gisf

UNOCHA/Antoine Lemonnier

Security Risk Management (SRM) Strategy and Policy Development: A Cross-Functional Guide

A GISF GUIDE FOR NON-GOVERNMENTAL ORGANISATIONS

Global Interagency Security Forum

About the Global Interagency Security Forum (GISF)

The Global Interagency Security Forum (GISF) is a diverse network of member organisations active in the fields of humanitarian aid, international development, human rights, and environmental protection, who value security risk management (SRM) as an important element of their operations and programme delivery. In a rapidly changing global landscape, GISF values the importance of continuous documentation, adaptation, and innovation of SRM policy and practice. Therefore, we take an inclusive approach to SRM and don't believe in 'one-size-fits-all' security. We recognise that different staff face different risks, based on the diversity of their personal profile, position, context, and organisation. In summary, we are the leading NGO SRM network and a one-stop-shop for information sharing, knowledge management, coordination, and collaboration.

Meet the Authors

Lead Author

Beth Chapman (International Location Safety)

Beth has 15 years of director-level experience in the operational delivery and management of overseas safety and security, including the role of Director of Programmes at International Location Safety (ILS). She has worked in partnership with many humanitarian, development, human rights and environmental NGOs to deliver safe and effective programme visits in complex environments, as well as supporting organisations to develop and implement strategic and operational SRM projects. She is a member of the BSI SVS/5 committee and BS8848:2014 working group and has a strong understanding of duty of care, enterprise risk management and security risk management and training.

Co-Authors

Nathan Toms (International Location Safety)

Nathan is a specialist in threat assessment, risk mitigation and building the capacity of NGOs, governments and security forces. He has held senior management roles in security management and programme operations in politically complex contexts, including Iraq, Ukraine and Nigeria. Nathan has nine years' experience as an officer in the British Army, and in senior management positions within international NGOs.

Hannah Eastwood (International Location Safety)

Hannah is a Senior Risk Advisor at International Location Safety (ILS), with extensive experience providing operational and strategic risk advice. She has previously worked as a Senior Threat Analyst for Crisis24 and for Palladium within the FCDO Office for Conflict, Stabilisation and Mediation. She has wide country experience, including in Papua New Guinea, Moldova, Ukraine, UAE, Rwanda, Kenya, and Indonesia.

About this guide

The aim of this resource is to act as a pathway to approaching security risk management (SRM) at a strategic, policy development and organisational level. It is not a 'how to' guide, or a 'one-size-fits-all' methodology. Instead, it aims to offer a conversation on some of the key issues facing SRM and provide senior leaders with subsequent areas for consideration on how to approach the development and implementation of SRM strategic plans. The resource also aims to provide guidance and support on how to improve communication, understanding and collaboration between SRM and other senior function leaders within an organisation. This guide is targeted at staff with direct responsibility for developing and implementing the organisational SRM strategy and policies at the HQ level, as well as senior leaders from other strategic level work streams.

Methodology

This resource was developed from 19 in-depth, semi-structured key informant interviews (KIIs). Participants included senior-level security managers from national and international humanitarian NGOs, key experts with experience in SRM in the humanitarian sector, and corporate and donor representatives. Five facilitated group workshops with senior-level security managers and two online surveys (with 23 strategic-level respondents and 29 operational-level respondents) were also conducted. An in-depth literature review complemented this information with a final peer-led review of the resource and toolkit.

Suggested citation

GISF. (2024) Security Risk Management (SRM) Strategy and Policy Development: A Cross-Functional Guide. Global Interagency Security Forum (GISF).

Acknowledgements

The ILS team has benefited hugely from the guidance and inputs of members of the GISF working group, comprised of leading subject experts and humanitarian practitioners working in the sector. Special thanks are due to Owen Dacayan, Neil Elliott, Noemi Munoz, Peter Walsh, Wahidullah Ahmadzai, and Toby Woodbridge for their expert insights and feedback. The guide also benefited from the input of SRM specialists outside the sector, whose time and knowledge we are immensely grateful for our colleagues at ILS and GISF provided significant input, support and quality assurance to the project. We are grateful to Lisa Reilly (former GISF Executive Director) who planted the idea for this publication. We would also like to thank Panos Navrozidis, Dimitri Kotsiras, Tara Arthur, Dan Ford and Shaun Bickley, for reviewing and commenting on the draft. Finally, we are grateful to the GISF teams who made it possible to present our initial findings at the 2023 GISF Autumn Forums in Madrid and Washington, D.C.

Moldova

A humanitarian worker conducts a survey with a refugee arriving from Ukraine.

IOM/Muse Mohammed

Disclaimer

GISF CIC is a limited company, registered in England and Wales with registered number 14937701. Our registered office is at Romero House, 55 Westminster Bridge Road, London, England, SE1 7JB. GISF CIC is a member-led organisation. While references to 'GISF CIC' in this disclaimer shall include GISF's members, observers, its secretariat, and administrative staff, the views or opinions expressed do not necessarily represent the views of donors or of GISF CIC's individual member organisations.

The information contained in this publication is for general information purposes only. The information is provided by GISF CIC and while we endeavour to keep the information accurate and complete, we make no representations or warranties of any kind, express or implied, about its completeness, accuracy, reliability or suitability.

Any reliance you place on such information is therefore strictly at your own risk. You should obtain professional or specialist advice before taking, or refraining from, any action based on the content of this information. In no event will we be liable for any loss or damage, including without limitation, indirect or consequential loss or damage in connection with its use.

This publication was produced by GISF through Awards No. 720FDA20GR00341 and No. 720BHA24GR00016, funded by the United States Agency for International Development (USAID) and through ChildFund International.

This guide is made possible by the generous support of the American people through USAID. The contents are the responsibility of the Global Interagency Security Forum and do not necessarily reflect the views of USAID or the United States Government.

Table of Contents

Acronyms

AI	Artificial Intelligence
BoD	Board of Directors
CINFO	Swiss Centre of Competence for International Cooperation
CMAG	Civil-Military Advisory Group
CMT	Crisis Management Team
CSR	Corporate Social Responsibility
DEI	Diversity, Equality and Inclusion
DoC	Duty of Care
GISF	Global Interagency Security Forum
ISO	International Organization for Standardization
KII	Key Informant Interview
KPI	Key Performance Indicator
MEAL	Monitoring, Evaluation, Accountability and Learning
NGO	Non-Governmental Organisation
NSAG	Non-State Armed Group
OCHA	UN Office for the Coordination of Humanitarian Affairs
PSEAH	Prevention of Sexual Exploitation, Abuse and Harassment
ROI	Return on Investment
SLT	Saving Lives Together
SOP	Standard Operating Procedures
SRM	Security Risk Management
ToC	Theory of Change
TRM	Travel Risk Management
UN	United Nations

Glossary

Business continuity: the strategic and procedural planning that an organisation undertakes to ensure that essential functions can continue during and after a disruptive event.

Crisis management: the planning, coordination, and execution of procedures and action plans designed to effectively navigate and mitigate the impacts of a crisis.

Duty of care: the moral and, in many cases, legal obligation of an employer to provide a reasonable standard of care towards its personnel, and to mitigate, or otherwise address all foreseeable risks that may harm or injure its employees, those acting on its behalf, or for whom it has a level of responsibility.

Enterprise/organisational risk management: the process of identifying, assessing, managing, and monitoring an array of risks across an organisation that could impact its objectives, operations, and stakeholders.

Organisational resilience: an organisation's ability to anticipate, prepare for, respond, and adapt to incremental change and sudden disruptions.

Programme criticality: a framework used for decision-making on acceptable risk, that ensures that the impact and needs of programmes and activities are balanced with the security risks.

Security risk management (SRM): the process and approach of identifying threats, assessing vulnerabilities and consequences, and mitigating risks related to the security of an organisation’s assets, information, people, and operations.

Introduction

A robust security risk management (SRM) strategy is critical for an organisation to meet its mission and vision. Embedding and nurturing a strong SRM culture goes beyond safeguarding staff, consultants, volunteers, and working with partner organisations; it serves as a catalyst for improved operational efficiency, stronger regulatory compliance, and increased stakeholder trust. Moreover, it establishes the groundwork for high-quality, innovative, and sustainable programming in the long term.

To achieve this, a good strategic approach to SRM requires an organisation to conduct an in-depth analysis of the organisational context and areas of work, to identify its strengths and weaknesses, to actively promote cross-functional collaboration between teams and departments, and to strengthen and enable all aspects of programmes and operations. It also requires a participatory approach, wherein the organisation continually assesses and adjusts its direction in response to internal feedback and changing external environments.

This resource has been developed to serve as a high-level strategic guide, positioning SRM as an organisational risk and offering comprehensive guidance on how to address cross-functional SRM issues and leverage them as an opportunity to impact and support broader organisational strategies, policies and functions. Those with responsibility for leading SRM must have the capacity to influence board members, senior management, and other functional leaders. By providing links to ongoing sectoral debates and best practices, this guide can help equip leaders with the tools to strategically present how the challenges of SRM can impact an organisation as a whole, ensuring the identification and implementation of effective and appropriate cross-function solutions.

Who is this guide for?

This guide has been developed for HQ/senior-level staff directly responsible for developing and implementing the organisational SRM strategy. It is also relevant for senior leaders from other strategic level functions to help them better understand the impact and relevance of SRM across all functions and themes.

How to use this guide

This guide has been designed to be used by both SRM professionals and those in SRM-adjacent teams, such as programmes/operations, HR, IT, finance, and legal. It provides tools and advice on how to integrate SRM across all functions within an organisation.

This guide follows a linear structure for developing an overarching SRM strategy and progresses to policy and implementation across various organisational functions. However, each chapter emphasises a specific focus area, allowing readers to navigate directly to the section most pertinent to their organisation's comprehensive SRM strategy:

- **Chapter 1** delves into the process for developing a strategy for security risk management (SRM) and ways to integrate it into the broader organisational strategy.
- **Chapter 2** focuses on placing SRM within the organisation's governance framework and ensuring leadership commitment.
- **Chapter 3** delves into the practical integration of the SRM strategy across various organisational policies and functions.
- **Chapter 4** looks at how to strengthen both internal and external strategic coordination and collaboration, including interagency security collaboration.
- **Chapter 5** explores building organisational resilience through an agile approach to SRM and enhancing preparedness for crises.
- Finally, **Chapter 6** addresses the integration of a monitoring, evaluation, accountability, and learning (MEAL) system within a comprehensive SRM strategy.

1

Chapter 1
SRM Strategy Development

2

Chapter 2
SRM Governance

3

Chapter 3
Cross-Functional Integration

4

Chapter 4
SRM Strategic Coordination and Collaboration

5

Chapter 5
SRM's Contribution to Organisational Resilience and Business Continuity

6

Chapter 6
SRM Monitoring, Evaluation, Accountability and Learning (MEAL)

Chapter 1: SRM Strategy Development

In simple terms, an SRM strategy is important because it aligns your organisation to a single goal in support of your vision and mission. Doing so can help increase transparency in your field operations, and make for easier decision-making at senior management level. In other words, an SRM strategy should play a key role in developing, and being part of achieving, wider organisational strategies and policies. Embedding the SRM strategy in this way is crucial not only to justify budget allocations, but also to gain engagement and buy-in from strategic leads across the whole organisation.

1.1 Essential elements of an SRM strategy

A typical SRM strategy is generally structured as follows:

- A foreword, ideally written by senior management, such as your CEO, Managing Director, or a Board Member, to champion your plan.
- The aim or mission statement aligned with the organisational strategy in support of the overall vision.
- Your principles and values (this should link to your organisation's risk attitude and approach to duty of care).
- A context statement (background to the current context your SRM framework will operate within – both internally (the organisational context) and externally (the operational context).
- Between three to six strategic objectives, themes, or goals which align with your organisational strategy (see Tool 1: Developing your Strategic Directions).
- Guidance for implementation and review (short, medium, long-term).
- You could also choose to include any assumptions incorporated into your plan, an outline of key stakeholders, and details of specific roles and responsibilities (see Chapter 2).

1.2 Embedding SRM within wider organisational strategies

Organisational strategies are often tied to a growth trajectory for the organisation, which can translate into increasing coverage, expansion of services (thus more staff), opening of new country offices, or responding to emerging crises directly or through partners. Safety and security are critical to ensuring these goals are met. But SRM is not always included as a cross-functional, or even as a standalone, component of planning for these multi-annual cycles of programming.

SRM should not be viewed as a separate discussion/approach or be brought in to 'safely and securely' operationalise an approved strategy. Instead, SRM should be used as an enabler for the organisation's strategic mission, vision, and objectives (see Tool 3: SRM Planning Template). A specific SRM strategy should demonstrate how it will help meet the organisation's long-term objectives, ensuring a good duty of care to staff, partners and associates, while maintaining a clear understanding of the organisation's risk attitude and thresholds (see section 1.5).

To integrate SRM seamlessly into broader strategic plans, it is essential to actively link your SRM strategy with all facets of the organisation's overarching approach. Fostering a good organisational culture and approach to SRM involves efforts to ensure that senior leadership understand the SRM strategy's goals and recognise their positive impact on the organisation as a whole.

To help highlight this connection, your SRM strategy should also use the same format, the same language, and the same structure as your organisation's multi-year strategy. For example, if your organisational strategy talks about 'strategic directions' or 'strategic themes', replicate these words and phrases in your SRM strategy. Ensure you clearly stipulate where SRM will help other functions meet their strategic objectives (and vice versa). For instance, if a long-term objective of your organisational strategy is to 'increase the number of national partners involved in programming', then specify how your SRM strategy, or specific objectives will help your organisation achieve this aim. As an example, this might look something like this: 'SRM will develop comprehensive due diligence procedures and prioritise resources to enable better support to national partners'.

Establishing goals and objectives with clear lines of accountability, as well as monitoring and reporting back on these goals to the wider senior leadership team, will also help to elevate and integrate SRM into strategic-level discussions (see Tool 2: How to rationalise your SRM strategy).

1.3 Understanding the operational environment and global trends

Any approach to developing a clear SRM strategy should begin with an in-depth analysis of the context in which the SRM framework is expected to operate in relation to the programmatic priorities. This should consider both the external (environmental) context and the internal (organisational) context.

The analysis of the external environment across the board should consider, for example:

- What relationships does the organisation have with external stakeholders and how important are these? What needs or requirements do these different stakeholders have around SRM?
- What laws, regulations, rules or standards apply to your organisation? How do these impact your legal duty of care requirements?
- What are the external trends around SRM? (These could include changes in expectations of staff around security risk management, partnerships and risk sharing, new technologies and innovations, or best practice trends within the sector).

The analysis of the internal organisational context should consider:

- What are the organisation's aims, programme priorities, structure and methods of operation?
- Who are the internal stakeholders and how are they currently involved in SRM? This should include delivery partners.
- What risk management processes/procedures are already in place? Are these currently effective?
- What is the legal structure of the organisation?
- What are the insurance policies and what external assistance provision does the organisation have in place?

