities include information sharing and periodic meetings. • Members share reports/information directly via email or online chat platforms.	• Formal network with membership criteria & agreement. • Chair/co-chair elected to lead network. Chair/co-chair positions change periodically. • Activities include information sharing, regular meetings, thematic workshops, and training events. • Information shared directly by members or via network leads, enabling anonymised reporting. • Network may also represent NGO interests at various coordination fora or with UNDSS.	• Full-time/part-time Security Advisor appointed to support NGOs involved. • Security Advisors have Terms of Reference (ToR). Recruited by host organisation. • Security Advisors' time may be divided between NGOs and host organisation – eg 70% for NGOs & 30% for host. • Activities include security updates, technical security support and training. • NGOs influence ToR (via an advisory group) but management rests with host organisation. • Host organisation responsible for HR, and if funded, donor contracts.	• Linked to wider coordination body or stand-alone security structure. • Managed/hosted by NGOs. • Steering committee oversees the initiative's activities and services. • Full-time security staff provide support to forum members. • Security team may include other roles – Info Analyst, Training Officer. • Activities include facilitating meetings, providing security updates and regular reports, training, technical support, and crisis assistance. • Forums are usually capital-based, with travelling security staff. However, in some contexts the forum may have presence in specific areas.	• Independent organisation with own staff. • Advisory Board established with in-country NGOs to ensure services meet the needs of NGOs. • Offer extensive menus of NGO security services including threat warnings /alerts, incident tracking, security reports, briefings and meetings, orientations, training, security reviews, and crisis assistance. • Information and services are limited to registered NGO partners. • Facilitate cooperation with UNDSS and other security actors – international military and local security forces. • Security staff presence at both national and sub-national levels.

	Peer-to-Peer Security Group	Inter-agency Security Network	Security Consortium/ Partnership	NGO-managed Security Forum	NGO Security Platform
FIELD EXAMPLES	• Bangladesh INGO & Corporate Security Forum. • Latin America and the Caribbean (LAC) Regional Security Forum. • Afghanistan INGO Safety & Security Group (Skype). • Colombia Grupo de información de seguridad. • El Salvador Grupo de Puntos focales de Seguridad.	• Middle East and North Africa (MENA) Region Humanitarian Safety & Security Forum. • East Africa Regional Security Forum. • Haiti Forum de Sécurité (FOSEC).	• NGO Safety Advisor Program – South Sudan (DRC). • Safety and Security Advisory Group – Northern Iraq.	• Libya INGO Forum – Safety Advisor. • Ethiopia Humanitarian INGO Forum – NGO Safety Officer, Tigray. • South Sudan NGO Forum – Security Team. • Pakistan Humanitarian Forum – Safety Team.	• INSO is the leading provider of country-level NGO security platforms. All previous NGO security platforms have been replaced by INSO platforms. • INSO platforms currently exist in Afghanistan, Burkina Faso, Cameroon, CAR, Chad, DRC, Iraq, Kenya, Mali, Niger, Nigeria, Somalia, South Sudan, Syria, Ukraine.
PROS	• Quick and easy to establish. • Limited commitment required from participating NGOs. • With small groups, often easier to establish a level of trust. • Fairly discrete mechanism, unlikely to face restrictions from authorities.	• Slightly more control over members' behaviour – agree to certain protocols. • Possibility of anonymising incident reports may prompt sharing of sensitive information. • Provides a platform to agree coordinated approach or to raise issues of concern.	• Good for organisations with limited security capacity, no full-time security staff. • High trust levels/info sharing if Security Advisor seen as neutral. • Possibility to have security position funded by donors. • Opportunity to build capacity of partners and L/NNGOs through direct security support and training.	• More neutral role, NGOs more likely to share information on incidents. • Feeling of ownership by NGOs, more committed to supporting initiatives. • Strong voice through coordination body to agree coordinated approach or to raise issues of concern.	• Comprehensive range of services – free of charge. • Inclusive service, available to both INGOs and L/NNGOs • No administrative burden or financial risk for NGOs. • Consistency of services, regardless of staff turnover. • High levels of incident sharing – perceived as neutral body.

	Peer-to-Peer Security Group	Inter-agency Security Network	Security Consortium/ Partnership	NGO-managed Security Forum	NGO Security Platform
CONS	• Short lifespan – difficult to maintain if key people leave. • Information is not verified. • Limited influence on members' behaviour – more risk of info sharing breaches. • Often involves security staff from larger INGOs – excludes non-security staff or L/NNGOs.	• Relies on larger NGOs with full-time security staff to instigate and take the lead. • Some NGOs may be unwilling to undertake chair roles. • Not all incidents will be shared with the network – depending on size, organisations involved.	• Significant burden on host organisation. • Expectations of participating NGOs can be difficult to manage; conflicting demands sometimes occur. • High turnover of advisors leads to gaps in coverage.	• Substantial funding needed to ensure staffing levels and long-term provision. • Due to higher profile, authorities may restrict certain activities or censor information. • NGOs have tendency to become passive – requires more effort to maintain engagement.	• Exist mainly in high-risk operational contexts. • Often takes time to establish – support, funding, staffing, and registration.

A leading provider of country-level security platforms for NGOs is the **International NGO Safety Organisation** (INSO). INSO provides a wide range of free services to partner NGOs operating within high-risk settings, including the establishment of country-level and area-specific NGO security coordination platforms.

International NGO Safety Organisation (INSO)

- INSO country-level security platforms provide a wide range of services depending on the security context and the specific needs of the NGO community, but in general services include incident alerts and tracking, analytical reports, crisis assistance, site security reviews, staff orientations and training.
- INSO platforms are accessible to both INGOs and L/NNGOs, provided they are legally registered or constituted within the country where the platform is established, and they adhere to INSO's Code of Conduct. INSO also assists NGOs in security coordination with the UN agencies under the Saving Lives Together Framework.
- INSO platforms are usually established at the request of NGOs operating in the country. A group of NGOs may come together, or work through an existing NGO forum, and invite INSO to undertake a scoping mission to assess the feasibility of establishing a platform within the

country. However, decisions to launch INSO platforms are also subject to the availability of funding and the ability of INSO to legally register within the country.

- For all platforms, INSO establishes a voluntary Advisory Board which includes representatives from the in-country NGO community. The Advisory Board assists in determining the scope of services INSO will provide, and meets regularly to monitor the implementation of these services and INSO's performance.

2. Other mechanisms and initiatives

In addition to NGO-led or focused security collaboration mechanisms, there are several other initiatives that aim to strengthen security collaboration between organisations that may be active in the operating context.

Saving Lives Together (SLT)

Saving Lives Together (SLT) is an initiative to strengthen security collaboration between the UN Security Management System (UNSMS), INGOs and International Organisations (IOs). The objective of SLT is to enhance the ability of partner organisations to make informed decisions and manage risk based on shared information and knowledge.

Although sometimes misinterpreted as a list of services that the UN provides to NGOs, the SLT framework is a partnership initiative whereby organisations commit to collaborate on several areas, such as improving coordination, sharing information and resources, and facilitating access to training.

Organisations perceive and assess risks differently, and therefore implement security arrangements which suit their organisation and its operational conditions. SLT aims to support an organisation's existing security risk management framework, not replace it – all organisations retain responsibility for the safety and security of their own staff.

