**Project Outline:** Security Risk Management (SRM) Policy Resource and Toolkit

***Background:*** Security risk management (SRM) in the humanitarian and development sphere has made noteworthy advancements over the past twenty years. For the most part, ad hoc field arrangements and questionable practices have been replaced by well-articulated security plans that follow a standardised typology covering all aspects of operational security. International NGOs have also made significant investments in building the capacity of their field staff while educating them on good practices of personal and organisational security. This journey has been supported by benchmark sector documents such as *Interaction’s Minimum Operating Security Standards (2006)(MOSS)*, the Good Practice Review, *Operational Security in Violent Environments, Humanitarian Practice Network (2010*) (GPR8), and several in-house GISF publications in the last decade.

***Current situation:*** Considering today’s approach to SRM in the sector, the MOSS and GPR8 could be considered outdated given the significant changes in the **a**. global and local humanitarian architecture, **b.** the operating environment, and **c.** the way modern non-profits are structured and managed. A new project (2022-2025) coordinated by Humanitarian Outcomes and implemented in conjunction with Global Interagency Security Forum (GISF) and the Humanitarian Practice Network (HPN) known as *Research for Improving Humanitarian Coverage, Operational Reach and Effectiveness (CORE)* aims at updating the *Good Practice Review, Operational Security in Violent Environments (GPR8) as well as producing a ‘state of SRM in the humanitarian sector’ report. V.3 of GPR8* will reflect the latest sector thinking and cover issues such as localisation, remote management, a person-centered approach, access negotiations, global epidemics, and more. It is anticipated the revised version of GPR8 will be published in 2024.

While this is a significant development expected to offer a great wealth of new knowledge, the document will still be oriented towards field operations to strengthen country offices and keep aid workers safe.

***Project Scope:*** With that in mind, GISF has recognised the need to develop a community of practice **SRM** **Policy Resource and Toolkit** as a higher-level strategic guide offering Headquarter Offices a pathway for recognising security as a business risk and linking with some of the most current sectoral debates and acting accordingly to identify effective and appropriate solutions.

Each of the suggested modules/ thematic areas will:

**a.** Introduce the debate reflecting the most current and informed discussions relating to SRM

**b.** Present the challenges and opportunities

**c.** Offer organizational pathways or else consideration options that will enable senior leadership to shape their policy principle for each of the thematic areas

**d.** Be accompanied by a technical toolkit as needed

While the primary users of the *SRM Policy Resouce and Toolkit* will be the staff with direct responsibility for developing and implementing the organisational SRM strategy at the HQ level, given the interdisciplinary nature of this product, senior leaders from other streams of work will benefit too. The toolkit part will include guidance on good practices and policy principles in the different thematic areas, and therefore, to ensure organisational and culture change, those with responsibility for SRM must also be able to influence board members, senior management, and other function leads, such as Human Resources, etc. Therefore, each module will target different groups, as appropriate, in a two-way relationship where SRM Strategic Plans address cross-cutting issues but also offer an opportunity to influence other organizational strategies presenting security as a business function.

This toolkit will be informed by the broader trends in the humanitarian and development sectors and lead with the foundational argument that a strong SRM culture and infrastructure equals quality programming in the long term. The project will take a modular approach, with a short introduction and a ‘how to use’ section followed by a series of modules.

***Project Audience:***The *SRM Policy Resounce and Toolkit's primary audience is senior staff responsible* for staff safety and security. This includes those with direct responsibility for developing and implementing effective SRM strategies and policies as well as senior leadership and management teams (SLT/ SMTs) and Board of Directors (BoDs). It is anticipated that while those at senior levels may have limited exposure to SRM, they will have an understanding of Enterprise Risk Management. Each module will include different sections targeted at the different audience groups, as appropriate.

**Overall Project Objectives**

The *SRM Policy Resource and Toolkit* aims to highlight key policy concepts while offering practical guidance to enable organisations to develop appropriate strategies to implement effective security risk management. While the primary audience is those responsible for the organisation’s SRM, the *Policy Resource and Toolkit* should also provide tools targeted at other key stakeholders who must participate in the process to ensure effective SRM can be developed and implemented, such as senior managers, the Leadership Team, and Board members.

Using a modular format, it is anticipated that content and tools will be updated as required over time.