Understanding the complexities of your whole organisation in this way will enable you to develop a relevant and practical SRM strategy.

Top tip: Systemcraft methodology for developing an effective SRM strategy

Systemcraft INSTITUTE

1. Set your strategy by focusing on collaboration.

SRM should not be siloed or seen as a technical skill that only those working in the space can understand. SRM links directly to providing good duty of care and ensuring business continuity and is therefore relevant to all functions of an organisation. When SRM works well, an organisation can remain focused on its mission and achieve better programme results. It is therefore in everyone's interest for SRM to operate effectively. Use this language and keep repeating it when discussing SRM. Enable easier collaboration through assessing what structures for sharing currently exist and use them. For example, if you already have an organisational risk management committee, ensure security is part of this.

2. Set a clear direction (zoom in/zoom out).

Any strategy needs to have a clear direction as well as both short-term and long-term actions and goals to enable people to connect and engage. Similar to embarking on a lengthy journey, consider the pursuit of a strategy as working towards a destination. There always needs to be designated stopping points on the way where you take a moment to pause, reflect and re-assess your objectives and actions before proceeding. Setting shorter-term goals to achieve your objectives (three to six months) as well as longer-term goals (two to three years) can be a useful approach to setting your SRM strategy.

3. Make it matter.

When forming a strategy, ensure it takes into account what matters to other members of the strategic leadership team. If people need to make changes or adapt, then they need to understand why it matters to them (and their teams/departments). Align your SRM strategy development cycle with the overall organisational strategic plan and resource mobilisation. SRM needs to be recognised as a key enabler for success, the same way that investments in new finance and HR software, workflows or capacity building, for example, are identified as pivotal to the success of a multiyear organisational strategic plan. Engage with other departments to discuss their strategic aims and concerns. Then communicate in plain language that can be understood by all and frame the conversation in a manner that resonates with their specific concerns and experiences within their function.

Top tip: Systemcraft methodology for developing an effective SRM strategy *continued*

4. Change the incentives.
Most systems already work to some extent, and often this can create a reluctance to change. Understanding some of the reasons why people do or don't engage with SRM strategies can help with creating and establishing new incentives. Sometimes this can be as simple as providing them with access to technology or applications (such as an incident reporting app) or simplifying some of the language or procedures so that they are easier to understand.

5. Harness collective intelligence.
Typically, those in senior positions of authority are the ones who develop and 'produce' SRM strategies, tailoring them for their 'consumer' (i.e. the rest of the organisation). This can lead to a disconnect between the ones setting the strategy and the ones who end up having to translate the strategy into operational reality. Organisations which have weak collective intelligence, such as poor access to field-level information and analysis, will typically reinforce a disconnect between strategic and operational approaches. Working towards a participatory approach, which harnesses collective intelligence from all levels of an organisation – particularly from those who operationalise SRM at field level – is key

Dr Simpson, K and Randall, I. (2020), Systemcraft: A Primer

Top tip: Fostering an agile approach to SRM

- ✓ Conduct a 'SWOT' analysis (see Tool 4 SWOT Analysis Template) – reflect on your organisation's Strengths and Weaknesses, as well as the Opportunities and Threats presented by the operating environment. Make sure to consider 'PESTLE' elements that are out of your control, but may impact your operations – Political, Economic, Social, Technological, Legal and Environmental factors.
- ✓ Conduct a backcasting exercise – reach a common understanding of the desired future endstate and work backwards by identifying waypoints to reach this desired outcome. Set 'SMART' (Specific, Measurable, Achievable, Relevant and Time-bound) goals and identify action areas. Ensure progress and feedback channels are maintained.

Top tip: Fostering an agile approach to SRM *continued*

- ✓ Ensure visions are aligned – strategic level staff must all be on the same page. Work to ensure that they use the same language, that reporting metrics are complementary, and that goals are common goals. Team objectives must align with function objectives, which must, in turn, align with overarching strategic organisational objectives.
- ✓ Prepare for conflict – cross-functional working brings together teams that may be traditionally siloed, which can result in people jostling for influence and resources. It is important to be prepared for conflict. This may mean giving cross-functional teams room to fail in order to make breakthroughs.
- ✓ Built in flexibility – an organisational SRM strategy must be relevant in all your operating environments, but it must not be a 'one-size-fits-all' approach. Flexibility is key: SRM strategies must be enabling, not stifling.
- ✓ Raise awareness – building awareness into onboarding processes and conducting regular training are easy ways to integrate cross-functional SRM into organisational culture.

1.4 Ensuring a common approach to risk management

Due to the interconnectedness of different risks, a well-integrated organisational approach should consider all areas of risk management instead of siloing risk into different functions.

Organisations should not separate or prioritise one risk over another, and SRM should form an integral part of an organisation's approach to risk management. When SRM is recognised as a critical element of an organisation's overall approach to risk management, it is easier to nurture a holistic security culture and encourage cross-functional senior leadership buy-in and support.

Developing an integrated organisational approach to risk should be a collaborative effort, harnessing 'collective intelligence' (see Systemcraft methodology) to assess the critical safety and security risks the organisation faces and the potential impact on an organisation's business continuity.

SRM should be at the front end of the decision-making process and a key part of any risk management planning cycle. Aggregating security risk information, presenting it coherently, and integrating the information into overall organisational risk management strategies is critical to informing policies and procedures and ensuring the adequate resourcing to mitigate these risks across the organisation.

Top tip: Embedding SRM within organisational risk management:

1. Use simple, non-technical language.
Remove overly technical references and explanations from conversations and presentations. Instead, focus on speaking about risk in terms of business goals and outcomes.

2. Link SRM to business continuity and crisis management planning.
SRM needs to be viewed as a preventative mechanism. It can help to identify, support and enable whole business objectives, whilst also highlighting possible safety and security issues and working with other departments to manage and mitigate these risks.

3. Information should be easily accessible.
Start by sharing real time information on potential external safety and security threats, and offer to help function heads to assess if and how these will affect their areas of responsibility. This includes helping them to determine specific triggers, establish mitigation measures and set risk thresholds.

Analysing and sharing internal safety and security trends is also critical to show value to other functions in an organisation. Sharing information and learning about your own organisation's incidents and near misses enables other functions to gain a tangible understanding of how and why safety and security risks matter to them.

4. Develop your awareness of risk triggers and quantify risk data.
Artificial intelligence has helped create many data information capture applications, which can pull reports of potential incidents and trends across locations and within different programmatic areas. Using these tools and the data they generate can help organisations support and inform qualitative risk assessments based on more subjective interpretations and provide a layer of more quantitative-based information.

5. Ensure accountability and awareness at a senior level.
While risk leaders are responsible for risk management, the board and senior executives are responsible for enterprise risk oversight. Work to ensure there is commitment and accountability from these leaders, or at least from one 'champion', to set the right tone and clearly communicate the importance of SRM throughout the organisation.

1.5 Setting SRM strategy based on organisational risk

A successful SRM strategy must be informed by the organisation's approach to risk, notably its (a) risk attitude (b) risk tolerance and (c) risk thresholds. These may vary greatly depending on an organisation's mandate, mission and operations, as well as donor requirements.

Key definitions

- **Risk attitude** is the amount of risk that an organisation is willing to accept to achieve its objectives.
- **Risk tolerances** are acceptable levels of variation in the organisation's risk attitude based on specific circumstances.
- **Risk thresholds** are the maximum level of exposure the organisation is willing to accept.

"The risk attitude (appetite) statement is generally considered the hardest part of any Enterprise Risk Management implementation. However, without clearly defined, measurable tolerances, the whole risk cycle and any risk framework is arguably at a halt."
Institute of Risk Management

Responding to risk can take many forms, with USAID identifying the following:

- Avoidance of risk by not pursuing a particular approach or not signing an agreement with a particular partner.
- Reduction of risk through a strong system of internal controls, targeted mitigation measures, or training and capacity building efforts, among other options.
- Sharing of risk through strategic partnerships with key stakeholders.
- Acceptance of risk without mitigation, with the appropriate safeguards.

Deciding on the balance between programme criticality (the process of determining an organisation's levels of acceptable risk to its programmes) and SRM can be complex and there is no 'one-size-fits-all' approach (see section 1.6 on how to develop a programme criticality framework).

Strategic leads and/or senior leadership should consider explicitly stating the level of risk the organisation is willing and unwilling to tolerate in pursuit of its mission and strategic objectives. This should align with its risk capacity, meaning the risk levels (tolerances) that it can sustain in relation to its operational footprint and resources, as well as its risk management capabilities and expertise.

This can take the form of a risk attitude statement (see Tool 5: Example Risk Attitude Statements) as well as defined organisational risk tolerance and thresholds beyond which they will not continue to operate (see Tool 6: Establishing Organisational Approach to Risk).

Top tip: The difference between risk attitude, tolerance and threshold

Think about the risks associated with driving. Organisations recognise that there is an inherent risk associated with driving, and the faster a vehicle travels, the greater the risk is. However, no organisation would insist on not travelling in vehicles at all or driving consistently at 10mph as this would mean they would never meet their destination, or strategic objectives.

Organisations therefore are prepared to accept some level of risk, but may reasonably put in place certain mitigation measures to help manage these risks. For example, wearing seatbelts or imposing speed limits would be mitigation measures. This approach to risk is often referred to as an organisation's risk attitude or appetite for risk.

In reality, however, there is typically some leeway where an organisation is prepared to flex. This is called risk tolerance. This is similar to how a police officer is unlikely to pull a driver over and issue a speeding ticket if they are going less than 10 per cent over the speed limit. Exceeding this tolerance level though, will eventually put a stop to any driving. This is the risk threshold.

Chapple, M, (2023): Risk appetite vs risk tolerance; how are they different, Tech Target

Establishing an organisational risk attitude statement specific to SRM can allow for more meaningful assessments of the risks that are relevant to achieving organisational aims. Without the framing provided by your risk attitude, it is harder for SRM teams to drive through actions when needed. Furthermore, staff throughout the organisation are left without the necessary information to make day-to-day decisions which align with the strategic approach to SRM.

Encouraging employees to take informed and appropriate risks, based on your organisational approach to risk (and tolerance/ability to flex where needed), can help break the perception of SRM as a 'blocker' to programme teams achieving their aims. Establishing a clear and consistent approach to risk which is well communicated and understood at all levels can cultivate better working relationships between the SRM function and the rest of the organisation.

Top tip: How to draft an SRM risk attitude statement

Set the context: Provide a brief explanation of how SRM risks relate to, and may impact, the overall strategy of the organisation, based on its mission, aims, objectives and operational context. Are there any external drivers that should be considered?

Identify boundaries: Specify clearly what there is zero attitude for, what there is cautious attitude for, and why in some circumstances there could be a higher level of risk attitude (e.g. donor requirements, high-risk programme locations). Risk thresholds can be visualised on a spectrum or by using an adapted Eisenhower decision matrix that ranges from 'Avoid', 'Cautious', 'Open', to 'Accept'.

Set indicators: Outline the key risk indicators that will be used to assess whether the organisation is operating within, close to, or outside risk thresholds. These indicators will also help determine a course of action regarding the management of different risks.

Donovan, L (2022), 'What is risk appetite and how do you implement it?', Risk Leadership Network

As risk attitude is often a qualitative measure, strategic leads should also consider how to communicate strategic-level risk attitude to staff across the organisation as well as to partner organisations. If SRM is seen as a participatory process across an organisation, involving not just security staff, this can prevent a disconnect between the decisions taken by senior management at headquarter level and those made by field staff.

Simple approaches to establish and operationalise risk attitude in regard to SRM and beyond:

- ✓ Posters with clear visuals on key risk thresholds, such as zero tolerance of sexual harassment or no driving after dark. These should include contact details if further guidance is needed.
- ✓ Clear lines of responsibility – who staff can go to for advice or guidance regarding risk attitude and thresholds.
- ✓ Alignment to risk attitude as a standing agenda item at programme planning meetings.
- ✓ Easy lines of communication when staff or partners need guidance. This could include regular risk review meetings, responsive guidance, dedicated communications channels or email addresses for queries and support.
- ✓ Inclusion of SRM policies, procedures and practices in new staff induction packages.

✓ A list (ideally no more than 10) of 'golden rules' which are easily translatable and give clear guidance on your organisation's risk thresholds and any specific 'hard stops'. These should be adaptable to different contexts and easily understood by partner organisations and staff at all levels.

1.6 Balancing programme criticality with SRM risk attitude

The humanitarian imperative and the need to gain access to hard-to-reach communities are key drivers within the NGO sector. They can often push the boundaries of organisational risk attitude. However, programmatic criticality needs to be balanced against the potential safety and security risks and the impact this could present to an organisation from a business continuity perspective. For example, staff fatalities may affect reputational value and translate into financial damage if donors withdraw.

Determining how to balance meeting the overarching strategic objectives of an organisation with the potential security risks is critical. A 'programme criticality framework' can provide a structured process to this decision-making. It can also help an organisation weigh the residual risks against commitments to humanitarian principles, particularly those guiding who the organisation assists, and the principles of humanity and impartiality.

Top tip: Tools to balance programme criticality and security risk assessment

The Programme Criticality Framework is a United Nations (UN) system for decision-making on acceptable risk. It puts in place guiding principles and a systematic structured approach to ensure that activities involving UN personnel can be balanced against security risks.

UN Programme Criticality Steering Group (2016), United Nations System Programme Criticality Framework, CEB/2016/HLCM/23

Security risk managers are often tasked with making decisions or providing advice to programme and operational teams once a programmatic strategy has already been developed and approved. Instead, SRM should filter into strategic discussions around risk attitude at the planning stage. The information on and analysis of security risks should be part of any decision-making on activities and programmes.

Forming a cross-functional risk management committee, with an SRM presence, is an excellent way to manage this. The committee should meet regularly to discuss emerging risks, threats and concerns and have the authority to make decisions. For example, the committee could decide on whether a new geographical or technical area of programming meets or exceeds the organisational risk attitude approach as a whole. See Chapter 2 for more.

Useful Resources

- Systemcraft Toolkit – A Primer
- Strategic Planning for NGOs: A guide to understanding the basics of strategic planning
- How to do Strategic Planning: A Guide for Small and Diaspora NGOs – INTRAC

Syria
Researchers with Amnesty International collect evidence of airstrikes. Gaining access to dangerous areas like these can push the boundaries of an organisation's risk attitude.

Chapter 2: SRM Governance

Good governance and accountable structures are the backbone of any effective SRM framework. Staff at all levels within an organisation bear a degree of responsibility for their own security. But organisations are responsible for ensuring that effective governance structures are in place and that staff are aware and understand their roles and responsibilities within this architecture.

SRM governance implies that an organisation actively exercises controls over the risks it faces and provides direction for the security of its organisation. While working in complex and constantly changing environments, organisations, regardless of size, mission complexity and operational footprint, should ensure they have an appropriate governance structure.

2.1 Placing SRM within the organisational risk governance framework

SRM must be placed within an organisation's risk management architecture, so it promotes a positive culture that filters through the whole organisation. This will differ depending on the organisation's size, risk attitude and programme delivery. But the key to success is ensuring that its positioning is correct for the organisation.