Saving Lives Together Framework

Saving Lives Together, launched originally in 2001 as the 'menu of options' and then rebranded as Saving Lives Together in 2006, is a framework for improving UN-NGO security collaboration in humanitarian operations and includes:

- Establishing security coordination arrangements and forums.
- Sharing relevant security information.
- Cooperating on security training.
- Cooperating on operational and logistics arrangements, where feasible.
- Identifying resource requirements for enhancing security coordination between the UN, INGOs and IOs, and advocate for funding.
- Consulting on common ground rules for humanitarian action.

SLT collaboration mechanisms may be established at country level and replicated at area/regional level where required. SLT implementation is divided into two levels: Regular and Enhanced:

- **Regular Level SLT** – focus is on establishing dialogue and information sharing arrangements.
- **Enhanced Level SLT** – for more complex security environments, resulting in more enhanced information sharing, security coordination, and operational arrangements.

Determination of the appropriate SLT implementation level is made by the SLT Oversight Committee in close consultation with SLT partner organisations at national, regional and HQ levels.

The primary benefit of SLT is access to additional security information, access to UN Safe and Secure Approaches in Field Environments (SSAFE) trainings and other collaboration opportunities. SLT global counterparts at HQ level receive daily situation reports and can access a common online platform, country WebEx sessions and SLT contact information, as well as access to UNDSS security training.

SLT is available to all INGOs with established operations, or significant activities in the country, regardless of whether they are UN implementing or operational partners. There are no fees or contributions for SLT participation, although some services may be provided on cost recovery basis. Access to SLT is determined at country level and is not dependent on any agreements or counterpart arrangements between United Nations Department for Safety and Security (UNDSS) and the respective INGO or IO at the global level. Where NGO security collaboration mechanisms exist, these can help foster greater SLT cooperation and engagement through the facilitation of information sharing and promoting the needs of the wider NGO community.

While L/NNGOs cannot attain SLT partnership status and therefore do not fall under the SLT Framework, they may still benefit from SLT support through existing NGO security networks or platforms established within their country, such as INSO, or wider coordination bodies and NGO forums. For example, coordination platforms such as the South Sudan NGO Forum and the Humanitarian Forum Yemen have facilitated access to SLT support for their L/NNGOs members.

To ensure coherent implementation of Saving Lives Together, an Oversight Committee (SLT OC) has been established. The SLT OC also decides on the application of the SLT implementation levels. The SLT OC is co-chaired by UNDSS and an INGO representative and includes representatives of different UN agencies, the Steering Committee for Humanitarian Response (SCHR), and NGO coordination platforms, including GISF, ICVA, and InterAction.

UN partner security support

In addition to SLT mechanisms, several UN agencies provide additional security coordination support to implementing partners. For example, World Food Programme (WFP) has established initiatives to improve security collaboration with cooperating partners and other humanitarian organisations operating at country level. The aim is to improve security information sharing, to provide technical advice and to contribute to improved humanitarian access.

{TESS+} Telecommunications Security Standards

Facilitated and coordinated by WFP, {TESS+} is the primary source for guidance and support on Security Communications Systems (SCS) between the UN Security Management System (UNSMS) and NGOs at the global and field-levels.

{TESS+} is mandated by UNDSS, in collaboration with the Interagency Security Management Network (IASMN) and the Emergency Telecommunications Cluster (ETC), to provide field support in establishing pragmatic and cost effective SCS solutions.

{TESS+} provides guidance on standards and the implementation of procedures, and conducts regular field missions to provide hands-on technical support, including training, to strengthen SCS technologies and infrastructures in remote areas and challenging conditions.

Further information and resources on {TESS+}

This collaboration mechanism is coordinated through GISF and WFP. NGOs submit support requests through their HQ, to link security focal points at national or local levels with WFP Security Advisors in country.

Donor security support initiatives

Humanitarian donors increasingly recognise their vital role in supporting security risk management and the need to improve the exchange of security information among partners, as it ultimately leads to better programme implementation.

Several donors have established initiatives to strengthen security collaboration between organisations and to provide greater security support to their implementing partners. For example, USAID's initiative, the Partner Liaison Security Operation (PLSO), aims to enhance the sharing of security information and advice between USAID and its implementing partners, both international and national organisations, and to support implementing partners to better manage and mitigate their own security concerns.

PSLO projects have been established in Nigeria, Haiti, Kenya, South Sudan and Ethiopia, in addition to Security Advisor positions within Afghanistan and Nepal. In most cases, PLSO implementation has been outsourced to commercial risk management companies, but the services offered under this programme are free to all USAID implementing partners, and in some cases are extended to organisations funded by other donors.

USAID Partner Liaison Security Operations (PLSO)

Partner Liaison Security Operations (PLSO) is a USAID-funded initiative to enhance communication and support between USAID and its Implementing Partners (IPs) regarding safety and security. PLSO provides a variety of services to USAID and its IPs, including:

- Threat alerts – by text and email.
- Security awareness briefings.
- Online and in-person security training.
- Workshops and networking events.
- Security resources and templates.
- Office and operating area risk assessments.
- Security advisory services.

The UK's Foreign, Commonwealth & Development Office (FCDO), previously DFID, and the German development agency GIZ have established Risk Management Offices (RMO), jointly in Nepal, and separately in Nigeria (DFID), Yemen and Afghanistan (GIZ). While the RMOs principally support the donor's own staff and programmes, security advice, information, training and support is also extended to partners.

3. Establishing a collaboration mechanism

Regardless of the many benefits of security collaboration, it does not happen automatically; it is a challenge to initiate and will be ineffective if not developed through careful assessment and planning of its expected scope, structure and activities.

3.1 Assessing need

Coordination or collaboration mechanisms tend to proliferate during emergencies, especially large-scale humanitarian responses. They are time-consuming for organisations to engage with and can require significant resources, so there needs to be a clear added value in establishing additional mechanisms. However, if well run, they can significantly improve the response.

When looking to establish an NGO security mechanism, careful consideration must be given to why it is needed, and which collaboration type or model will best meet the security needs of the different NGOs in that specific context.

Key questions

- Who are the primary stakeholders – L/NNGOs, INGOs, or all NGOs, and what implications might this have for the type of security mechanism established?
- How many NGOs have full-time security staff or security-specific focal points, and will non-security staff be involved?
- What coordination or information sharing mechanisms already exist, and what are the language requirements for meetings and security information?

- What are the main security information and support needs of the NGOs involved?
- How sensitive is discussing and sharing information on security within the context, and how does this impact the visibility of the security mechanism?
- Which organisations have the capacity to lead and/or support the initiative?
- What potential resources and funding are available to support a security collaboration mechanism?

It is important to note that security information and support needs may evolve over time, and the collaboration mechanism will need to adapt to these changes. For example, what starts as a small group of NGO security staff forming a network to exchange security information may in time become a security forum with a full-time security coordinator.

Alternatively, due to a significant deterioration in the security situation, increasing NGO demand and the availability of donor funding, NGOs may request INSO to establish a stand-alone platform to expand security support services to all NGOs operating in different areas of the country.

When identifying and developing a suitable collaborative initiative, it is important to consider scope for expansion and growth, as well as down-scaling, and identify indicators that may trigger such changes. This flexibility will enable the mechanism to continue to meet the adapting needs of NGOs involved, and to respond to changes in the security situation.