**Document** **Outline**

This modular guide will use a dynamic format, including case studies, practical examples, and suggested tools. The proposed structure is for guidance only; additional thematic areas and modular re-structuring may be developed as required. Thematic areas (modules) could, for example, include the following areas of interest:

***Module 1 – SRM Strategic Development***

This module will act as an introduction to the topic of SRM, primarily in the humanitarian sector but also consider nuances for development and human rights-based programmes.

This module will introduce the basics of SRM Strategy development, explaining how the organization's vision, mission, size, program complexity, and overall organizational strategic objectives play a crucial role in defining organizational risk appetite and, by extension, influencing corporate SRM strategies.

*Multi-annual strategic plans* are nowadays prevalent among INGOs. Long-term organisational objectives are linked with their growth trajectory, which translates into increasing coverage, opening new country offices, or responding to emerging crises. Safety and security are not always included as a cross-cutting or even as a standalone component of these multi-annual cycles of programming, missing the opportunity to establish and mobilise resources

Acceptable Risk Threshold: For any successful security risk management strategy to be developed, the organisation must be able to identify and articuale what its acceptable risk threshold(s), who are the risk owners and where responsibility and decision-making lie.

***Module 2: Governance***

* 1. **Security and Enterprise Risk Management:** When security risk management is recognised as a critical element of an organisation’s enterprise risk management approach, it is easier to nurture an organisational security culture and encourage senior leadership’s buy-in and support. When, for example, SRM makes it to the Board of Directors’ Core Performance Indicator (CPIs) quarterly reports, it is then seen as a prerequisite for quality programming and organisational success. It is at this level that security risk management needs to be recognised as a business risk to find its space at the decision-making table to play a positive and constructive role in organizational growth.
  2. **SRM Governance Models:** While these can differ depending on the size of the organisation, volume and complexity of programmes, maturity of risk management approach, and staffing structure, it is important for the Senior Leadership Team (SLT) to recognise that SRM needs to be situated in a way that allows the organisation to achieve its programmatic objectives and mission statement. There is no one-size-fits-all proposition here, but this section should provide a framework for developing an approach that reflects the organisational need and can evolve along with the organisation.
  3. **Budgeting and resources** continue to be one of the main concerns for an organisations ability to implement effective security risk management. The problem is often two-fold, with security staff unable to create an appropriate budget to identify the direct costs associated with SRM, combined with proposal writers and finance staff who do not understand the need to include security costs, so SRM is considered to be an overhead, and then resources are cut. A project Vs. program budgeting and planning approach is worth discussing in this section.
  4. **Insurance:** while not a primary function for the safety and security responsible staff, it is important that they are engaged in the conversation when it comes to selecting “All Risks” insurance, as the designated ‘risk / first responder’ will play a fundamental role in any crisis response action, planning for which is usually the responsibility of the SRM team.

***Module 3: Staff Care***

* 1. **SRM and diversity, equity, and inclusion (DEI)**. While over the last few years, DEI has been recognised as an organisational priority with significant resources channeled to address systemic inequalities, raise awareness, and capacitate staff, the intersection with security risk management has received relatively limited attention. Organisational policies on SRM and DEI should reciprocally and concurrently discuss how these two concepts/functions come together and the benefits of a holistic approach.
  2. **Person-centered approach:** It can be said that inclusivity is at the heart of successful SRM. Organisations must take all reasonable measures to protect their staff from foreseeable risks, including those that emerge due to an aid worker’s personal characteristics, such as gender, race, ethnicity, religion, gender, disabilities, and sexual orientation. Security professionals need to have a comprehensive understanding of how personal identities and characteristics can impact personal security. This knowledge should be integrated into security policies and approaches to be inclusive and effective for all.
  3. **Duty of Care** is an important area within risk management practice for organisations wishing to better address health (physical and mental), safety, and security issues for their staff. While it sounds straightforward, it has many facets. Organisational policies need to fully delineate their approach from pre-departure to deployment and return from mission. Things can become more complicated for national staff and where the country's legal frameworks and systems are weak. As an interdisciplinary matter, organisations need to decide who is the custodian for the duty of care and how to ensure a comprehensive approach so that it doesn’t fall through the cracks. HR, legal, security, and fiduciary aspects need to be incorporated.
  4. **Many organisations recognise Mental Well-Being** as a growing area of concern. It is closely tied to security at many levels. **a**. If a person does not feel safe and secure, they will not function to the best of their ability, **b.** if stress builds up, they are likely to make decisions that can put themselves and others at risk. And **c.** when dealing with a serious incident or crisis, mental well-being will be essential for the responsible team, and psychosocial support will need to be built in.
  5. **Safeguarding:** Insecurity can lead to conditions where abuse and harm can occur. In many organisations, safeguarding is managed by a team distinct from the one responsible for SRM. However, whatever the structure, implementing solid and collaborative policies and procedures is critical to achieving the duty of care toward aid workers and enabling them to work safely and sustainably.