Organisations must decide who is the ultimate custodian for each aspect of the SRM strategy and how to ensure an integrated approach to managing this within its over-arching duty of care framework so that nothing is neglected or missed. Organisations should consider using a RACI matrix to help them to break this down.

Top tip: RACI matrix

The acronym RACI stands for:

- **R** – Responsible
- **A** – Accountable
- **C** – Consulted
- **I** – Informed

Top tip: RACI matrix *continued*

Responsible

These people are the 'doers' of the work (functional managers). They must complete the task or make the decision. More than one person can be jointly responsible.

Accountable

This person is the "owner" of the work. They must sign off or approve when the task, objective or decision is complete. This person must make sure that responsibilities are assigned in the matrix for all related activities. There is only one person accountable, which means that the accountability cannot be passed to someone else.

Consulted

These are the people who need to give input before the work can be done and signed off. These people are involved and active participants.

Informed

These people need to be kept aware of what is happening. They need updates on progress or decisions, but they do not need to be formally consulted, nor do they contribute directly to the task or decisions.

The people responsible can be identified through the development of your organisation's Strategic Directions (as seen in section 1.2).

UNMAS South Sudan

South Sudan

A staff member wears protective equipment while working to remove landmines. Although organisations must ensure effective safety and security protocols are in place, staff also bear some responsibility for their own wellbeing.

An example for an SRM RACI Matrix may look like:

Task/stakeholders	All staff	In-country security focal point (SFP)	Country/ Regional Director	Global Security Manager	Risk Management Committee	Other function leads (e.g. Programmes, HR)	CEO/ CFO/ COO	Board/ trustees
Task 1: Endorse global safety and security policy	I	C	C	C	R	C	A	I
Task 2: Set risk attitude threshold	I	C	C	C	R	C	A	I
Task 3: Develop/ implement SRM framework (country S&S plans, security briefs, incident management plan)	C	R	R	R	A	I	I	I
Task 4: Develop travel risk management policy	I	C	C	R	R	C	A	I
Task 5: Develop organisational crisis management plan	I	C	C	C	R	R	A	I
Task 6: Building capacity through training on SRM	I	R	R	R	A	I	I	I
Task 7: Review incidents, set follow-up actions, and share lessons learned	I	R	R	R	A	I	I	I
Task 8: Review SRM policy and framework	I	C	C	C	R	C	A	I

RACI

● **R - Responsible**
The people who take action to get the task done. They are responsible for the work or making the decision. You can have more than one person responsible for a task, but to make the decision-making process effective, try having one person responsible for a single task.

● **A - Accountable**
The person who owns the task or deliverable. They might not get the work done themselves, but they are responsible for making sure it is finalised. To avoid confusion and the diffusion of responsibility, it's better to have one accountable person per project task.

● **C - Consulted**
The person, role, or group who will help complete the task. They will have two-way communication with the people responsible for the task by providing input and feedback over the task completion.

● **I - Informed**
The people, roles, or groups that need to be up to date on the task's progress. They will not have two-way communication, but it's essential to keep them informed since they will be affected by the final outcome of the task/project.

Adapted by International Location Safety from template provided by Academy to Innovate.

Understanding the risk management governance architecture of the organisation in this way enables you to ensure that all aspects of SRM are assigned and incorporate where other functions should also be involved and in what capacity (e.g. programmes, human resources, legal, and fiduciary). These links are expanded in Chapter 3.

Whilst ensuring a cross-functional approach to SRM, it is also important to consider an inclusive and participatory approach. To promote a culture of SRM, all key stakeholders need to be engaged. This engagement will provide the operational realities of the possible consequences of these policies, empower the people delivering the organisational aims and promote a positive, sustainable culture around SRM.

2.2 Building an Effective Safety and Security Structure

The structure of an organisation's safety and security function can vary based on factors such as the organisation's size, the volume and complexity of its programmes, the maturity of its risk management approach, and its staffing structure. Therefore, it is crucial for senior leadership to ensure that SRM is positioned in a way that enables the organisation to meet its programmatic objectives and mission. This involves integrating SRM into the risk management governance framework, giving it a significant role in decision-making processes.

All organisations, regardless of their structure, should consider having a cross-functional working group, committee or steering group representing different roles and levels within the organisation. Those on the committee should be identified across different functions with core responsibilities defined within the SRM RACI matrix. This collective approach encourages a greater sense of ownership, which ultimately aids implementation and compliance (see Tool 7: Example Terms of Reference (ToR) for Risk Management Committee).

Some organisations have an entire department dedicated to safety and security, whilst others incorporate it within other functions. Regardless of the structure, the key considerations for an organisation are:

- Can our SRM strategy be appropriately resourced (both human and financial) within our current structure?
- Do we have the appropriate knowledge of safety and security among positions with SRM responsibilities?
- Do we have an appropriate culture within the organisation to ensure our strategy is implemented effectively?
- Do we have the necessary soft infrastructure and hard infrastructure to support the implementation of the SRM strategy? Soft infrastructure can include human capital, comprehensive trainings, a solid policy framework, and agreements with third party providers. Hard infrastructure can include communication devices, personal protective equipment, and secure office compounds.

If the answer is no to any of these questions, then the organisation should seek to either re-structure or upskill its employees to ensure it is performing effectively.

Regarding the structure, there is no 'one-size-fits-all' proposition here. But there are some key considerations that need to be taken concerning organisational needs, which can evolve over time. There are three common structures used by organisations:

- Structured security positions
- Embedded security responsibilities
- External security providers.

Choosing the right people, in the right roles, to lead on security is the key to an organisation's success. Examples of different roles include:

Structured security positions

Dedicated SRM individuals positioned at key levels within an organisation who have roles and responsibilities dedicated solely to SRM. This can be at the global, regional and/or country level. These positions do not necessarily have to be at all levels but where there is the greatest need.

Pros: Allows experts in SRM across the organisation to develop, implement and assure SRM frameworks. Provides clear lines of responsibility and accountability for SRM within an organisation.

Cons: Does not always ensure a positive security culture. Security departments can become siloed, so this approach needs significant effort to ensure collaboration between SRM departments and other functions as well as ensuring a collective sense of awareness and responsibility. The most important element is for leads to recognise the need for active security risk management as part of effective programme delivery.

Embedded security responsibilities

Some organisations do not have resources, or simply prefer to embed security responsibilities within other roles.

Pros: If strong SRM frameworks are in place, and individuals are given time, support and training, then this provides an excellent opportunity to empower individuals and create a positive security culture which is well-integrated within the organisation structure.

Cons: Embedding security responsibilities relies on ensuring that the individuals identified have both the knowledge and understanding of SRM as well as the capacity to carry out these responsibilities alongside their other duties. Often organisations fail when trying to embed SRM responsibilities by not ensuring enough time, support or training for staff.

External security providers

Some organisations contract external security advisors, either to act as the sole representatives for SRM within their organisations, or to support other functions which do not have the capacity or technical skills to manage SRM.

Pros: External security providers can bring broad experience and connections into wider SRM networks, as well as knowledge of best practice across the sector. They can also provide a useful external view and non-biased perspective which can be helpful when tough decisions need to be made, or for external reviews and associated recommendations.

Cons: External providers do not necessarily have (or need time to develop) the embedded knowledge of the organisation and its structures and cultural approach to SRM. They can also lack the internal relationships and connections which can be essential to implement and roll out SRM frameworks. Notably, an overreliance on external providers can diminish responsibility, and ultimately undermine in-house capacity and institutional knowledge.

2.3 SRM Roles and Responsibilities

Roles and responsibilities around SRM should be clearly defined, demonstrating who is responsible for providing security advice, and who makes decisions. Using the RACI matrix and understanding how as an organisation you wish to structure security will enable you to effectively establish the roles and responsibilities.

Top tip: Consideration of job titles

If, as an organisation, you consider that there is a need to have dedicated security staff, special attention needs to be paid to job titles.

Security Advisor
Provides structured advice to guide the decision-making processes of others.

Security Manager
Manages organisational security, including day-to-day decision-making.

Safety & Security Director/Chief Security Officer/Vice President for SRM
This position is part of the leadership team and has access to the Board of Directors (BoD). It ensures security is part of the organisational risk framework and contributes to the quarterly BoD Key Performance Indicators (KPIs).

The job title can dictate the level of influence the individual has, particularly on programming activities, unless clearly stated. This has been known to cause organisational challenges due to conflicts between security and programming departments. Whilst this is also personality driven, the job title and clear roles and responsibilities lay out how the organisation achieves its SRM. Also worth considering is the geographic scope of each position. You might incorporate terms like 'national', 'regional', or 'global' into the titles listed above.

Organisational responsibilities

In addition to outlining staff roles and responsibilities, policies also need to clearly state the organisation's responsibilities to staff from a duty of care perspective (including national staff where the country's legal frameworks and systems may be different). Organisations must clearly understand and communicate their legal and moral duty of care responsibilities to staff, consultants, volunteers, and partner organisations.

There will always be grey areas, so policies should be less about setting rigid boundaries and more about who ultimately makes decisions and what remit they are working within (see section 1.5 on Risk Attitude and section 3.8 on Linking to Legal).

Key to success is the recognition that having senior level and leadership engagement is critical. But, for SRM to thrive, everyone in the organisation must accept a level of responsibility for their own safety and security.

Useful Resources

- GISF Security Risk Management A Basic Guide
- Mind Tools: How to create a RACI

ChildFund/Jake Lyell

Kenya
Staff with ChildFund International visit a rural village in Kenya. Different staff members should have clearly defined SRM roles and responsibilities, which can also include child safeguarding.

Chapter 3: Cross-functional integration of SRM and policy development

A successful SRM strategy hinges on cultivating a shared sense of awareness and responsibility among senior leadership, and across various key functions of an organisation. This ensures that SRM is integrated in all aspects of the organisation's planning and activities.

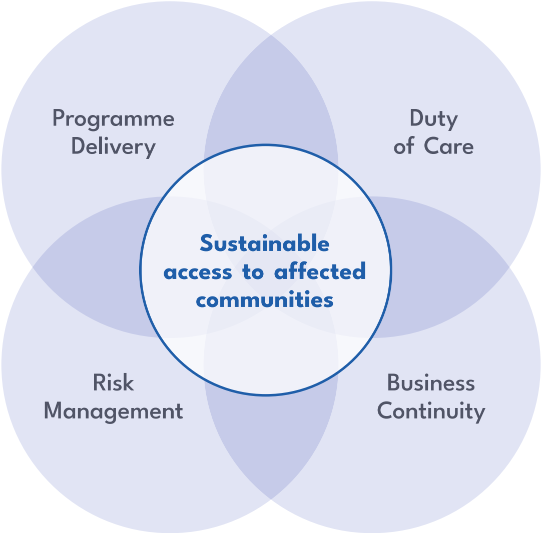
On the one hand, senior leaders can play a pivotal role in championing SRM and emphasising its strategic importance throughout the organisation. However, to ensure the effectiveness of SRM efforts, it is critical for all functions within an organisation to understand the significance of SRM to their specific roles and responsibilities (see Chapter 1). Everyone must also recognise the potential negative impacts, including the cost of incidents, if SRM is not considered in their own strategic planning.

> *"Other departments need to understand the security implications of their activities and decisions."* (KII Participant, NGO SRM strategic lead).

Different organisations may choose to approach these collaborations between strategic functions in different ways. For instance, they may facilitate working groups, one-to-one meetings, online messaging channels, shared reports, or internal cross-referencing between policies. No matter what, the critical element is understanding and clearly presenting how SRM intersects with each function to ensure long-term organisational resilience.

3.1 Establishing why SRM matters

To enable other strategic functions to see why SRM matters to them, it can be helpful to link SRM back to four core pillars of organisational resilience:



These four elements are not always widely understood across all departments. But they should be used as the common ground from which to demonstrate how SRM matters to all functions and how it connects with other risks, such as:

- Accessing communities in need and delivering the necessary assistance.
- Increasing general productivity by providing a structured and secure work environment.
- Providing assurance to donors and funders of stable, well-managed and effective programming, which can increase the chance of re-investment.
- Protecting personnel, data, intellectual property and assets.
- Reducing legal and financial exposure.
- Enabling operations/programming to access high-risk locations.
- Enhancing an organisation's reputation and credibility, which in turn can have a positive effect on competitiveness, staff turnover and talent acquisition.
- Improving staff confidence and psychological and physical wellbeing.
- Contributing to business continuity capability and organisational resilience.
- Demonstrating the organisation's ability to control its safety and security risks effectively and efficiently, which can help in lowering insurance premiums.
- Establishing more effective processes for crisis management. (Adapted from IEC 31010:2019: Risk Management: Risk Assessment Techniques).

The box below shows specific areas where SRM strategy directly links to other functions to support good programme delivery, provide duty of care, strengthen risk management, and ensure business continuity. These examples can provide suggested starting points for conversations between SRM leads and senior leaders in other functions of the organisation.

Table 1: Mapping connections between SRM and key organisational functions

Programmes/ operations	• Access and safe delivery of services • Programme planning • Changing operational environments • Changing funding environments • Access to partners and project sites • Contingency planning (evacuation/hibernation/relocation) • Security in digital environments, including new software and hardware in programmes and operations • Support to partners (duty of care, risk attitude/transfer, localisation)

Table 1: Mapping connections between SRM and key organisational functions *continued*

Finance	- Minimising loss of assets (people/resources) - Fraud and corruption (lack of access and oversight) - Resource management - Contingency funds (centralised or project-specific) - Cost of safety and security incidents (direct and indirect) - Insurance provisions
Communications	- Disinformation/misinformation - Social media threats - Internal communications around SRM - Reputation - External advocacy - Visibility and branding
IT	- Cybersecurity threats - Digital surveillance - Network and information security - Data backups
HR	- Diversity, equity and inclusion (DEI) - Mental health and wellbeing - Capacity building - Recruitment and retention
Legal	- Establishing duty of care - Due diligence - Working with partner organisations – contracts, local jurisdictions, context-specific regulatory processes
Safeguarding	- Safety of staff and beneficiaries
Travel	- Travel risk management - Context analysis - Authorisation and approval - Traveller tracking/monitoring - Evacuation/relocation
Advocacy* **discussed in Chapter 4*	- Civil-military coordination - Humanitarian access - Private security and military companies - Use of armed escorts - Use of convoys

3.2 The importance of agile SRM

Without good cross-functional workflows, communications and information-sharing, there is the risk that the department receiving notification of an incident or change in context will interpret that information through their own lens. They might also neglect to share this with other strategic leads, which risks further escalation or an increasing impact of the incident.

As demonstrated in Chapter 1, ensuring senior management understands how SRM strategy directly links to other internal functions is an excellent way of developing an agile approach to SRM. This ensures the whole organisation is aware of possible threats to business continuity.

3.3 Linking to Programmes/Operations

Programme teams are at the forefront of driving forward the organisational mission. They are often under pressure to achieve key strategic goals and objectives. Programme criticality therefore plays an important role when considering security risks and understanding SRM as an enabling function (rather than blocker). It is an essential component of integrating SRM into programme operations.