Determining factors

- **Level of insecurity** – in insecure environments, where aid workers are frequently targeted, NGOs will be looking for more comprehensive security information and support, provided by a stand-alone mechanism, with dedicated staffing.
- **Number of NGOs** – the more NGOs operating in a given environment, the greater the demand on the security services provided by the mechanism, which has implications for the structure and capacity required.
- **Geographical coverage** – where NGO operations are widespread then additional sub-national networks or forums may be required to support NGOs working in different areas of the country.
- **Existing coordination structures** – lack of, or frustrations with, existing coordination structures will influence demand for a separate security-focused mechanism. However, given strong overlap with NGO fora, it is often useful for such security networks or forums to be linked to existing mechanisms.
- **Attitude of authorities** – in some contexts, sensitivities or suspicion associated with security issues, and interference by authorities, may force NGOs to adopt a less formalised mechanism or limit certain activities.
- **Resources and funding** – larger mechanisms with staffing require significant resources. If funding is limited and NGOs are unable to contribute sufficiently

themselves, a less resource-intensive mechanism, such as a security network, may be required.

3.2 Defining scope, activities and support

With any security collaboration mechanism, it is essential to clearly identify its purpose, what it aims to achieve, and therefore what activities and support it should provide and, importantly, what limitations it may have. For example, is the primary focus to improve security incident reporting between organisations, or to provide a platform for NGOs to discuss the security situation and how each is responding, or is it to provide technical security support to organisations with less security risk management capacity?

Initiatives often lack buy-in and support if NGOs feel that they have not been sufficiently consulted when defining scope and activities, or have little or no say in the development of the initiatives. From the outset, it is important to solicit widespread participation in defining the aims and objectives of any initiative.

NGO security mechanisms can provide a wide range of support services. Some of the most common activities include:

- Convening security meetings/briefings.
- Issuing security alerts/threat warnings and advisories.
- Providing regular security reports.
- Preparing analysis of incident trends or specific security challenges.
- Liaison with UNDSS and other security actors (national security forces, including police and military, international military forces, etc).
- Facilitating access to security training.
- Providing support during critical incidents.

The full extent of services a security network or forum provides to its members should be documented within its Terms of Reference/Charter, or in a separate Scope of Services document, translated and widely disseminated, to ensure shared understanding of what the network or forum does and does not do.

Tools

- **Tool 1 – Terms of Reference (ToR)/Charter template**

It is important to clearly articulate the advisory nature of the information and support provided. The primary objective is to support informed decision-making through shared information, not to replace the internal security management systems of the participating NGOs. Security risk management and the duty of care to staff remains the sole responsibility of individual NGOs.

3.3 Membership and engagement

Ultimately, collaboration mechanisms are only as good as the organisations involved and the level to which they engage. During the early days of any new security mechanism, membership is likely to be small, and mostly confined to a few proactive security staff. However, as the mechanism matures, interest will increase, and with it a need for clear membership criteria. In some contexts, there may be good reasons for limiting membership, but a lack of transparency on who is involved and why creates a risk of the mechanism being accused of being elitist or discriminatory.

The individuals involved, and the profile and mandate of the different organisations who participate, will have a significant effect on the level of engagement, and ultimately the level of trust. A frequent criticism of NGO security networks, especially smaller informal groups, is that they are only accessible to security staff from the larger INGOs.

Efforts to ensure 'trust' relationships are maintained between security staff can make L/NNGOs, or smaller INGOs feel excluded, or result in the establishment of various sub-groups based on the size, type, or operational focus of organisations. Equally, if individuals or organisations involved in a network are perceived to have close links to the authorities or specific security actors, or adopt a strong advocacy position which is at odds with the position adopted by other members, then this will likely limit what other members vocalise or share within the network.

Although a large membership can affect information sharing and engagement dynamics, language and perceived priorities are also significant challenges to broader participation. However, the importance of L/NNGO participation in security networks and forums cannot be underestimated.

Security is all about trust, so not only does INGO-L/NNGO security collaboration provide an opportunity for trust building and networking, but sensitive security information is also often initially shared through L/NNGOs, with their strong relationships with local communities, religious leaders, and local volunteers. It is crucial that security collaboration mechanisms not only encourage L/NNGOs to participate, but also empower them to take greater leadership roles in the network or forum.

Strong engagement by all NGO members is not easy to attain. It is common to have a range of engagement levels and many NGOs may choose to be passive members. This is not necessarily a negative, as their presence alone may be equally important in terms of collaboration. It is important to note that even those less engaged NGOs can still value their membership and the services the network or forum provides.

Fostering member engagement

- **Create a welcoming and inclusive atmosphere** – all member organisations should have an equal 'voice', regardless of their size, status, or focus.
- **Identify membership benefits and responsibilities** – outline the network or forum's value to them as well as their responsibility and how they can participate.

- **Provide training** – organising an interagency security training or workshop will often stimulate interest in the security network or forum and strengthen the participation of members.
- **Ensure information and discussions are relevant for diverse membership** – provide content and engagement methods that are relevant and accessible to all members.
- **Establish clear and transparent decision-making processes** – each member should feel they can influence activities and that decisions represent the majority of the membership.
- **Define information and data protection policies** – members should be able to trust how information and data will be shared and used.
- **Create opportunities for members to participate in governance roles** – regardless of size, all member organisations should be able to take active roles in the network or forum.
- **Record and monitor engagement levels** – reach out directly to inactive members to explore reasons for not engaging, and identify any support requirements that may increase their engagement.
- **Establish feedback mechanism** – provide members with the ability to raise questions or express grievances about the mechanism, its governance, or the support it provides, including anonymously, if required.

Adapted from ICVA NGO Fora Member Engagement Guide, 2019

3.4 Governance, structure and responsibilities

Good governance is an essential component of any collaboration mechanism, regardless of its size and structure. An effective structure with transparent roles and responsibilities, and processes provides the foundation for attracting and retaining NGO support, and for ensuring the mechanism meets its objectives.

The most appropriate structure will be determined by the type of security collaboration mechanism established, and the activities and services it provides. However, it is important the structure enhances rather than hinders the functioning of the mechanism and it must be adaptable to changes in context, membership, and funding.

NGO security mechanisms often start out as informal security groups and then adopt more formal measures as the number of members and range of activities increases.

Most security networks have a chair or lead who coordinates the activities of the network, organising meetings and events. Network chairs/leads are normally full-time NGO security staff, who support the network on a part-time basis. Therefore, to limit the burden of the role, it is advisable to appoint co-chairs/leads to help share tasks and to rotate these roles amongst the participating organisations.

Sharing leadership roles often produces stronger engagement and better collaboration and helps ensure a network's sustainability despite staff turnover.

NGO security forums, the largest NGO-managed security mechanisms, normally have a full-time representative or coordinator, supported by a Steering Committee or Advisory Board.

The degree to which NGOs are involved in the mechanism's governance is dependent on the governance structure put in place. For example, a Steering Committee would be responsible for setting the mechanism's strategic direction and overall aims and objectives and maintains accountability to members.

Steering Committees usually nominate a Chair to ensure the Steering Committee functions properly and to provide direct support and advise the forum's Coordinator. Alternatively, an Advisory Board is a more informal group which has fewer responsibilities but can be consulted to ensure that the mechanism continues to meet the needs of the NGOs. Advisory Boards do not determine how a mechanism should be run or what services it provides; that responsibility rests with the security mechanism's internal management or its host organisation.

Essential documents

- **Terms of Reference (ToR)/Charter** – defines the mechanism's structure, components, membership criteria, and the scope of services. Document should also outline responsibilities and obligations for member organisations.
- **Information Sharing Protocol** – specifies the policy and procedures in relation to the sharing of information and data within the network or forum.
- **Steering Committee ToR** – establishes the remit, roles, and responsibilities of the governing body and the process for selection.
- **Host Organisation Memorandum of Understanding (MoU)** – clarifies respective roles, responsibilities, and decision-making authority between the host organisation, the forum's Coordinator/Secretariat and the Steering Committee with respect to human resources, financial management, donor relations, and operational and administration support.
- **Security Coordinator/Advisor Job Description** – describes the general tasks, responsibilities, and reporting lines of the forum's Security Coordinator/Advisor.