***Module 4: Coordination and Collaboration***

* 1. **Linking SRM with acceptance, humanitarian access, civil-military coordination, private military and security companies (PMSC), and counter-terrorism frameworks**. While country offices often apply an empirical approach in their operational doctrines, HQS need to have a clear understanding of the concepts, a clear position on how to engage, and increased awareness of the security implications that any given decision could have on the organisation. Civ-mil coordination, humanitarian principles and access are often under the auspices of the humanitarian advocacy or protection unit within an organisation; these departments do not usually actively seek to work with security-responsible staff, however, the need for proactive coordination and collaboration should be sought, and clarified at HQ level
  2. **Politicisation of aid, polarisation under a western-centric humanitarian system, and SRM**. Although most humanitarian NGOs abide by the principles of neutrality, impartiality, and independence, it is important for senior leaders to reaffirm their position given the complexity of modern contexts and especially given the overdependence on a handful of western donors. Engagement decisions need to be met with the necessary investments in SRM. The humanitarian imperative and access to hard-to-reach communities are often linked to corporate risk thresholds and appetite, however, little thinking goes into that.
  3. **Security in the digital world:** How can physical and digital security fit together in a world where cyber-attacks, social media defamation campaigns, and electronic frauds can quickly escalate and evolve into traditional security incidents? Are organisations well equipped to deal with such complex cases in a coordinated manner? How can we overcome internal silos and approach this from an interdisciplinary perspective? Which policy document will cover this part?
  4. **Cross-Sector engagement** is fundamental to good SRM. This is particularly true given the breadth of new threats to humanitarian security, such as shifting geopolitics and digital/cyber risks. To sufficiently address such risks, organisations must engage across the sector and coordinate with humanitarian, development, and human rights groups that have greater knowledge and experience in responding to these threats.
  5. **SRM and Global Advocacy Opportunity:** Traditionally, security is only included in advocacy efforts when talking about humanitarian access or in reference to the number of aid workers directly targeted in our line of work. Organisational commitment to advance aid workers’ safety and security could create engagement opportunities. Security in the humanitarian sector has a single-entry point to the global UN-led architecture. This is through the Saving Lives Together (SLT) framework, which could be used to influence donor policies and eventually increase funding for safety and security, which has traditionally been under-prioritized.

**Module 5: Localisation**

* 1. **Localisation and SRM:** Several global initiatives, including the Grand Bargain localisation work stream, aim to increase funding to local actors, improve their access, and strengthen their capacity. However, several security risk management challenges arise when looking at the localisation agenda. Localisation efforts may change the perceived neutrality, independence, and impartiality of international and local organisations, which could affect the security risks they may face. It is necessary to provide solid guidance to country offices on how to integrate SRM support into their localisation efforts.

***Module 6; Organisational Resilience***

* 1. **Organisational resilience and business continuity** are concepts that are gaining traction in corporate and non-profit environments, given the volatile world we live in. However, we rarely discuss what the term actually means. Safety and security have a significant role, from crisis management of critical incidents to fraud and corruption cases or global epidemics. We cannot consider the resilience of systems in isolation from the people we require to implement them. SRM professionals need to be at the table when organisational preparedness planning occurs. Resilience for organisations, teams, and individuals must be defined and referenced within SRM policies.
  2. **Monitoring, evaluations, accountability, learning (MEAL), and SRM audits:** Security audits are traditionally used to verify that current strategies are adequate, prove the organisation is compliant with established security policies and procedures, including Duty of Care, uncover operational security gaps and needs, and explore whether security training efforts are effective. It is always a struggle to monitor and evaluate a ‘negative,’ i.e. that there have been no security incidents. Going a step further, organisations should mainstream MEAL functions into Security Risk Management to ensure real-time adaptation and learning, but how can this be institutionalised? Consideration of non-traditional MEAL strategies should be considered.