Programme planning

Silos can develop when SRM is perceived to be an obstacle to achieving programme objectives. These challenges often arise when SRM is not included during the early development stages of a programme and is instead viewed as the final requirement prior to programme approval. Challenges might also arise when SRM is seen exclusively as a reactive incident support function.

SRM leads should work closely with programme leads when developing their respective strategies. This will help the programme staff to recognise the benefits to integrating SRM. For example, SRM teams can work alongside programme teams to identify when planned activities/locations may risk getting close to organisational risk thresholds, and prepare and mitigate for these risks together.

SRM leads should share their analysis and understanding of global, regional and national contexts and operating environments with programme teams. In turn, they should use feedback and input from programmatic staff, including local staff. This can help contextualise and localise SRM processes instead of relying on a top-down or 'one-size-fits-all' approach. This will support programme teams by providing practical and realistic advice on how to achieve their aims safely and securely. It can also help integrate new SRM approaches and technologies into programme plans.

SRM and programme leads should share the objective of safe and secure delivery of programme activities. SRM leads need to clearly frame that the goal is to empower programme teams to achieve their safe and secure programming. SRM is not a blocker. It is there to facilitate long-term, sustainable programming. It is also important that these conversations and decisions are guided by the organisation's strategic approach to risk attitude and tolerance.

Programme delivery and humanitarian access

Access constraints can be physical or bureaucratic, with the UN Office for the Coordination of Humanitarian Affairs (OCHA) listing the following as the most common constraints to accessing affected populations:

- Bureaucratic measures that delay, stall, or interfere with humanitarian operations.
- Misinformation and disinformation discrediting humanitarian actors.
- Sanctions and counter-terrorism measures that impede payments of fees, purchases of commodities or supplies of goods.
- Intensity of hostilities and explosive ordnance that impede humanitarians' movement.
- Attacks on humanitarian personnel and facilities, and theft of assets.

'Acceptance' is a key security and access strategy. It refers to the willingness of beneficiaries, local authorities, belligerents and other stakeholders to receive humanitarian and development NGOs into their communities. NGOs should actively cultivate and maintain consent from local stakeholders to enable continued acceptance. This in turn will support NGO access to vulnerable populations and allow them to undertake programme activities.

However, acceptance is increasingly coming under threat due to the erosion of civic space in many contexts. Increasingly, governments are accusing (I)NGOs of undermining national security or having political, cultural, or religious values that run counter to national interests. If an organisation is perceived to be aligned with any political or military objective, this can put staff lives at risk and further restrict their access.

Expert opinion

"For many NGOs, acceptance is the bedrock of good security practice. Any threat to acceptance should therefore be of concern to NGO security staff."
Morrow, E. (2023) 'Humanitarian Access & Security Management: considerations for staff security'

Programme and SRM leads should work closely to develop their strategic approach to access. This is particularly important in situations where the humanitarian principles of neutrality, impartiality, and independence are not an option or risk being compromised. For instance, this might include programmes focused on advocacy or supporting human rights. Moreover, an explicit link at policy and strategic levels between access and SRM is important to safeguard the sustainable delivery of services to hard-to-reach communities.

Top tip: Achieving effective strategic SRM within programme planning

1. Share, triangulate, and analyse access constraints internally

Understanding the types, drivers, and impacts of access impediments is the first step to addressing them. Consider establishing an internal strategic-level working group comprising programmes, security, operations, advocacy, and communications leads. Together, this group can identify constraints, analyse and mitigate risks, develop organisational access strategies, and establish red lines (risk thresholds) and organisational positions.

2. Train staff and create a culture of sharing and escalation pathways

Security staff can be crucial in strengthening communications, providing training, and encouraging information sharing. They play a key role in shifting organisational culture from 'implementation at all costs' to encouraging more reflective and strategic engagement on access issues. For organisations without dedicated access staff, clear pathways need to be outlined for staff to escalate internal and external issues. Security staff can support or lead on risk analysis related to access issues and assist with developing and disseminating internal policies and standard operating procedures.

Top tip: Achieving effective strategic SRM within programme planning *continued*

3. Be proactive in building relationships and understanding

Building relationships with government authorities and non-state armed groups, where present, is vital to acceptance. While it can be appropriate in some contexts, operating 'below the radar' is rarely a viable long-term acceptance strategy. Building relationships and networks is a vital skill for security staff and can be a valuable resource to guide staff engaging on access issues.

4. Engage the humanitarian community for a safer response

When faced with access impediments or security issues, all NGO security staff need to ask themselves the question – does this issue impact just my organisation, or could it impact other NGOs and people in need? In many cases, the answer is the latter. In these instances, access challenges must be shared and discussed (carefully) with other agencies to triangulate information, manage risks, and identify common positions before engaging with counterparts. This is critical to promoting acceptance of humanitarian action and staff safety.

Source: Morrow, E (2023) Humanitarian Access and Security Management: considerations for security staff.

Useful Resources

- Frontline Defenders Workbook on Security
- GISF Security Toolbox – Acceptance Analysis
- GISF Achieving Safe Operations Through Acceptance
- Save the Children: The Acceptance Toolkit

3.4 Linking to Finance

There are inevitable costs associated with managing safety and security. Developing and rolling out a comprehensive approach to security risk management can take significant financial resources. Costs associated with safety and security risk management need to be introduced in the early stages of planning. It needs to be communicated that they are an integral part of the programme design, necessary for its sustainability and success. In addition to effective resourcing of security, it is important to appreciate the potential financial impact associated with a security incident and to ensure adequate recognition at the strategic level of insecurity as an enterprise/business risk.

Security incidents can impact on many other areas of an organisation. For example:

- Additional internal/external staff to handle the incident/follow-up.
- Extra PR to repair brand damage.
- Additional training.
- Pausing programme operations during a security incident.
- Fraud and corruption cases resulting in direct financial loss.
- Potential loss of donor funding due to an incident.

Collaboration between finance and SRM leads is therefore essential to develop a more prepared and resilient organisation.

Minimising loss of assets/resources

Discussions relating to budgets can be particularly difficult for security professionals. In most functions, it is possible to present a clear, predictable return on investment (ROI). However, effective security-related expenditure is often about preventing or minimising a loss, rather than achieving net gain, which is far harder to quantify to financial decision-makers.

SRM leads should demonstrate the size of each risk and the potential costs, losses, and other repercussions if they're not mitigated by security systems and processes. This could relate to preventing fraud or corruption. It can also link to other risks with no direct monetary cost, but which can still have a dramatic effect on the bottom line. For example, a security breach can lead to reputational damage that affects donor or staff loyalty and causes a drop in funding or staff retention. Or if an organisation lacks access, the gap in oversight can lead to a vacuum where damaging activities can take hold.

Resource mobilisation, allocation and management

Effective long-term resource mobilisation, allocation and management must include consideration of safety and security. Traditionally, safety and security is one of the first areas to be impacted by reduced revenue. It is also often treated as a 'gap filler' budget line for other support functions. SRM-related resources are required to enable and support programme teams to meet long-term organisational strategic objectives.

> *"The opening of new field offices should not be considered unless there is enough funding to cover for the Minimum Operating Security Standards as stipulated in the country level security plans."* - KII interviews

It is critical to make the most efficient use of resources by eliminating waste and producing a higher ROI. If not properly invested in, maintained and managed, safety and security resources can become a drain on finances or risk a bigger outlay by having to 'fix' a problem once it has occurred, rather than planning and mitigating for it in advance. For example, investing in regular vehicle maintenance and driver training is more efficient and cost-effective than waiting for vehicles to break down and having to provide emergency transport or expensive last-minute repairs.

The ROI of strengthening organisational resilience is also a metric that most finance departments would be interested in. Security awareness training can help the organisation save money by lowering the chance of a security incident occurring due to human error.

How to cost and finance SRM

GISF's resource 'The Cost of Security Risk Management for NGOs' details how value for money is often one of the key objectives for not-for-profit organisations. There is a general perception that the lower the non-programme costs, the more competent the organisation is in allocating the majority of funding to direct programme expenses. However, spending most of a donation on programme costs does not necessarily mean that the programme is meeting its stated objectives or is being conducted in a safe and secure (and therefore sustainable) manner.

Another common practice is to allocate a percentage of the total programme budget to risk management costs. However, attitudes and assumptions about what is considered an 'acceptable' percentage vary widely across the sector. On the other hand, treating risk management as a generic non-programme institutional cost means that it is often reduced to the lowest possible level, both to be more acceptable to donors (as an indirect cost), and to be viewed positively by eternal bodies, such as auditors.

Aligning with annual budgeting cycles is important for the timely allocation of necessary resources. It is also essential to work with finance teams to develop the necessary departmental methodology (that requires its own attention). And advancing the appropriate managerial skillsets among SRM professionals is a critical step in the process too. Useful questions to discuss with finance teams include:

- Is your department budgeting project by project, or do you take a more strategic approach?
- Is SRM supported by core funding, or does it exclusively rely on donor support?
- Do you consider the life cycle of hard assets when budgeting?
- How are you expected to resource contingency and preparedness plans?

Insurance provision

Often, insurance provisions are decided by finance (or operations) teams which can result in two potential silos:

- A lack of communication on what the organisation's insurance needs are, based on the risk profiles of staff activities and locations (i.e. what locations, level of cover, and any add-ons required).
- A lack of understanding by those at field level on how to access insurance, what specific provisions are in place, and a lack of clarity on who is covered and at what level (e.g. international versus national staff).

Discussing these issues collaboratively with finance, SRM and programme leads at the strategic planning stage is essential to ensure decisions on programme activities factor in insurance requirements, identify any 'red flag' locations or activities, and ensure appropriate provision of insurance to all staff.

Useful Resources

- GISF The Cost of Security Risk Management for NGOS
- GISF Securing Aid Worker Security through Effective Budgeting, (page 76)

3.5 Linking to Communications

Communications and SRM teams should work to support each other from both an external and internal perspective. From an external perspective, communications and SRM functions should work collaboratively to manage and mitigate the risks presented from mis/disinformation, social media and security incidents. Internally, communication leads can play a key role in maintaining and enhancing the effectiveness of the SRM framework, supporting SRM leads to simplify messaging, and engage staff.

Key definitions

- **Misinformation:** information that is misleading, but the source disseminating it has no intent to harm.
- **Disinformation**: information that is false and the source is deliberately attempting to manipulate facts.

Disinformation and misinformation

Disinformation and misinformation are rapidly increasing risks for organisations, particularly those operating in politically high-risk environments. Their impact on security can be significant. For instance, false statements can lead to NGO staff being arrested or physically attacked.

It is critical to understand that online security threats can directly harm the physical security of staff or those connected to the organisation. The spread of dis- and misinformation online can generate widespread anger, which can be used to justify physical attacks.

Online dis- and misinformation also make it hard to know what online news is real and what is fake. This hinders the ability of SRM professionals to rely on online media to help them gather information about a place and make critical decisions, especially in times of crises or emergencies. In these situations, security experts are forced to dig through layers of fake news to find true information, which can waste critical time. This hurts the ability of these organisations and individuals to offer life-saving support quickly and critically to their staff. The nature of digital communications and the threats it poses require cross-disciplinary solutions. In response, organisations should connect communications departments—which typically have specialists in social media and online communications technology—with SRM teams so each can share ideas on how to best strategise managing and mitigating risks associated with the spread of disinformation.

Communications leads can support SRM leads to develop dynamic ways to identify and respond to disinformation and move from ad-hoc response systems to more streamlined workflows around handling disinformation.

Social media

Social media is a core part of organisational communications, advocacy, and marketing strategies. But the threats associated with social media are growing and present direct, critical risks to the safety and security of staff, as well as to organisational reputations. Considering an organisation-wide approach to developing social media strategies, including the involvement of security risk management staff, is recommended.

For example, communications teams may be unaware of how certain messaging on social media may affect the safety and security of staff in a particular context. Equally, staff, consultants and volunteers should also be briefed on the safety and security aspects of using social media to share work-related updates on personal profiles.

Internal communications

Developing good internal communications around SRM is critical to ensure engagement and a successful rollout of any SRM strategy (see Chapter 1). Working with communications leads to simplify internal SRM messaging, as well as considering how to translate key SRM messages in different contexts, can be huge assets.

Modes of communications could include internal social platform content, such as an intranet page or newsletter. Videos, 'town hall' meetings, online and face-to-face events, e-mails, and live 'casts' from key personnel are other viable options for SRM communication.

External Communications

Responding to a security incident requires teamwork across departments and disciplines. SRM incident responders may be working to manage and mitigate the impact of the incident while the communications teams develop a public response. How an NGO handles or ignores public disclosure of a security incident will significantly affect its reputation and ability to continue operating safely.

Clear communication, preparation and planning between these two functions is therefore essential.

Communications and SRM leads can and should also work together to develop strategic approaches to external advocacy around SRM. For example, this might include working with communications leads to develop external messaging around good duty of care and how this supports organisational resilience.

Useful Resources

- InterAction Risk Assessment Tool: Assessing organisational risk related to disinformation (p.25).
- Internews: Managing Misinformation in a Humanitarian Context
- CDAC Network
- GISF's Security Risk Management Toolkit: Strategies (p.14-15)

3.6 Linking to IT

As part of an increasingly holistic approach to SRM, many safety and security functions now incorporate digital security. This includes how staff can protect themselves and reduce their individual exposure to online threats. However, this sometimes creates a disconnect between digital security risk management and the scope and responsibilities of the IT departments (who typically focus more on organisational-level cyber security threats).

SRM and IT leads should share their approaches to cyber and digital threats and communicate their mitigations for online risk management. This will have a direct impact on improving the safety and security of staff, as well as ensuring good business continuity.

Key definitions:

- **Cyber security:** protects entire networks, accounts and computer systems in addition to user information.
- **Digital security:** protects your online presence, personal data, assets and information.
- **Information security:** protects the confidentiality, integrity, and availability of information.

Convergence of physical, digital and cyber security

Online threats can have a direct link to physical security. For example, digital surveillance can lead to nefarious actors accessing or sharing online personal information about an individual with different threat actors. This can enable either the actor that stole the data or another who has gained access to it, to track down and physically harm the individual(s).

As well as individual digital security threats, organisation-level cyber-attacks can also impact the physical safety and security of individuals. Given the confidential nature of humanitarian data and the politicisation of humanitarian work, losing personal data in a large-scale cyber-attack can be catastrophic. It can affect not only direct employees, but also those the organisation seeks to support, by increasing the risk of a targeted physical attack.

Example from the sector: Major cyber-attack on the International Committee of the Red Cross (ICRC)

In January 2022, the ICRC faced a significant cybersecurity breach, exposing personal data of over 515,000 individuals worldwide. The breach, which included personal data such as names, locations, and contact information, affected missing persons and their families, detainees, and other people receiving services from the International Red Cross and Red Crescent Movement amidst armed conflict, natural disasters or migration crises.