If the collaboration mechanism has more than one full-time staff member, then these employees would form a Secretariat. The Secretariat should be relatively autonomous and manage activities itself, with overall guidance and support provided by the Steering Committee.

Tools

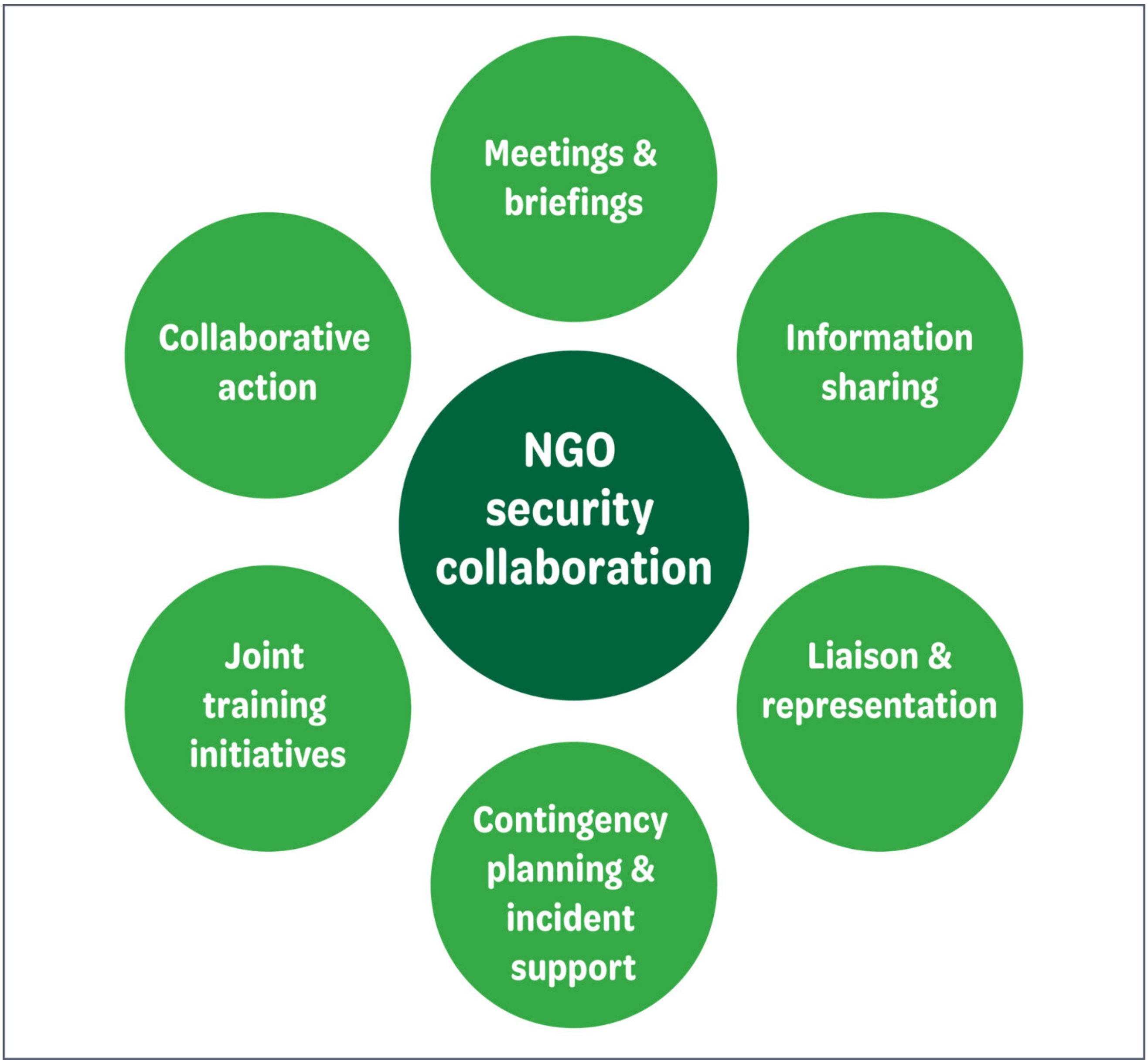
- **Tool 2 – Steering Committee ToR template**

- **Tool 3 – Security Coordinator/Advisor Job Description template**

The forum's Coordinator or Secretariat would typically be hosted by one of the member organisations, as establishing a separate legally independent organisation can be difficult, time-consuming, costly, and in many cases, unnecessary. The host organisation is responsible for contracting staff and holding any donor contracts therefore assumes the financial and legal risk.

4. Activities and support

The range of activities and support services that a security collaboration mechanism provides to NGOs will depend on the type of mechanism, its structure and capacity, the resources available, and NGO needs in that particular context.


Meetings & briefings
Collaborative action
Information sharing
NGO security collaboration
Joint training initiatives
Liaison & representation
Contingency planning & incident support

4.1 Meetings and briefings

A key role of any security network or forum is facilitating a space for NGO security staff to meet colleagues working within other organisations to share information, experiences, and concerns. Networking and face-to-face information exchange is vital to build relationships and trust amongst security staff from different NGOs.

Facilitating a regular security meeting or briefing enables NGOs to share information on incidents, discuss changes in the security environment and identify issues likely to arise in the future. It also provides an opportunity to exchange views on different security approaches, and in some cases reach agreement on common approaches that enhance the security for the broader aid community.

The frequency of meetings required will depend on the level of insecurity, and the schedule of other meetings. In the first few days after a rapid-onset emergency, or during a significant deterioration in the security environment, daily meetings may be required. In other contexts, a regular weekly or monthly security meeting may be more appropriate. Meetings should be scheduled at times to suit the majority of organisations; for example, early morning or evening meetings often draw the largest attendance.

Chairing NGO security meetings can be challenging, because of the diverse range of organisations with differing levels of security awareness and different priorities. Some organisations may avoid formal security meetings, but may be willing to share information to varying degrees through other less public mechanisms.

Facilitating security meetings

- **Prepare** – invest time in preparation to maximise use of time during the meeting. Attending meetings is costly for busy staff in terms of time and activities missed, so make sure they add value.
- **Location** – ensure meetings are accessible in terms of location and space requirements. Consider using technology to maximise participation (Skype, Zoom, etc.).
- **Timing** – ensure meetings respect participants' time commitments. Plan meeting times around travel requirements, significant events and security considerations.
- **Dynamics** – consider inter-organisational relationships and make sure all participants can voice their queries or concerns. Establish smaller sub-group meetings to ensure more inclusivity and engagement from smaller INGOs or L/NNGOs.
- **Language** – if participants do not speak the same language fluently, ensure effective translation mechanisms are in place so that all participants can fully participate.
- **Agenda** – prepare an agenda in advance and explain the purpose and structure of the meeting, who is chairing and who will be attending. Try to manage expectations and provide an opportunity to clarify questions or discuss concerns before and after the meeting.
- **Ground rules** – establish ground rules immediately. Reach early agreement on confidentiality when sharing information or discussing incidents.
- **Inclusivity** – provide a safe inclusive space that enables all participants to express their opinions and share experiences.
- **Meeting management** – stick to the agenda and keep discussions focused on key issues. As chair, manage digressions – interrupt if necessary, but allow flexibility for closely-related issues and concerns. Try to be a neutral party, avoid talking too much or getting involved in heated discussions, be a good listener.
- **Document** – maintain a record of meeting attendees and share minutes of meetings and related action points with all participants promptly after meetings.

Online or virtual networks

The most marked change in NGO security collaboration and coordination has been the growth of online or virtual networks and groups. Most NGO security networks now exist online, and even for networks that still meet face-to-face, much of the information sharing and discussion takes place via online messaging platforms including Skype, WhatsApp, Signal, Telegram, and Slack.

Collaboration examples

In Colombia, security focal points from over 20 NGOs within the Humanitarian INGO Forum formed an online security group (Grupo de gestión de información de seguridad Foro de ONG humanitarias) to strengthen the flow of information on violence and insecurity in Colombia and to create a space to discuss security challenges faced by INGOs.

The group hosts monthly virtual meetings exploring different security-related topics, and an active WhatsApp group where members share security updates and incident alerts as they occur.

The group has established ToR which outlines the objectives of the group and requirements for participation, together with basic rules for sharing information within its WhatsApp group.

Establishing an online security network offers huge benefits. Members can communicate directly with each other, share and discuss contextual updates and incident reports, or seek advice from their peers on security issues and challenges. But online networks also come with additional security, privacy, and reputational risks.

Tools

• **Tool 4 – Online Group Chat Protocol template**

Which platform to use depends on the location, quality of data network, number of organisations in the network, and the sensitivity of information being shared. However, new platforms are emerging all the time, and staying abreast of these developments is critical to a network's success.

Further information

- **Frontline Defenders Guide to Secure Group Chat and Conferencing Tools**
- **GISF Security Risk Management Toolkit: Digital Security**

Managing online groups

- **Prioritise security and privacy** – in some contexts, the use of certain social media platforms is prohibited or subject to government monitoring. Assess digital security risks to determine which communication platform offers accessibility for members and sufficient security and privacy.
- **Identify admin team** – seek volunteers from within the network to act as group administrators. Administrators are responsible for monitoring posts and discussions and dealing with new members. Consider forming a committee/advisory group to help with new membership or removal decisions.
- **Control membership** – closed platforms should be used and only the group administrators should be permitted to add new members. All new membership requests should be checked to ensure individuals meet the group's criteria. Establish a process for removing members when they leave their role/organisation.
- **Establish ground rules** – guidelines are important for keeping conversations and posts positive, effective, and appropriate to the network. Create a transparent process for issuing warnings, and if required, removing members because of inappropriate posts. The online group's guidelines should be posted regularly to remind people and to provide the names of group administrators in case members have questions.
- **Monitor discussions** – despite issuing guidelines, there will be times when you need to remove comments/posts or address an issue. It may be more effective to address issues with individuals directly rather than through the open forum, but in some circumstances it will be important for the whole group to be aware.
- **Establish a process for anonymising posts** – some members may be reluctant to raise questions or post information within the group because of concerns about being identified as the source. To allow the information to be shared, provide a mechanism through group admins for members to post anonymously.
- **Create recognisable post format** – group administrators should use the same format for posts so that important information can be easily identified by group members.
- **Initiate discussion** – members may initially be reluctant to engage with each other online. Try to initiate discussions and get members talking through regular posts and updates.
- **Continually review the platform** – as technology advances, look to improve the security and functionality of the group, even if it means switching platforms.
- **Assess risks for admin team** – although administrators need to be known to ensure trust, in some contexts their association with the group can place them at increased risk from authorities, security forces or other actors due to the existence of the group or its posts. Look to minimise exposure of the admin team and keep their details and contact information confidential.

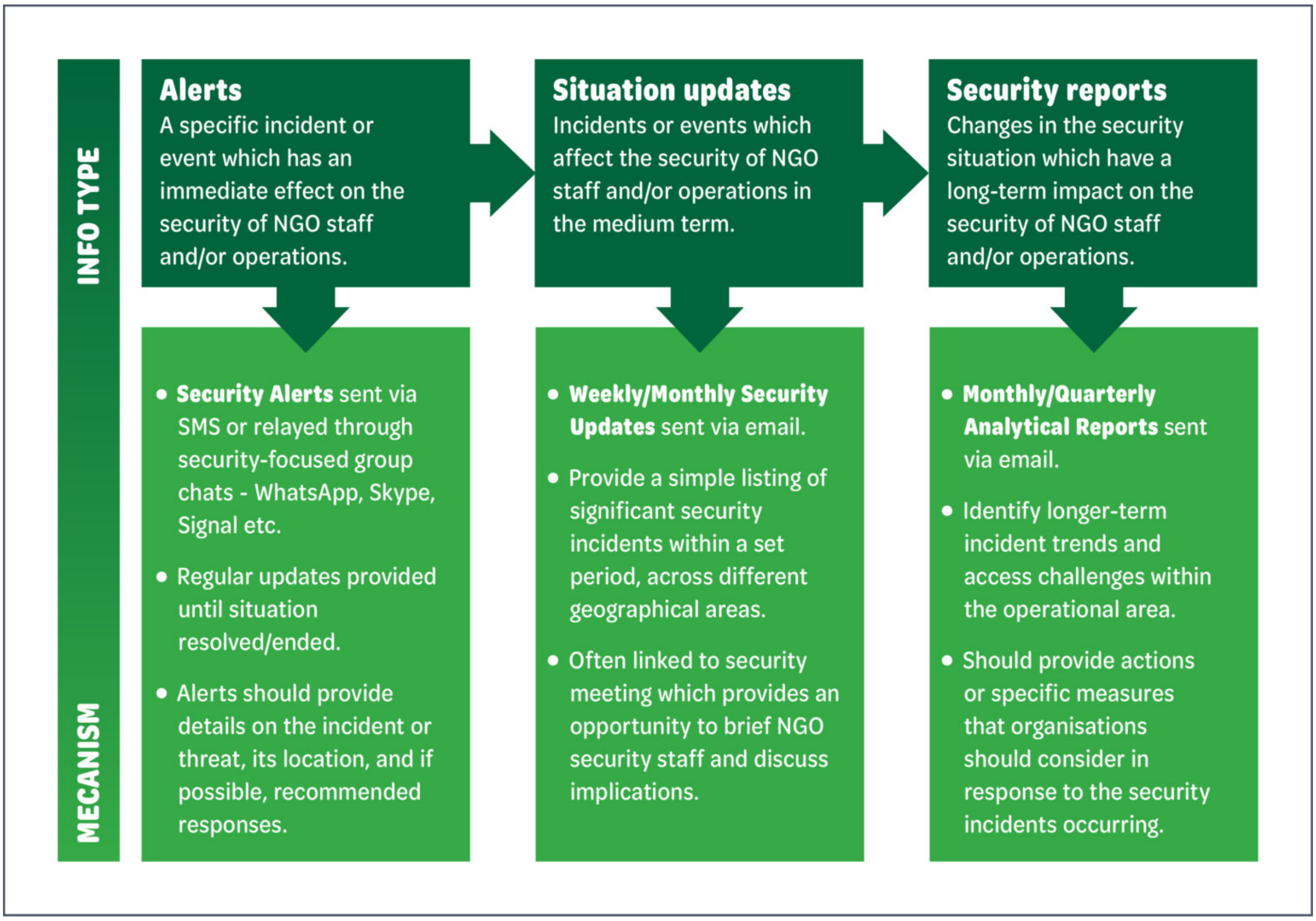
4.2 Information sharing

Improving the flow of security information is a core function of most security collaboration mechanisms; this is often the most utilised and valued activity that such initiatives provide.