The data breach highlighted a concerning trend in cyber operations targeting humanitarian organisations. These kinds of attacks pose grave risks to already vulnerable populations who can face potential harm due to the exposure of their sensitive information.

In response to the breach, the ICRC is now working with its Movement partners to strengthen the legal and policy framework protecting the data and infrastructure of humanitarian organisations. They are now actively advocating with governments for enhanced online protections.

Read more: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

Even when organisations or individuals are not directly targeted, they can still be impacted, such as when a cyberattack is committed against a private actor with whom the organisation or individual has a relationship. In 2020, SolarWinds—a private American IT company—was hacked and had much of its data stolen. Since the company housed the data of several other companies, government agencies, and non-profit organisations, a wide variety of different organisations had their data and information stolen. This compromised the health and safety of those whose data was being housed by SolarWinds.

Expert opinion

"[Cyberattacks] put huge pressure on NGOs' limited resources, which not only prevents NGOs from fulfilling their missions in the short-term, but can also create long-term reputational damage and undermine the confidence in its ability to fulfil its role in current and future crises and emergencies."

Reliefweb, 'Cyberattacks; a real threat to NGOs and not-for-profits', 2022

It is crucial to improve communication and coordination between IT leads working directly to manage organisational cybersecurity threats and those creating SRM strategies to protect staff from digital security threats. Gaps and weaknesses within an organisation's cyber risk profile are often due to lack of understanding of the risks at a human level. SRM and IT teams should work closely together to identify the key threats, assess where potential gaps lie, and develop training and support approaches for staff at all levels of the organisation.

Simplifying technical language

Assessing and presenting cyber and digital security risks with non-technical language is also critical to engage with organisational risk management leads and enable strategic level decisions to be informed by the respective risks. Translating these risks and mitigation measures into clear, plain language which demonstrates the potential impact on organisation operations is essential. This should ultimately help ensure that these risks are taken sufficiently seriously and help organisations make the changes necessary to become more secure.

Useful Resources

- GISF Humanitarian Security in an Age of Uncertainty: the intersection of digital and physical risks
- Integrating Cybersecurity and Enterprise Risk Management (ERM)
- GISF Security to Go: Module 4 Digital Security
- GISF Digital Security of LGBTQ+ Aid Workers

3.7 Linking to HR

The relationship between HR and SRM is integral to the effective planning, management and mitigation of safety and security risks to staff across all operating environments. While there are clearly different areas of responsibilities between HR and SRM functions, there remains a core interdependency, fundamental to fulfilling an organisation's duty of care.

The GISF article 'Toward inclusive security risk management' notes that NGOs increasingly consider the profiles of the aid workers they hire and deploy to maximise acceptance and mitigate risks. Establishing systems that recognise and acknowledge different staff profiles, enable better understanding of the risks each individual faces, and ensure adequate measures are in place to mitigate them, is vital for improving access and keeping staff safe. It is not enough, however, to simply identify staff profiles as a risk mitigation strategy in and of itself. HR and SRM leads must also collaborate to ensure these adapted security approaches and specific measures are adequately communicated to individual staff. The resources shared below offer further examples of how organisations can improve their person-centred approach.

Diversity, Equity, and Inclusion (DEI)

Like security, DEI is cross-functional and may have dedicated roles or focal points across an organisation. However DEI is structured, or named, within an organisation there remains an intrinsic link to both HR and SRM. To foster a safer and more inclusive operational environment, HR and SRM must collaboratively develop a framework for sharing essential safety and security information. Involving DEI practitioners and practices can ensure security information disseminated to staff accounts for the different personal characteristics. These include ethnicity, race, religion, physical or mental disability, gender identity, and more. Other factors include medical needs and prior experience.

Top tip: DEI acronyms and terminology

DEI may be known under different headings based on the organisation and aims of that function. Some examples of these may include GEDI (Gender, Equity, Diversity, Inclusion), JEDI (Justice, Equity, Diversity, Inclusion) among others. There are cases where this function may sit independent from HR though they would still have interdependencies.

Providing safe and secure avenues that encourage all staff to report concerns, incidents, and near-misses, especially where this relates to specific profiles, can also help organisations to reflect on and review practices and make adjustments where needed. The mechanisms for facilitating this do not have to be complex and can enhance good SRM practices. Some examples include ensuring there is a cross section of staff represented while developing risk assessments or reinvigorating processes to capture ongoing feedback. Working alongside DEI-HR practitioners, SRM can remain agile and responsive to the intersectional needs of staff.

Mental health and wellbeing

SRM extends beyond physical security to include psychological safety. Staff should be given access to, or the support to develop, safe mental health spaces. Doing so can have a hugely positive impact on programme activities and long-term strategic goals.

The dangers and distresses inherent to humanitarian work make it particularly important that humanitarian organisations take steps to protect the mental health of their employees. GISF's podcast on 'Psychological Safety' documents the challenges to mental health and wellbeing in the humanitarian sector. Mental health challenges can often impact physical health. Likewise, untreated mental health diseases—and their subsequent physical health challenges—can accumulate to create large expenses for the individual and their employer. Therefore, underprioritising mental health is a key business risk.

Recent research by McKinsey & Company demonstrates that strong psychological safety is one of the strongest predictors of team performance, productivity, quality, safety, creativity and innovation. It is also predictive of better overall health. Improving conditions for organisations to create and sustain psychologically safe environments can have universally positive impacts on an organisation's security. This is also more likely to promote an inclusive security culture with cross-cutting results.

To effectively achieve this requires a strong ongoing relationship between SRM and HR leads. This is especially important in areas such as staff retention, incident reporting and ongoing strategic level efforts to strengthen the organisational culture around mental health and wellbeing.

Much progress has been made to build awareness of the mental health needs of those working in the aid sector. But there is still a need for greater awareness and discussion at the strategic level about the extent to which poor staff mental health can impact organisational objectives. Discussions between HR and SRM strategic leads on how to best manage and mitigate these risks are key. They are particularly important in less widely documented areas. This can include vicarious (indirect) trauma and supporting staff from, or operating in, different cultural contexts, where, for example, mental health and wellbeing is not as widely recognised or spoken about.

Recruitment and retention

Many organisations are finding it increasingly difficult to attract, train, retain, and motivate competent SRM staff. This is a major concern that can have severe impacts on operations and an organisation's resilience. Given the ever-changing landscape, funding restrictions present additional vulnerabilities in the recruitment and retention of SRM staff. This, coupled with challenges for some SRM professionals to demonstrate their impact, with key performance indicators not always aligning to strategic objectives, makes it hard to adequately inform and influence strategic-level decision-makers. For example, a qualified SRM professional may have no access nor reporting line to the organisation's key decision-makers or executive suite. Yet they still have a mandate to foster an improved security culture.

SRM and HR leads should also discuss and regularly review their approach to recruiting and retaining SRM staff. Rather than using set specifications and competencies for all SRM staff, a more adaptable strategic approach should allow for greater flexibility on the experience and skills needed for specific roles in the organisation.

Capacity building

Identifying learning and development needs should form a key part of strategic-level planning, with associated collaboration between SRM and HR leads (see Tool 8: Learning and Development Plan Template). Establishing strategic goals that aim to build the capacity of SRM staff should be viewed as an investment, rather than as an additional expense (see Tool 9: Strategic Training Matrix Example). Critical to this is ensuring a strategic approach to continuing professional development – one that outlines and encourages opportunities for progression and growth of SRM staff, allowing them to remain agile to changing needs while deepening good practice.

Useful Resources

- GISF Managing the Security of Aid Workers with Diverse Profiles
- GISF Towards Inclusive Security Risk Management
- GISF Security to Go: People Management
- GISF Podcast – psychological safety episode
- McKinsey & Company: What Is Psychological Safety?
- GISF Humanitarian Security in an Age of Uncertainty: The Intersection of Digital and Physical Risks

3.8 Linking to Legal

Legal and SRM functions share a common goal: to protect an organisation from harm. Through close collaboration and communication, each function can help the other optimise security and compliance throughout the organisation. It is also inevitable that different laws will affect the work of the security team. Determining which regulatory frameworks apply is only the first step, as SRM and legal leads also need to discuss and decide how those regulations should be interpreted within specific operational contexts.

Meeting duty of care requirements

Duty of care refers to an organisation's legal (and moral) requirement to take all the necessary steps to ensure the physical and mental wellbeing of their staff. Although most organisations have a good understanding of how duty of care relates to their direct employees, complexities arise when establishing duty of care responsibilities towards:

- Staff operating in different legal contexts.
- Staff on different types of contracts, such as international staff, national staff, consultants, volunteers, and dependents.
- Staff working for external delivery partners or external consultants.
- Delivery partners (see GISF Resource: Security Management and Capacity Development: International agencies working with local partners).

Top tip: Duty of Care Self-Assessment Tool

The Swiss Centre of Competence for International Cooperation (CINFO) and GISF developed a comprehensive Duty of Care Self-Assessment Tool. This allows organisations to assess the safety and security aspects of their duty of care. The tool uses five steps, from an initial to an optimised level, to determine an organisation's strengths and areas for improvement in four areas: information, monitoring, prevention and intervention.

Resource: https://dutyofcare.cinfo.ch/index.html

Example from the sector:

> *"Risk sharing was a massive challenge for us when we were working with consultants and partner organisations. Our client and delivery partners often struggled with the prospect of having a degree of duty of care for a consultant, as they were not their employee or contracted directly. To resolve this, our security and legal teams drew up a number of MoUs to clarify roles, as no one was clear on who should assume responsibility. This sometimes meant projects were delayed considerably, and processes became really resource intensive."*
> (KII Participant, NGO Operational-level SFP)
>
> *"The question of duty of care for national staff in medical terms at my last organisation meant that when a member of staff was involved in a car accident and the surgery was not available to prevent amputation, we had to airlift him from Somalia to Ethiopia and fund extensive costs for ongoing care and physiotherapy."*
> (KII Participant, NGO Strategic Lead)

From a strategic perspective, it is essential for several function leads to have a clear understanding of where duty of care complexities exist and establish where responsibilities sit. SRM, HR, programme, and legal teams should carry out stakeholder mapping exercises to help clearly articulate and assess their organisation's duty of care complexities. The outcomes of these activities can then feed into strategic planning and practical implementation.

Example of stakeholder mapping:

Stakeholder	Direct duty of care	Shared duty of care	Moral duty of care
Direct employee (FT, PT)	X		
Consultant (internal)	X		
Volunteer	X		
Visitor	X		
Delivery partner personnel		X	
Consultant (external organisation)		X	
Personnel seconded to an external organisation		X	
Employee of a member association			X
Grantee			X
Dependent of an employee			X

Where a shared duty of care is held, appropriate due diligence should be carried out between partner organisations. Clear agreements or memoranda of understanding (MoU) should be established, outlining responsibilities, expectations and any agreed minimum standards related to duty of care.

Where these is a moral duty of care, an organisation should clearly outline the support, resources and mechanisms that may be provided. Guidance and advice may also be provided, but there is no legal obligation for the stakeholder to comply.

Creating a culture of understanding around the 'duty on individuals'

Employers have a duty of care responsibility to their staff. But employees also have a responsibility to their organisation to actively participate in safety and security planning, follow the emergency and standard operating procedures in the company's policies, and to use general common sense to avoid unnecessary risks when carrying out activities on behalf of their employers.

Ideally, duties on an organisational and individual level go hand-in-hand. Together, they should create a culture in which employers care about the health, safety, security and wellbeing of their employees. Employers should develop and deploy appropriate SRM policies, procedures and guidance to protect staff from harm. In turn, employees should actively engage with and follow these protocols.

To create this culture of joint responsibility at the strategic level, there is a need for a healthy and reciprocal relationship between the employer and the employee. Employees should act in a responsible and safe manner, but employers also need to be proactive about setting appropriate parameters. Setting unrealistic expectations at the strategic level will result in a lack of engagement if staff feel they cannot practically achieve their objectives by working within those parameters.

It is therefore essential to define the organisational stance on duty of care and the expectations on individuals. This should not only be based on contractual obligations, but also on the feedback and involvement of staff. Providing clear and easy ways to give feedback is a key start point.

Options may include:

- Regular line manager reviews.
- Anonymous reporting mechanisms.
- Clearly established accountability lines so staff know who to report concerns to.
- App-based reporting.
- Exit interviews.
- Creating a positive culture around near-miss reporting (for example linking near-miss/concerns reporting to line manager KPIs).

Useful Resources

- ISOS Global Duty of Care Benchmarking Report, 2015
- CINFO Duty of Care Model

3.9 Linking to safeguarding

Acknowledging that the exact definitions, and scope of safeguarding may differ between organisations, there are several areas where security and safeguarding align. In the humanitarian space, safeguarding broadly means preventing harm to people – and the environment – in the delivery of development and humanitarian assistance. Through safeguarding's evolution in the sector, many organisations include protecting the health, wellbeing and human rights of all individuals – with a focus on the communities we serve – to live free from abuse, harm and neglect. This demonstrates the continued need for close collaboration between safeguarding and SRM functions.

Collaboration on approach

It is essential to recognise that safeguarding issues can quickly become safety and security issues for all individuals involved – from those submitting the concern, to the alleged perpetrator and those tasked with investigating.

Expert opinion

"There are no safeguarding issues that aren't also safety and security issues."

(KII Participant, NGO SRM Strategic Lead)

Targeted campaigns and aggression towards an organisation and its staff can quickly spiral from even one safeguarding allegation. Operating in contexts where there is a lack of access to monitor, assess and report safeguarding issues can also increase the risk, requiring a more integrated and strategic approach.

Example from the sector:

"In Somalia, the risk of recruiting underage staff or staff with previous criminal records is ever present and verification is often reliant on liais[ing] with the local police and community leaders in rural areas.

Recruiting in this context threw up numerous issues, including inter-community rivalry for the organisation I used to work for. [W]e had to evenly balance numbers recruited from differing ethnic groups, and ethnic leaders would turn up at the office demanding justification if they thought they had been overlooked. We were alerted to a case of job selling for sex by a community leader which prompted a safeguarding review. Then one woman, who we had verified as over 18 through the community, appeared to suggest that she was only 16 to another staff member and we were forced to defend ourselves against child labour accusations.

Another member of staff had apparently told colleagues that he was about to marry one of the community girls and these staff reported to me that she was maximum 13 or 14 years old. After a lot of community resistance, we eventually spoke to the girl who reported that she was 18 and consented to the marriage, but it appeared that she was under community pressure. Additional safeguarding training was put in place through local facilitators but early marriage and job selling cases still cropped up."

From a KII Participant, NGO Operational SRM Manager

From a strategic perspective, SRM, safeguarding, HR and programme leads need to work in close collaboration to ensure potential risks are identified, mitigations agreed, and roles clarified in prevention, reaction and recovery. Paramount to this relationship is ensuring the contextual understanding of the operation and the roles needed to mitigate safeguarding and the escalation of security risks.

Safeguarding incident management cycles may slightly differ between organisations. But there are entry points where a solidified relationship between security and safeguarding can help streamline processes and enable safer outcomes for all parties involved, as well as fostering understanding and informed approaches to incident reporting.