Organisations do not operate in a vacuum – what affects the security of one NGO will almost certainly affect the security of others, therefore actively sharing information on security incidents and potential threats can improve the awareness and understanding of all organisations, enabling them to minimise risks to their own staff and programmes.

While security information may be shared via general coordination structures, it can be difficult to reach those staff responsible for security and safety at the national or local levels, or at an organisation's HQ. Establishing security-specific networks or forums helps to provide a central point to which incidents can be reported, and then shared directly amongst security staff within different organisations.

Even where informal security groups are established, agreeing a simple protocol for reporting security incidents, and distributing the information sensitively amongst security staff from other NGOs, will benefit everyone involved.



INFO TYPE

Alerts
A specific incident or event which has an immediate effect on the security of NGO staff and/or operations.

Situation updates
Incidents or events which affect the security of NGO staff and/or operations in the medium term.

Security reports
Changes in the security situation which have a long-term impact on the security of NGO staff and/or operations.

MECANISM

- **Security Alerts** sent via SMS or relayed through security-focused group chats - WhatsApp, Skype, Signal etc.
- Regular updates provided until situation resolved/ended.
- Alerts should provide details on the incident or threat, its location, and if possible, recommended responses.

- **Weekly/Monthly Security Updates** sent via email.
- Provide a simple listing of significant security incidents within a set period, across different geographical areas.
- Often linked to security meeting which provides an opportunity to brief NGO security staff and discuss implications.

- **Monthly/Quarterly Analytical Reports** sent via email.
- Identify longer-term incident trends and access challenges within the operational area.
- Should provide actions or specific measures that organisations should consider in response to the security incidents occurring.

However, sharing security information is not without challenges. The process of gathering and verifying incident data takes time, requiring cross-referencing from many sources to ensure reliable security information and analysis. It is very easy for rumours to quickly escalate if suitable verification processes are not established.

More formal collaboration mechanisms with their own staffing will have the capacity to verify incident reports and can provide a broader range of security information services, including live security alerts and advisories, weekly/monthly security updates, together with the ability to analyse security incidents trends on a monthly/quarterly basis to support NGOs in their decision making.

Effective security information is also dependent on organisations being willing to share security information with others, and quickly. To assist the flow of information, members can agree in advance the minimum levels of information to be shared (for example, location, date, type of incident and its severity) to ensure that essential information is still circulated.

Tools

Tool 5 – Information Sharing Protocol template

In certain contexts, security collaboration mechanisms and the sharing of security information will be particularly sensitive, especially in countries with high levels of state interference. The existence of any NGO security mechanism, and the information it shares, may result in increased threats to the NGOs and individuals involved. In such contexts, the availability of an independent platform to gather and circulate information on security incidents will likely provide a greater level of protection for the organisations involved.

Receiving incident reports

A major barrier to information sharing is trust. Concerns about indiscreet use of sensitive information shared via security networks can be a substantial barrier to sharing information. While there have been examples of information shared in such forums turning up on social media or quoted in the press, these are the exception.

In most settings, NGO security staff treat the information they receive sensitively. However, it is important to establish and agree clear protocols that explain how the information received will be handled, what will and will not be shared with the network, how to report information sharing breaches, and how these will be dealt with by the network.

Further Information

- Insecurity Insight Security Incident Information Management (SIIM)
- SIIM in NGO Security Collaboration

There may be different opinions as to what constitutes a security incident and what information is relevant to the security of aid workers. How security incidents are defined and the boundaries between other significant incidents, such as corruption or safeguarding allegations, or violence in the wider operating environment, are not always clear. Therefore, it is important to define what incidents the mechanism will monitor, share and disseminate, and to issue clear guidance to the NGOs involved.

Sometimes only limited information on an incident is shared, making it difficult to relay sufficient information to the network for other organisations to take action. Staff on the ground may not be authorised to share further information until they get clearance from their HQ, or will be reluctant to do so in case it exposes them to further security risks, or breach confidentiality or data protection. This means that the time between an initial incident report and it being shared with the network can be extended.

Encouraging information sharing

- **Promote the benefits** – while most organisations want to receive information, not all proactively contribute or share information with others. They may take some convincing and reassurance to appreciate the added value.
- **Build trust** – the primary focus, especially in the early phase, needs to be on building trust, not only among the individuals directly involved in the network or forum, but also in the effectiveness of the mechanism to provide relevant information on a timely basis.
- **Emphasise neutral role** – if not a separate structure, the neutrality of network/forum and the staff involved should be emphasised through clear statements from the chair/lead and articulated within the ToRs.
- **Meet face-to-face** – members are more likely to share information with people they know; the more individuals meet on a regular basis, the more willing they are to keep each other informed.
- **Create networking events** – such events provide an informal setting for members to meet and connect. They can build community and increase collective understanding and trust.
- **Establish clear protocols** – if members understand how any information received will be treated and disseminated, and how issues of confidentiality are managed, they will be more willing to share information.
- **Make it easy to report** – establish simple processes to report incidents or share information with the network, and where possible make use of technology and simple reporting apps to remove any administrative burden on those reporting.

In contrast, the speed at which information is shared via social media means that initial reports about a situation or incident are often unverified and therefore unreliable. When receiving information, it is important to consider its source and reliability, and seek to verify the information before sharing with the wider network.

Verifying information

- **Establish a process** – put procedures in place for verifying incident reports to ensure the information collected is as accurate and complete as possible. The verification process should assess the source, the report or post, and its content.
- **Build and maintain a network of trusted sources** – carefully select who you verify reports with and identify a range of stakeholders to gather different perspectives.
- **Identify verifiable indicators** – determine what information can be verified and what aspects of the incident report may be unverifiable.
- **Confirm the source** – identify and verify the primary source. Where possible, follow up with the source directly to verify the report or to identify corrections. Relying on secondary sources such as other NGOs, media reports or social media could perpetuate rumours.
- **Check their credibility** – evaluate the credibility of the source. Are they reliable? Have their previous reports been accurate? What are the source's credentials and affiliations? If the report is via social media, check the source's posting history, online activity, internet presence, and their possible connections.
- **Be sceptical** – challenge any assumptions. Who reported it? How do they know? Could they be mistaken, or their opinion be biased?
- **Confirm events** – information can change after initial reports. Double check what happened to whom, where and when, especially the location, date and time.
- **Triangulate the facts** – when possible, check the information with more than two sources, ensuring these are reliable and independent of each other.

Information on some incidents must be treated confidentially, such as incidents of sexual assault or abduction/kidnapping of NGO staff. Some information may be shared with those leading the network or forum to solicit additional information or support in managing the incident. While these incidents may have implications for the safety and security of other NGO staff working in the same operational area, it is vital to clarify what, if any, information on the incident can be shared with others. In some situations, it may be sufficient to alert members to the occurrence of a serious incident, without providing any details. In any case, the personal details of individuals involved should never be shared.

Further information

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

Storing and analysing incident data

The regular collection and analysis of incidents that occur in the operating environment will enable organisations to understand where, how and why the security situation is changing, and what this change means for the security of their staff, programmes and partners. Security incident data collated by local security networks can also be shared with incident analysis platforms such as **Aid Worker Security Database** and **Insecurity Insight** in order to contribute to the sector's wider analysis of aid worker insecurity.

Further information

- **Insecurity Insight SIIM Example Datasheet for Recording Incidents**
- **Insecurity Insight SIIM Classification of Incidents**

There are several off-the-shelf software packages and open-source tools that can be utilised to record and analyse incident data. However, simple spreadsheets to log key information from different incident reports may be sufficient for smaller networks.

Logging incidents

- **Identify your audience** – understand who needs what information and why. Is the information for NGO security colleagues or will it also be used by others – programme and advocacy staff or safeguarding colleagues etc.? Identify what information is needed and build the database accordingly.
- **Define an incident** – clarify which incidents should be monitored and recorded. Is it only incidents directly affecting NGO members, or broader events that impact aid access? Do you also include safety incidents such road traffic collisions and natural hazards, and administrative barriers, etc.?
- **Define an aid worker** – clarify whether to monitor and record incidents affecting only NGO members and their staff, or include NGO partners, UN agencies and/or other stakeholders.
- **Provide definitions** – provide a reference document with definitions for incidents that are recorded and shared. Make sure the documentation is clear and consistent.
- **Keep things simple and consistent** – create a basic spreadsheet to log the events. Use dropdowns for agreed categories to make it easier to capture information. Set fields to the desired format such as date, text or number and include additional fields for specific purposes, such as instant sharing or trend analysis.
- **Develop codes for information providers** – many organisations will want assurance of anonymity as a precondition for information sharing. However, you may need to trace information back to the original source if there are questions. Develop a code system to record the information provider that is anonymised but can be decoded if needed. Make sure to keep the information required for decoding in a safe place and restrict the number of people who have access to it.

- **Combine multiple reports into a master database** – encourage NGOs to share incident information in a standard format to enable a quick 'cut and paste' of information into the database. However, avoid creating any additional administrative burden to the sharing of incidents.
- **Build flexibility into the system** – plan additional fields that can be recorded later and consider how definitions will be applied to complex events.
- **Regularly clean the data** – despite best intentions there will be inconsistencies and inaccuracies in the data. Make a habit of regularly cleaning the data. Amend the definitions based on real-life examples to ensure consistency.

A challenge in maintaining any central database of incident data is the inconsistency in how organisations record and classify incidents. Some organisations may only record certain types of incidents, or two organisations may categorise the same incident in different ways, making it difficult to undertake cross-organisational comparisons.

Organisations within the network or forum can be encouraged to use standard definitions and classifications to help facilitate analysis. However, many will be working to their own internal classifications, therefore incident reports received will need to be assessed and, if necessary, re-categorised to ensure consistency with the database's parameters.

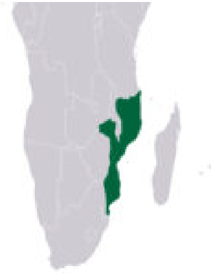
Analysing incident data

- **Detect patterns** – for different incident types (locations, targets/victims, timings, or behaviour/tactics of the perpetrators, etc). What are the similarities and differences in the incidents that have occurred? Why might these similarities or differences occur?
- **Consider trends** – either by specific geographic locations and/or during a specific time period. What are the key trends in the overall security situation? Does the data indicate any emerging trends that may affect the security of aid workers in future?
- **Describe changes** – explain the differences between the most recent data and previous analyses. What are the most significant changes, and why?
- **Identify actions** – suggest actions or specific measures that organisations should consider in response to the security incidents occurring.

Incident reports shared with the security network or forum may also omit useful information such as specific location information or details on staff affected, including their gender and nationality. It can require further dialogue with the organisation affected to clarify aspects of the incident and to determine what information can be shared or not with the wider network.

Maintaining a comprehensive database enables a security mechanism to provide more detailed analysis and produce regular reports highlighting trends in security incidents over a certain period, for example the type of incidents occurring, and their frequency, severity, location, and timing. Providing such analysis enables NGOs to develop a broader understanding of the risks, and adapt or strengthen their security approaches in response to these changes.

Collaboration examples



In the aftermath of two devastating cyclones (Idai & Kenneth) in 2019, the security situation in the Cabo Delgado region of Mozambique quickly deteriorated, with a sharp rise in violence perpetrated against the civilian population by militants. At the time there were no functioning security collaboration structures in place, and limited information and analysis on incidents.

Insecurity Insight was asked to provide regular threat analysis to organisations responding to the cyclone, as part of its Aid in Danger project. Insecurity Insight received verified security information and incident reports from its partner agencies and monitored local news media and social media, in collaboration with **Standby Task Force.**

Monthly threat analysis reports were shared through various NGOs networks at the local, national, regional and global levels.

During large scale emergency responses or in particularly challenging security environments, with many organisations involved, significant numbers of security incidents being reported, or sensitivities regarding the monitoring and reporting of security issues, it may be worth an NGO security network or forum seeking assistance from specialist organisations outwith the operating context to provide information on and analysis of incidents affecting aid worker security.

Disseminating information

Providing both real-time security alerts and weekly/monthly updates to members of a network or forum requires careful consideration.

Further information

- **Insecurity Insight SIIM Incident Alert Template** and **Example**
- **Insecurity Insight SIIM Weekly or Monthly Summary Report Template** and **Example**

Email distribution lists are sufficient for less time-critical information, such as security reports, but they are unreliable for sharing real time security alerts and threat advisories. SMS blaster services and, increasingly, online chat platforms are a much faster and more effective way to share information and alerts between members of a security network or forum.

The most suitable platform will depend on the location, quality of data network, number of organisations in the group, and the sensitivity of information being shared.

Sharing incident information

- **With whom** – will information only be shared amongst members, or distributed to other coordination platforms or external stakeholders?
- **When** – is the requirement for instant alerts to members, shared whenever an incident occurs, or aggregated incident data shared on a weekly or monthly basis?
- **Which format** – do members require text-based descriptions of individual events or analysis in the form of graphs and maps? Do you have capacity to geographically track and map incident reports?
- **Which platform** – will information/reports be circulated via online platforms (What's App/Skype etc), SMS, or email? Can other platforms be utilised, such as a dashboard or maps to present live updates?
- **Anonymous or known reporting** – are members comfortable sharing incident information directly with each other? Would they prefer to share information anonymously through a trusted intermediary, or to use technology such as reporting apps to enable anonymous reporting?
- **Who manages** – if using an online platform to record and share security incident information, do you have the capacity/time to manage the platform directly or will you require support from external specialised services?

In addition to members of the security network or forum, there may be other stakeholders and interested parties who wish to receive the updates and reports produced. For example, the HQ security focal points of NGOs that are not present in the country, but who have staff visiting regularly or are working through local partners, or other NGO security networks and forums within the region or globally. Consider with whom information should be shared and agree a protocol for sharing information with non-members.

4.3 Liaison and representation

Regular liaison with various security actors in the local environment, including national and international military forces or non-state armed actors, police forces, and private security companies, is a vital part of gathering security information, verifying reports of incidents and possible threats, and in some cases facilitating in-extremis support. However, given the number of NGOs in many humanitarian operations, security actors can be reluctant to liaise directly with each individual NGO, preferring to work through recognised focal points.

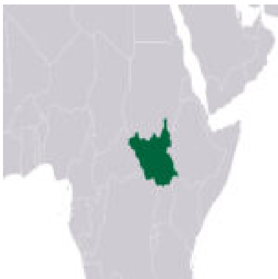
In other contexts, NGOs may be uncomfortable developing relationships with certain security actors due to the risks such cooperation may generate. NGO security collaboration mechanisms can help to centralise engagement, while also acting as a buffer for security liaison and information gathering between NGOs and various security actors.

NGO security networks and forums can also act as conduits for strengthening NGO-UN security relations, working directly with UNDSS and security staff from other UN agencies to facilitate the sharing of security information, and to highlight the security concerns of NGOs.