One way to ensure closer collaboration is by holding investigation trainings. These sessions should articulate the organisational roles during a safeguarding incident, ensuring that both safeguarding and SRM focal points are involved and that all parties are following clearly laid out, evidenced-based protocols. Keep in mind that while SRM staff may need to be informed, they are unlikely to be the right team to manage or lead a safeguarding incident.

In some organisations, the relationship between safety and security is more intertwined. For instance, the safeguarding focal point may also be the security focal point. There is no one way this relationship must be established or works best, as it will largely depend on the organisational needs and expectations. What is important is that an organisation understands the functions of both safeguarding and security independently as well as their interconnectivity.

Useful Resources

- Safeguarding Resource and Support Hub
- GISF Webinar: Intersection of Security and Safeguarding
- InterAction Blog: Launching the safeguarding community visual toolkit
- GISF 'How-to' Note On Implementing the safeguarding cycle

3.10 Linking to Travel Management

The management and monitoring of staff travel is often strongly led by budgetary demands. It is increasingly led by corporate social responsibility (CSR) policies too, such as targets for reducing carbon emissions. However, the recent publication from the International Organization for Standardization (ISO), ISO 31030: Travel Risk Management, clearly presents the case for safety and security risk management to be closely integrated into the strategic planning of staff travel (both international and national).

Travel Risk Management (TRM)

ISO 31030 lays out key advice and guidance to organisations on how to ensure that travellers can perform their duties optimally in an environment which is as safe and secure as reasonably possible.

SRM functions should be heavily involved in developing and supporting good practice in TRM policies, providing key technical input into:

- Context analysis and briefing, such as what information sources to use and how these are presented and communicated.
- Authorisation and approval, such as establishing a system for travel approval and authorisation based on risk assessments and traveller profiles and activities, not just financial considerations.
- Traveller tracking and monitoring, such as ensuring organisation-wide awareness of traveller locations in case of incidents.
- Evacuation and relocation, such as developing contextually appropriate contingency plans.

- Developing organisational standard operating procedures (SOPs), which might include per diem expense rates, as well as accommodation and transport selection policies that support good security risk management.
- Developing in-country travel and movement planning procedures.

Useful Resources

- ISO 31010: 2021 Travel Risk Management: guidance for organisations

UNOCHA/Viviane RAKOTOARIVONY

Madagascar
A staff member with World Central Kitchen travels to Madagascar to assist with a meal distribution in the aftermath of a cyclone. Any staff travel should always be guided by robust travel risk management policies.

Chapter 4: SRM Strategic Coordination, Collaborations and Partnerships

Given the breadth of new threats, ranging from shifting geopolitics to digital and cyber risks, the importance of strategic-level security collaborations has become critical. This includes fostering sector-wide partnerships, establishing dedicated global, regional and country based networks, forming working groups, and maintaining key connections with other agencies and official and unofficial bodies. This process is often done effectively at an operational level. But organisations can struggle to formulate and implement these partnerships, networks and working groups strategically, relying on operational-level staff to form many of these relationships, formally or informally.

ISO 31000:2018 Risk Management guidelines highlights the importance of stakeholder engagement through communication and consultation during the risk management process.

The engagement of different stakeholders at the operational level is critical for sharing security information, assessing risks and implementing effective security measures. However, the absence of strategic level coordination and collaboration with different actors, supported and guided by senior leadership, exposes staff to additional risks. This is increasingly important in complex working environments when engaging with non-state armed groups (NSAGs) and ensuring compliance with counter-terrorism legislation.

4.1 Interagency security collaboration

Organisations must engage across the sector and coordinate with humanitarian, development, and human rights groups to share knowledge and experience in responding to threats. Cross-sector engagement is fundamental to ensuring good SRM. There are already several operational and strategic mechanisms for national, regional and global UN-NGO coordination in humanitarian security risk management and parallel disciplines. These include Civil-Military Advisory Group (CMAG), Global Access Working Group, Saving Lives Together (SLT) country-based access and security working groups, and humanitarian country teams.

In recent years, NGOs have also formed various security networks and platforms at country, regional and headquarters levels. These security collaboration networks and platforms help to facilitate the exchange of security information, raise awareness of good SRM through trainings and workshops, and promote best practice between organisations.

Organisations should seek to formalise such collaborations at a strategic level and ensure they are promoted and understood at the operational level to support staff in engaging and collaborating with organisations. The GISF NGO Security Collaboration Guide provides advice and practical resources to support NGOs in facilitating effective security collaboration with other organisations operating in the same context.

Cross-sector engagement and collaboration is particularly important for small NGOs, in-country start-ups, and emergency response teams, as it enables immediate access to critical information that an organisation may not have the resources to identify on its own. There are several external and internal barriers to effective SRM collaboration, and organisations need to try and overcome these challenges to ensure closure collaboration.

Some important considerations include:

- ✓ Advocacy – Do we promote the need to collaborate with other organisations? Are the benefits of security collaboration understood across and within organisations? A good example is fundraising through institutional donors and influencing of the policy frameworks around direct/indirect costs.
- ✓ Accountability – Are our staff held to account for maintaining relationships with other organisations? If relationships with other organisations are not managed effectively, how can we improve this?
- ✓ Resources – Have we resourced, both human and financially, to enable the organisation to be present at these coordination mechanisms? Do we need to look at our security architecture as an organisation? Do we have the appropriate systems in place for budgeting for security?
- ✓ Diversity of security approaches – Different organisations have different security approaches and capacities, but how can we learn from others? Do we benchmark our security approaches with other organisations operating in the same environments?
- ✓ Confidentiality – Organisations don't like to share sensitive information as it can expose them to additional risks. What information can we share and how can we share it? Building relationships with others during or ideally ahead of emergency response operations can pay dividends as it helps with enhancing trust and reciprocal exchange of information.
- ✓ Priorities and time constraints – Attending security meetings and engaging with other organisations takes time and resources. How do we ensure security collaboration is prioritised and seen as an enabler that augments and improves programme delivery?

Answering these questions may lead to the need for guidance, additional responsibilities and resources. Making the need for collaboration, cooperation and partnerships explicit in your SRM strategy will increase organisational capability in the long run, to promote information exchange and coordinate more effectively between organisations.

An example of how this can work is the Saving Lives Together (SLT) framework, established for UN-NGO coordination. The objective of SLT is to enhance the ability of partner organisations to make informed decisions, manage risks, and implement effective security arrangements that enable delivery of assistance and improve the security of personnel and continuity of operations. Include this in your SRM strategy and ask your staff to engage accordingly.

To understand what coordination bodies or collaboration opportunities are available and relevant, organisations should conduct a key stakeholder analysis for SRM. This should be conducted at a strategic level but informed thorough understanding of the operational level coordination bodies that staff are engaged in and the initiatives that have been formed. Undertaking this process through a participatory approach, will enable organisations to develop SRM coordination strategies that are linking global to field operations and vice versa.

4.2 Internal Collaboration and Coordination

A recurring theme when ensuring an SRM strategy is being implemented effectively within an organisation is engaging all stakeholders. This does not mean just talking with operational staff members, but instead bringing them into the process. This can include engaging operational staff with a cross-functional risk management working group (see Chapter 2) and bringing them on the journey of policy development. To do this, organisations should:

- Regularly assess the operational needs – Conduct key informant interviews (KIIs), hold regular SRM meetings, and find out what are the most common or critical risks they face in their roles. This information can be used to influence the priorities of SRM.
- Discuss real-life scenarios – Try to make the scenarios relatable to what staff are facing in their day-to-day needs. Highlight how SRM can enable them to perform effective programming.

Once the concerns and issues have been identified, it is vital to follow up and prioritise:

- Communication and informing – Operational staff will engage more if they are updated with the organisational process. A transparent approach can enable staff to understand how and when SRM strategies are being developed. This will increase engagement and support a culture of security.
- Aligning the organisation's SRM with the organisation's risk attitude and security culture – This is about showing how risk management is integrated within the organisation's strategy, vision and goals, and highlighting how it strengthens organisational strategy and enables sustainable programming.

Considerations when implementing global policies at an operational level

There are many factors that need to be considered when implementing global policies at a regional or country level. If there is little to no engagement with operational staff when new policies are introduced this can lead to several significant challenges:

- Context – Organisations often work across multiple regions, each with significantly different environments. There cannot be a 'one-size-fits-all' procedure within an organisation.
- Culturally appropriate – Culturally, people approach risk management differently, often in a way that is intuitive to the environment that those people are from.
- Technology – In recent years organisations have sought to find technological solutions. This could be mobile apps that enable group communication or provide tracking and security alerts. Are these accessible for staff within the organisation? Will the organisation appropriately fund and resource this?
- Language – SRM language can be complex and technical. Staff with English as a second language can struggle with the terminology. Simplicity is key when considering SRM. It is essential for SRM specialists to change the language rather than for others to understand SRM language. SRM is an enabler, so it must do what it can to gain traction and buy-in. This can lead to more efficient and more accurate communications.

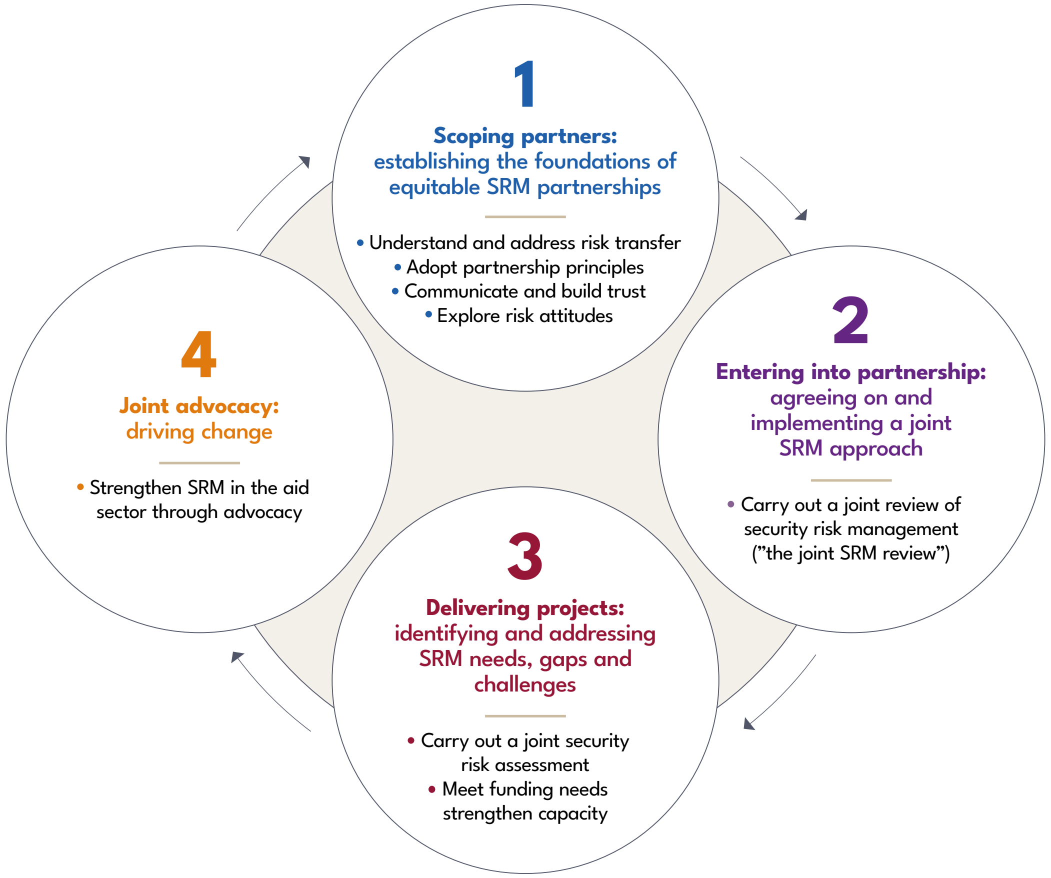
Example from the sector:

"My organisation has had some really good policies and strategies to improve SRM, but they haven't considered the realities on the ground. Staff don't read English, and the internet signal is unreliable in our field office locations, so app-based systems aren't appropriate. We have also spent a number of months trying to explain that the safeguarding policy being introduced is not contextually appropriate."
From a KII Participant, Country Director in the Middle East

4.3 Policy Development for partnerships

When developing partnerships with other NGOs, UN agencies, and donors, a full understanding of an organisation's SRM strategy is critical. This includes understanding the organisational risk approach and its policy on working in partnerships including a clear delineation on duty of care responsibilities.

Partnerships can come in many different forms: international, national and local; member associations; external delivery partners; and increasingly working within consortiums. GISF's Partner Joint Action Guide provides a detailed guidance on establishing equitable partnerships between INGOs and local or national NGOs.


1
Scoping partners:
establishing the foundations of equitable SRM partnerships
• Understand and address risk transfer
• Adopt partnership principles
• Communicate and build trust
• Explore risk attitudes
2
Entering into partnership:
agreeing on and implementing a joint SRM approach
• Carry out a joint review of security risk management ("the joint SRM review")
3
Delivering projects:
identifying and addressing SRM needs, gaps and challenges
• Carry out a joint security risk assessment
• Meet funding needs strengthen capacity
4
Joint advocacy:
driving change
• Strengthen SRM in the aid sector through advocacy

This guide offers plenty of tools and guidance on how to formalise SRM within partnerships. However, organisations also need to set a global policy or position on forming partnerships. This should be a cross-function policy that enables all aspects of duty of care, including security to be considered.

At a basic level, partnerships should fall in line with the organisation's strategy. It is also important to question why partnerships are being formed. Is it being done to localise the delivery of humanitarian aid or are partnerships being formed to minimise risk to the organisation? If the latter, are the risks being 'transferred' to partners or 'shared' with partners?

Risk transfer relates to the full movement of risk from one party to another, which may be suitable in some circumstances if fully transparent, identified and agreed by both parties. However, for risk sharing to truly occur, both parties need to understand the risks that each party is exposed to, that these are agreed on equal terms, without power imbalances, and that resources to address them are allocated equitably.

Top tip: Donors and risk

Key questions about risks and partnerships can also be asked of donors, particularly if they are transferring the risk completely. Pressure from donors is one of the most frequent responses when discussing taking unnecessary risk. So, donors must also understand the risk levels you are willing to operate at.

As outlined in GISF's research paper, Partnerships and Security Risk Management: from the local partner's perspective, it is critical for NGOs to view partnerships from the perspective of local NGOs with which they work.

Successful partnerships require creating, transferring, and sharing security risks between partners. Doing this requires a detailed understanding of the security challenges for both organisations in the partnership, and how, as a supportive partner, you can work together to improve the overall security of all organisations involved.

Another common concern for operational staff, that many strategic-level staff cannot answer, is: what is my duty of care to our partners? To answer this question, the duty of care approach needs to be appropriately documented and guidance provided to staff. To do this the following questions should be considered:

Security risk management partnership questions (linking with your SRM strategy)	
Duty of care	What is our legal and moral duty of care for our partners? The answer should set the parameters of care which the organisation should provide.
Governance and accountability	What standard of SRM do we expect from our partners? How will we measure this? Will partnership agreements document SRM?