The existence of an NGO security network or forum is also a key requirement for developing formal relationships with UNDSS as part of the SLT framework and for NGOs to participate in UN Security Management Team meetings or other coordination meetings and events.

Despite the obvious benefits of regular liaison with different security actors, there are risks involved. Engagement and close cooperation with certain actors may undermine the security collaboration mechanism's independence in the eyes of some NGOs, the authorities, or other actors. All relationships must be carefully managed to ensure they remain transparent and impartial, and that there is no real or perceived compromise to the network or forum's independence.

Collaboration examples



In South Sudan, two NGO Safety Advisors were hosted by the Danish Refugee Council to provide security information, civilian-military liaison, advice and support, and training to NGOs working in and around the Malakal and Bentiu Protection of Civilian (POC) sites respectively.

The initiative was part of a wider programme to strengthen NGO security coordination and improve access within Unity and Upper Nile States.

The NGO Safety Advisers in both states represented the NGO community at the UN Areas Security Management Team (ASMT) meetings. The bi-weekly meetings included various UN agencies, including UNDSS, UNOCHA, UNPOL, UNHCR, and UNICEF, together with UNMISS Force Commanders.

4.4 Contingency planning and incident support

Ensuring timely and effective responses to a sudden deterioration in security or a natural disaster, being able to quickly relocate or evacuate staff to a place of safety, or getting staff in remote locations access to suitable medical care in an emergency, all require considerable planning and information gathering in advance.

Collaboration examples

In north-eastern Syria, several NGO security focal points collaborated on mapping medical facilities using Google Maps. NGOs working in different areas were asked to

add information on the location, capacity, and contact details for different health facilities to an online map.

The populated map was then circulated amongst NGOs to aid their contingency planning when expanding into new areas and to enable staff to quickly access information on the nearest medical facility in an emergency.

Security collaboration mechanisms play an important role in supporting members to prepare for situations which pose a significant threat to staff and operations. Often, simply bringing security staff together to discuss and share information on their respective contingency plans provides significant support to those organisations looking to develop or strengthen their own plans.

In some cases, NGO security mechanisms can also support the development of inter-agency contingency plans, in collaboration with UN agencies and IOs, for the potential evacuation, relocation or medical support arrangements for NGO staff in specific operational areas. While larger NGOs tend to have measures and support mechanisms in place to respond to critical incidents involving their staff, many smaller organisations do not and frequently reach out to NGO security networks or forums for support in the event of an incident.

In life-threatening situations, most security mechanisms will try to provide support to the member involved, especially in coordinating responses with UN agencies, or military forces and other security actors. However, the extent of critical incident support that can be provided to members will have limitations. It is important that these limitations are clearly explained in advance to avoid misunderstandings or unrealistic expectations.

4.5 Joint training initiatives

Training is a vital part of improving the security awareness and capacity of staff. With greater recognition of duty of care and the value of security training, many NGOs have established comprehensive security training programmes, or provide staff access to external courses run by NGO-focused security training providers in the major humanitarian hubs. In practice, however, the majority of NGOs struggle to resource and provide security training for their staff, especially for national staff who are most exposed to security risks in day-to-day operations.

Collaboration examples

In Libya, the **Libya INGO Forum** organised security trainings for international and national staff of INGOs. Trainings consisted of Personal Security Awareness, Hostile Environment Awareness Training (HEAT), and Advanced Security Management, together with access workshops and training for humanitarian drivers in hostile environments.

Trainings were in a mixture of in-person and online formats, and conducted in Arabic and English.

All trainings were by external providers selected through a competitive procurement process managed by the Libya INGO Forum's host, the Norwegian Refugee Council.

NGO security networks and forums play a significant role in improving access to training. Firstly, in identifying training opportunities through the UN SLT framework, or in liaison with external training providers*, and sharing information with members. Secondly, engaging with NGO security staff facilitating training at the national and local level to encourage organisations to provide access to other NGOs on these trainings, if spaces are available.

Pooling resources and collaborating with others to provide security training to staff and partners not only helps to reduce costs, but cross-organisational learning strengthens networking and information sharing which benefits security collaboration in the operating context.

Further information

- **GISF Security & Safety Training Pack**
- **GISF Training Hub**

In some cases, collaboration mechanisms have taken the lead in providing security training and capacity building events for NGO staff, for example by organising security workshops focused on specific security issues and challenges. However, maintaining a regular programme of personal security and security management trainings requires significant resources and is likely to be limited to larger platforms with sufficient staffing capacity.

Participation in joint security training and workshops is normally on a reimbursable basis, but if funding is available then subsided or free places could be made available to certain NGOs.

** GISF maintains a **comprehensive list of training courses** around the world, from crisis management training to personal security. All training providers have been recommended by at least two GISF member organisations.*

4.6 Collaborative action

When faced with increasing threats and restricted access, coming together as a group to raise concerns with authorities, communities or the wider humanitarian community is a vital role of NGO security fora.

Generating a collective voice on security concerns through common NGO positions and joint statements which unite organisations in the condemnation of a specific security incident or increasing risk to aid workers can have greater impact and lead to positive improvements in terms of security and access. However, it is important to note that advocacy is not limited to public statements, and often involves a mix of strategies that are less visible such as lobbying, building relationships, and influencing key stakeholders and decision-makers.

Collaboration examples

In response to a spate of security incidents affecting humanitarian aid workers in Ethiopia in March 2021 – including the killing of a GOAL driver and an incident during which Médecins Sans Frontières (MSF) staff in Tigray's Eastern Zone witnessed armed forces assault an MSF driver and execute four civilians – the Humanitarian International Non-Governmental Organization (HINGO) Forum issued a joint INGO **statement** condemning attacks against relief staff. The statement called for greater protection of aid workers, and for the attacks and killings to be investigated and those responsible to be held accountable.

Raising issues through a collaboration mechanism can also provide a degree of protection for individual NGOs – the mechanism is acting on behalf of all its membership without singling out any individual agency.

A security network and forum can increase the impact of advocacy efforts by drawing support from those members who are able to contribute expertise, time and resources to developing a statement and key messages.

Although collaborative action and advocacy can achieve positive results, it is not without challenges. Asking multiple NGOs, with different mandates and approaches, to agree to joint statements is a difficult process; it takes time, and sometimes compromise, to achieve consensus.

Further information

- **Toolkit: Responding to Violence against Humanitarian Action on the Policy Level**
- **ICVA NGO Fora Advocacy Guide**

A clear system should be in place for how joint statements are developed, reviewed and endorsed by the membership. However, some members will be reluctant to participate, for different reasons, therefore there should also be clarity on how the statements are issued without the involvement of certain members.

Developing joint advocacy statements

- **Identify the goal** – be clear on what needs to change or what parties need to do.

- **Seek consensus** – solicit support for overall key messages and circulate drafts to members for them to add input or raise concerns.
- **Explain the process** – statements should be developed through an agreed process**.** Clarify the approval process and what happens when a member does not wish to sign off on the statement.
- **Identify risks** – consider possible consequences for and negative reactions of different actors.
- **Prepare a media/communications plan** – provide members with additional information and talking points for use on social media.

5. Tools

- Tool 1 – Terms of reference (ToR)/charter template
- Tool 2 – Steering committee ToR template
- Tool 3 – Security coordinator/advisor job description template
- Tool 4 – Online group chat protocol template
- Tool 5 – Information sharing protocol template

For further information on NGO security collaboration and humanitarian security risk management be sure to visit GISF's resource library.