Security risk management partnership questions (linking with your SRM strategy) *continued*	
Risk transfer vs risk sharing	Are we transferring all risks and the responsibility for managing these risks to partners, or is the intention to share risks with partners? Are we willing for our partner to take more risk than we would expect our staff to? If yes, what level of risk is this? What support should we provide to assist them in managing these risks? Are we willing to increase support to our partners in line with the level of risks involved? If yes, what support should we provide?
Policies and principles	Do our partners need to align with our humanitarian principles, and specific policies?
Critical incident management	What support will we provide to our partners in the event of a critical incident? Does this differ to support we provide our own staff?
End of partnership	What is the extent of our duty of care towards partners at the end of the partnership agreement?

Navigating partnerships and due diligence is a complex process, but one that needs to align with organisational strategy and values. Therefore, to ensure consistency within all partnerships, policies which outline the organisation's duty of care towards partners should be widely communicated and reviewed at a strategic level (see also section 3.8 Linking to Legal)

Useful Resources

- ISO 31000:2018 Risk Management Guidelines
- GISF Co-ordination for Humanitarian Security Management
- GISF Collaborative Security Risk Management: A case for local development
- UN Saving Lives Together Framework
- GISF Partnerships and Security Risk Management Joint Action Guide

Joseph Mankamba/OCHA-RDC

Democratic Republic of the Congo

Staff members from ECHO, OCHA, Action contre la Faim, and Oxfam discuss a joint humanitarian response. When working with partners, it is vital that legal and moral duty of care is well established and understood.

Chapter 5: SRM's contribution to organisational resilience and business continuity

To be a resilient organisation is to be prepared for adversity, able to respond effectively to disruptions and crises, and capable of positively adapting in the face of challenging conditions. Humanitarian and development organisations frequently find themselves having to navigate increasingly politicised environments, no longer perceived as politically neutral and faced with shrinking civil spaces. The scale of and frequency of crisis confronting organisations is unprecedented. Organisational strategies must recognise and address the connection between security and safety risks, business continuity, and organisational resilience. All organisations must have comprehensive mechanisms in place to effectively respond to and withstand – sometimes unpredictable – shifts in operating contexts and critical events.

5.1 Preparedness and Planning

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 related policies, alongside practical measures on how SRM can support the wider organisation in discussions around readiness and response planning. Safety and security play significant roles in both traditional crisis response settings as well as incidents of fraud, reputational risk, safeguarding or global pandemics.

OCHA/Gema Cortes

Venezuela
An aid worker measures the temperatures of a family during the Covid-19 pandemic. Organisations must have mechanisms in place to adapt their security procedures in response to critical events, such as public health emergencies.

Key definitions:

- **Business continuity:** The strategic and procedural planning that an organisation undertakes to ensure essential functions can continue during and after a disruptive event.
- **Crisis:** An event, or series of events, that significantly disrupts normal operations, has caused, or is likely to cause, severe consequences which will impact the whole organisation. A crisis typically requires a response beyond normal management mechanisms to address the impact and its aftermath.
- **Critical incident:** An adverse event that results in, or could result in, severe harm to staff, disruption to programmes and activities, or loss or damage to the organisation's assets or reputation, but is manageable within normal protocol with support from HQ.
- **Incident:** An incident is usually managed solely by individuals located in the country or close to where the incident occurred or is occurring.
- **Organisational resilience:** An organisation's ability to anticipate, withstand, respond to, and recover from security threats, incidents, or disruptions while maintaining its essential functions, reputation, and stakeholder trust.

Preparing for SRM-related crises or crises with SRM implications

The successful resolution and management of any crisis situation depends on the organisation's ability to take appropriate decisions quickly. This requires preparation, a good flow of information, and clear channels of communication that all staff understand. While every crisis is different and you cannot plan for every eventuality, you can plan for how to respond effectively to each crisis, allowing critical bandwidth for the organisation to continue to operate without using all its resources to resolve a single event. An organisational strategic approach to crisis management and business continuity plays an important role in allocating to SRM the necessary resources to prepare and respond to disruptive events.

Preparedness and planning will vary depending on the organisation and between different strategic functions. For instance, organisations operating in conflict-prone environments are more likely to develop a framework for risk-informed decision-making, invest resources in building more secure facilities, deploy trained security personnel, and establish strategic partnerships and mechanisms to better coordinate their crisis response. Meanwhile, organisations operating primarily in lower-risk contexts may only make modest investments in their infrastructure, or review their crisis management plans periodically, or in accordance with forecasted periods of unpredictability, such as elections or seasonal weather hazards. Both contexts present risks that pose a significant threat to organisational operations, so it is vital that SRM and preparedness are not solely viewed through a safety and security lens.

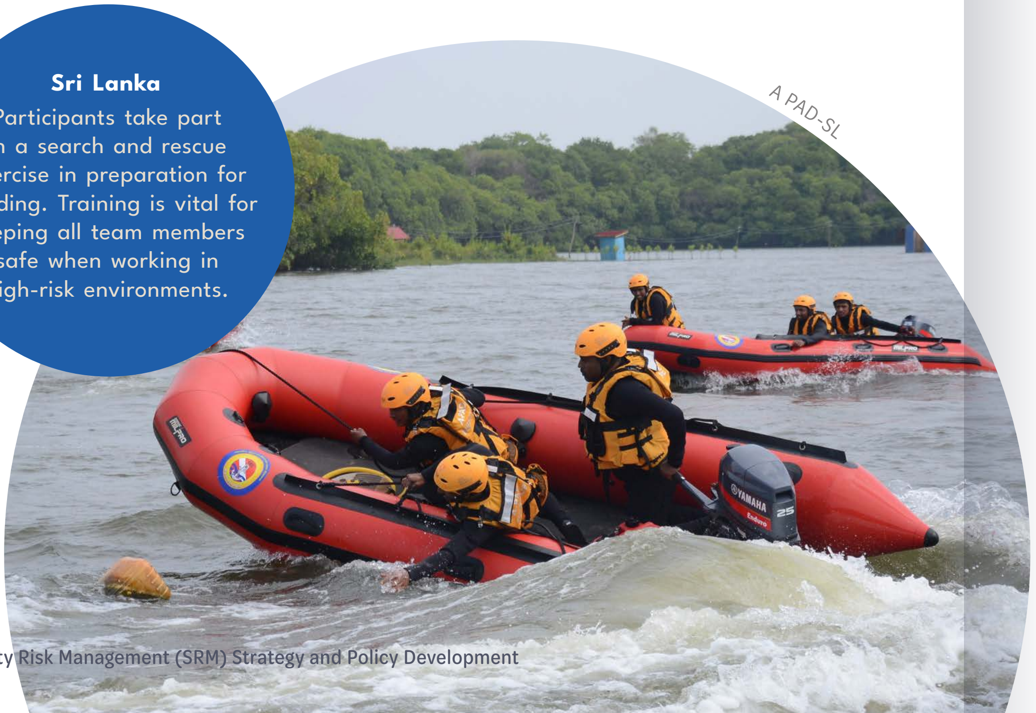
Strategic organisational preparedness can take the form of comprehensive risk assessments, strategic scenario planning, risk-based resource allocation, and continuous learning and improvement. SRM leads can also conduct a training needs assessment for the whole organisation, leading to opportunities for staff to pursue relevant qualifications and build organisational capacity.

5.2 Cross-functional approach to crisis management

A cross-functional approach is key to successfully managing a crisis affecting your organisation, staff and/or assets. A successful outcome within any crisis is dependent on a cross-functional team working together; collaborating and communicating to achieve a common goal: crisis resolution. This cross-functional collaboration needs to be nurtured and developed ahead of a crisis occurring, rather than while trying to respond to a situation.

Cross-functionality during a response to a crisis

Notwithstanding the importance of identifying a crisis team lead (organisations typically select their CEO, COO or a Director with significant institutional knowledge or crisis management expertise to fill this role), all functions represented within a crisis management team are ‘action owners’, with interrelated but nevertheless defined roles and responsibilities. SRM leads should be viewed as equals in a team comprised of representatives from other key functions.

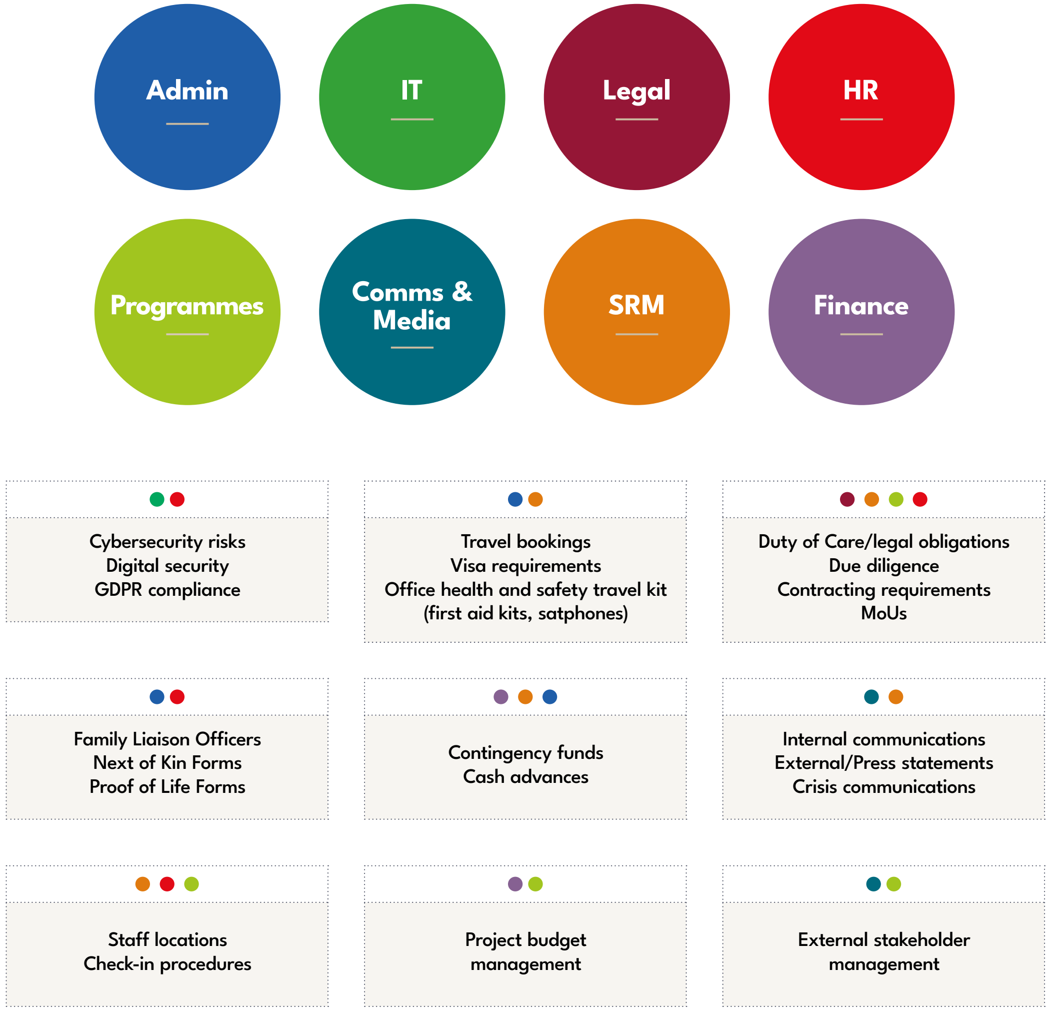


A PAD-SL

Sri Lanka
Participants take part in a search and rescue exercise in preparation for flooding. Training is vital for keeping all team members safe when working in high-risk environments.

The relationship chart below demonstrates the cross-functional relationships within a crisis management team.

Examples of cross-functionality during a response to a crisis, International Location Safety



Admin

IT

Legal

HR

Programmes

Comms & Media

SRM

Finance

● ●
Cybersecurity risks
Digital security
GDPR compliance

● ●
Travel bookings
Visa requirements
Office health and safety travel kit
(first aid kits, satphones)

● ● ● ●
Duty of Care/legal obligations
Due diligence
Contracting requirements
MoUs

● ●
Family Liaison Officers
Next of Kin Forms
Proof of Life Forms

● ● ●
Contingency funds
Cash advances

● ●
Internal communications
External/Press statements
Crisis communications

● ● ●
Staff locations
Check-in procedures

● ●
Project budget management

● ●
External stakeholder management

Business as usual

Crises are incidents that cannot be managed within routine measures and processes. As such, it is important for organisations to factor into the design of their crisis management and/or business continuity plans the extent to which they could continue to meet normal and ongoing business requirements while key function leads are busy responding to a major incident. Effective organisational resilience requires all function leads, including security, to ensure that there are sufficient resources, skill and capacity to maintain its essential functions and operations, and to be able continue to deliver services during or following a crisis.

Useful Resources

- GISF NGO Crisis Management Exercise Manual
- GISF Crisis Management of Critical Incidents
- Frontline Defenders Handbook

UN OCHA/Matteo Minasi

Haiti

Humanitarian actors coordinate their response in the aftermath of an earthquake. Organisations need to factor the potential for major crises into their plans to determine how they will respond and continue their normal functions.

Chapter 6: SRM Monitoring, Evaluation, Accountability and Learning (MEAL)

6.1 Why MEAL matters – basic concepts

Key to the success of any SRM strategy is establishing processes to monitor and evaluate its effectiveness, and ultimately its impact. Implementing a comprehensive SRM strategy requires continuous evaluation and adaptation. Therefore, having a comprehensive MEAL system will help ensure continuous quality and improvement in the process, its efficiency, and its outputs. An integrated MEAL system also allows the organisation to monitor how well its SRM strategy is enabling or supporting the achievement of wider organisational goals.

Key definitions:

- **Theory of Change:** A comprehensive illustration of how and why a desired change is expected to happen in a particular context. It pictures the pathways to achieve each outcome. It does this by first outlining the desired long-term outcomes and then working back to identify all the conditions (sub-outcomes) that must be in place (and how these relate to one another causally) for the outcomes to occur.
- **Logical framework (Logframe):** A logframe is a table or matrix that lists programme activities, short term outputs, medium term outcomes, and long-term goals. It shows the logic of how the activities will lead to the outputs, which in turn lead to the outcomes, and ultimately the goal. It includes the indicators that will be used to measure progress, the source of data, and assumptions necessary for project success.
- **MEAL Plan:** A summary document of how to carry out monitoring and evaluation plans, including a list of what to measure and why, key activities, budgets, responsibilities and deadlines.

Determining how to monitor and evaluate your SRM systems, setting reporting requirements for those accountable, and detailing how learning will be shared requires experience in monitoring and evaluation techniques and practices. It is therefore strongly recommended that strategic SRM leads work closely with MEAL technical specialists in their organisation to develop the process that will work best for them.

Top tip: Eight reasons why your SRM strategy should include a MEAL plan

1. Enables stronger and more user-friendly systems, policies and procedures.
2. Keeps track of how well you are meeting your strategic goals and desired outcomes.
3. Ensures money and resources are spent efficiently and effectively.
4. Provides accurate data which can be used for external and internal communications, funding applications, and donor or board reporting.
5. Can feed into business continuity and crisis management planning to identify gap areas or threats.
6. Enables a dynamic and adaptive approach to practical implementation of safety and security strategies.
7. Gives staff, clients and key stakeholders a voice.
8. Improves motivation and focus of people implementing your safety and security strategy.

6.2 Developing a MEAL Plan

A MEAL plan will allow you to communicate your approach and evidence how you will achieve your objectives, including who is responsible and what funding/resourcing is required. This helps demonstrate accountability and learning and ultimately enables you to enhance your credibility while fostering a shared understanding of what your ultimate aims are (see Tool 12: Example MEAL Plan).

Top tip: Creating an effective Theory of Change and MEAL Plan

- ✓ Start with the end in mind: define your long-term objectives.
- ✓ Be specific and realistic when deciding on indicators, make sure they are SMART (specific, measurable, achievable, relevant and time-bound).
- ✓ Set 'waypoints' identifying short, medium and long-term outcomes.
- ✓ Involve your stakeholders (see section 6.3) to ensure their engagement, feedback and input into the process – they are the ones who will need to make the process work.
- ✓ Contextualise your goals. How change occurs may be different for a team working in a high-risk country with a single-party repressive regime, compared to a team working in a low-risk setting in a multi-party democracy. Tailor your indicators to the context in which they are being used.
- ✓ Review and revise your theory of change model to reflect learnings on what works, as well as changes in your strategy or operating environment.

6.3 Routine monitoring of SRM progress

Selecting SRM indicators

Indicators can be quantitative, such as numbers of reported security incidents, security trainings delivered, or staff trained. Or they can be more qualitative, such as people's concerns, feedback, or experiences. As long as you can capture and use the data to demonstrate a journey, then you are succeeding in showing impact.

Each indicator should be:

- Directly related to the output, outcome or goal listed on the theory of change.
- Something that you can measure accurately using either qualitative, quantitative or mixed methods, and your available resources.

Selecting SRM datapoints

These are some examples of specific SRM datapoints that can feed into tailored indicators which could be used to highlight change, both positive and negative:

- Reported incidents.
- Reported concerns or near-misses.
- Measuring engagement or use of reporting channels.
- Safety and security feedback taken from programme reports.
- Feedback reports from one-to-one debriefs and exit interviews or forms.
- Perception surveys that measure awareness.
- Understanding and engagement with SRM policies and procedures.
- Attendance at training (internal and external).
- Attendance and minutes of SRM or security focal point meetings.
- International travel logs.
- Insurance claims.
- Budgeted and actual spend on SRM resources.
- Benchmarking to external standards.
- Internal audits connected to:
  - Completion and reviews of SRM documents (safety and security plans, risk assessments, incident management plans, security briefings, travel safety and security procedures).
  - Office safety and security checks or records.
  - Vehicle safety checks or records.
  - National staff movement logs.

6.4 Evaluation

Being able to quantify social and cultural change in a measured, tangible way, can be an essential tool to communicate the value and effectiveness of investment in SRM. There is no single method or approach used for measuring or evaluating impact. One approach is to use a theory of change (ToC) model, which maps out the links between your inputs, activities, outputs and how these bring about the required outcomes and impact.

The most effective ToC models are simple and focus on:

- The problem your SRM framework is seeking to solve (e.g. lack of awareness and engagement in SRM, increased threats to staff)
- The impact you are trying to make (e.g. creating a safe and secure environment for everyone working for, and on behalf of, your organisation)
- The conditions required to meet these outcomes (see Tool 10: Simple ToC diagram).

6.5 Accountability

Organisational buy-in is a prerequisite to successfully building a good SRM culture. Therefore, it is vital to engage senior leaders, trustees and colleagues in your learnings from MEAL, as well as to be transparent on accountability if targets are not being met. For example, establishing SRM as a part of the Board of Directors' KPIs included in quarterly reports, can ensure good integration of SRM by clearly linking it to organisational success.

Having appropriate audit and compliance systems in place at all levels of the organisation should come with clear outcomes and punitive action if compliance is not met. Clear lines of responsibility, as well as specific actions for compliance, should also be stated within the logframe to ensure full accountability.

Example from the sector:

"Our organisation had a good written system and process in place for SRM, however, these were never properly monitored or reviewed. Policies would be sent out but there was no follow-up, or repercussions if a risk assessment or incident management plan wasn't completed. There was no forum or established mechanism to review, share or check-in with the policy implementation. It was just assumed that once a policy had been sent out, staff would be expected to implement it – with little support from senior strategic leaders or follow-up up on progress or impact."

From a KII Participant, NGO Operational Manager

6.6 Learning

The most successful SRM strategies are those that constantly review, adapt and adjust, with opportunities for ongoing, structured and/or informal collective reflection and learning.

Expert opinion

"We never collect data for the sake of it. We only collect data that we're going to use as part of our discussions on reflection and review."

(KII Participant, NGO Strategic Lead)

It is good practice to share learnings at all levels, both positive and negative, as this strengthens accountability and transparency and encourages a more participatory approach.

Expert opinion

"Our [Security Focal Points] meet on a regular basis to discuss S&S issues of interest with their Country Directors, who then distil key information for dissemination to the wider staff team in all-staff sessions."

(KII Participant, NGO S&S Global Director)

The learning process should work in both directions. This includes a feed forward process to support sharing of SRM information from strategic leads (i.e. assimilation of new learning) to the wider organisation. Likewise, it also includes a participatory feedback process, which makes use of what has been learned and establishes clear actions based on these lessons.

By supporting learning across the organisation in this way, it is possible to build an SRM culture that becomes rewarding and self-sustaining. Through this process, organisations can build an openness to change which ultimately supports strategic renewal.

Top tip: Good learning mechanisms

- Map the flow of knowledge. Who has access to what information? Who does not have access to beneficial information? Who are the gatekeepers of knowledge? How can you easily share that knowledge both internally and externally?
- Engage your senior leadership team in the process. Demonstrate your assets and highlight the untapped potential.
- Reflect on your organisation's strengths and highlight areas for improvement.
- Optimise periods of change. Significant organisational changes can be stressful, but they can also provide opportunities to lay foundations for new ways of working.
- Seek light-touch ways of capturing knowledge. Hold team and all-staff sharing sessions and think about the potential audiences for all information to maximise its potential.
- Create resources in accessible places and refer people to them at every opportunity.

Wilsdon, N. Institute of Voluntary Action Research, 'Taking a strategic learning approach to evaluation'

6.7 Data Collection Methods

While developing a MEAL Plan, an organisation first needs to establish what it wants to monitor. The focus then shifts to selecting your data collection method(s). There are a variety of quantitative and qualitative tools and methodologies to choose from. Many of these can be used in tandem or combined, based on your organisation's budget, objectives and time. Although techniques may change, all present SRM teams with an opportunity to regularly and thoroughly review how effective your SRM strategy is. This not only ensures that money is spent, and resources are invested impactfully, but also allows for adjustments, adaptations and feedback on the strategic approach.

A summary of example data collection tools is provided below.

Type of Tool	Pros	Cons
Routine Monitoring	Provides up-to-date data and allows for course corrective actions.	
Survey	Allows data to be gathered from a large number of people. Highly versatile: surveys can be conducted online, by phone or in person, and gather both quantitative and qualitative responses.	Can be difficult to ascertain the extent of the cause-and-effect relationship between two or more elements.
Interviews	Allows for a more in-depth discussion of a topic. Unstructured or semi-structured interviews provide the opportunity to tailor conversations to needs and allow flex for participant answers. Useful for sensitive topics.	Can be subject to interviewer bias (where the interviewer's beliefs or attitudes can shape a respondent's answers) or social desirability bias (where a respondent provides the answers they think the interviewer wants). Time and resource intensive. Harder to produce quantifiable data.
Focus Groups	Suitable for gaining a more in-depth understanding of an issue or perspective and sharing feedback and learnings.	Time-consuming to conduct and analyse. Participants with less dominant personalities may not share their opinions.

continued

Type of Tool	Pros	Cons
Case Studies	Suitable for gaining an in-depth appreciation of a specific topic, such as a group, individual or programme.	Difficult to generalise observations or findings. Risk of bias, as researchers will likely seek to use case studies that validate their assumptions rather than provide objective evidence of an issue.
Face-to-face audits	Allows information to be gathered in a more natural setting, which may elicit more accurate results.	Planned audits may prevent participants from acting genuinely. Covert observational studies fail to provide participants with the opportunity to consent to participation.
Security Logs/ Incident Database	Tracks safety and security concerns, near misses and incidents in a uniform way, and thereby well suited for official reporting purposes.	Needs to be easy to access for all staff. Requires a good reporting culture – where reporting is seen in a positive light.
Key/Core Performance Indicators (KPIs/CPIs)	Can be qualitative or quantitative. Focus on specific goals/areas of the organisation. Fosters accountability.	Should be combined with other methods so it is not seen as a purely punitive mechanism.
Annual Audits (internal or third party)	Provide a comprehensive analysis of SRM knowledge, attitude and practice in a given context and can evaluate operations against the Minimum Operational Security Standards.	Can be expensive and require additional resources.

Useful Resources

- Oxfam's Participatory Capacity and Vulnerability Analysis: A practitioner's guide
- The World Bank: M&E; Some Tools, Methods and Approaches
- Overseas Development Institute: Supporting Adaptive Management
- INTRAC: M&E Universe
- Bond UK: Choosing Appropriate Evaluation Methods

Amnesty International

Ukraine

A Weapons Investigator with Amnesty International carries out a field investigation. As safety and security are preventative areas of work, it can be hard to measure success. Therefore, it is especially important to have a robust MEAL plan in place.

SRM Toolkit

Tool 1
Developing your Strategic Directions – Example

Strategic Direction 1: Organisational Approach to SRM

Outcome: All stakeholders are aware of the organisational approach to risk and where risk thresholds lie.

No.	Objective	Who is responsible	Target date	Measure of success
1.1	Establish risk attitude and thresholds	Executive Teams	Feb-25	* Risk attitude statement developed and rolled out to all staff. * Risk threshold matrix completed and communicated to all strategic leads.
1.2	Confirm SRM strategy approach	SRM Global Director and Risk Management Committee	Dec-26	* Contextual analysis of all country operations and activities completed. * Programme and SRM teams agree on approach of acceptance, protection and deterrence in each operational context/programme. * Approaches included in internal training.

Strategic Direction 2: Raise Awareness

Outcome: All stakeholders are made conscious of, and accept, their roles and responsibilities in reducing the risks to people, information and physical assets.

No.	Objective	Who is responsible	Target date	Measure of success
2.1	Promote understanding of SRM at strategic, operational and functional levels through a structured internal awareness programme.	SRM Department	Dec-26	* SRM internal awareness programme developed and rolled out to all staff. * Six-monthly review of which risk management practices are followed by different stakeholders (e.g. incident reporting, development of risk assessments/risk management tools).
2.2	Provide internal and external safety and security training (as per training matrix).	SRM Global Director and Risk Management Committee	Dec-26	* Annual review of level of participation in safety and security training. * Quarterly review of level of satisfaction with training provided.
2.3	Governance structure in place relating to SRM.	Executive Teams	Feb-25	* Governance structure agreed, and clear roles and responsibilities assigned at each level. * Staff recruitment process confirmed. * Governance structure communicated to all staff.

Strategic Direction 3: Cultural Focus on Safety and Security

Outcome: The culture of the organisation and approach to programmes and achieving organisational objectives is underpinned by good safety and security awareness. Security risk management is a key part of the planning process.

No.	Objective	Who is responsible	Target date	Measure of success
3.1	SRM included in planning stages of operational activities.	SRM Department	Dec-26	* SRM regularly features in agenda items and minutes. * Planning processes include SRM involvement/sign-off.
3.2	Establish 10 ‘golden rules’ which are well understood by all staff.	SRM Global Director and Risk Management Committee	Dec-26	* Internal audit to check staff awareness of golden rules – 80% awareness minimum. * Golden rules clearly displayed on website, internal offices, national staff offices.
3.3	Risk management committee established and active.	COO	Feb-25	* Members of group confirmed from across all functions. * Quarterly meetings occur, minuted and shared with Executive Leadership Team.

Strategic Direction 4: Reporting, Reflection and Review

Outcome: All stakeholders are made conscious of the need to report concerns, near-misses and incidents and are confident these will be regularly reviewed and actioned by senior leaders.

No.	Objective	Who is responsible	Target date	Measure of success
4.1	Develop SRM feedback mechanism for reporting incidents, near-misses and concerns.	SRM Global Director and Risk Management Committee	Dec-26	* Feedback mechanisms developed and regularly used by all staff. * Log of all incidents, near-misses and concerns regularly updated.
4.2	Review and reflect on incidents, near-misses and concerns.	SRM Global Director and Risk Management Committee	Dec-26	* Action log with clearly assigned action owners and progress reports in place. * Six-monthly review of serious incidents and analysis of trends completed and shared with Executive Leaders.

Strategic Direction 5: Best Practice

Outcome: The organisation is up to date with and follows best practice guidance and shares and collaborates with others in the sector.

No.	Objective	Who is responsible	Target date	Measure of success
5.1	Interaction, communication and collaboration within and across sectors.	SRM Global Director and Risk Management Committee/ Working Group	Dec-25	* Membership of relevant SRM forums and groups within the sector, such as GISF. * Established relationships with SRM professionals outside the sector. Quarterly/bi-annual check-ins, minuted and shared with Risk Committee.
5.2	Regular benchmarking reviews.	SRM Global Director and Risk Management Committee	Dec-25	* External review of duty of care practices relating to ISO standards conducted using an external provider. * Internal benchmarking review of good practice process established and conducted every 18 months. * Results of audits/reviews shared with Executive Leadership and communicated to wider staff with follow-up action points.

Adapted from template by Draper, R, (2014), How to Write a Strategic Security Plan
https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper/

Tool 2
How to rationalise your SRM strategy

Visioning	Set your vision. Decide on a specific timeframe which is practical for the organisation and ask yourself: Where would you like to see SRM within your organisation in five years' time? Who is your target audience? How do you want others to view SRM? How will you achieve your goal? **Remember:** • Use simple language that can be understood by people of all backgrounds. • Your vision should be appealing and inspiring to engage people. • It has a broad context. • It should be written in the present tense.
Metrics/Data Analysis	To prove the vision statement, it is important to have justifications. These can include figures and metrics which will finally determine if the SRM strategy has made an impact, as planned (see Chapter 6). **Strategic SRM leaders should ask themselves:** • What is the name of the metric and what it will display about the organisation? • What kind of data needs to be produced from the metric and where can the data be found? • What type of chart or visual will best display the data? • What are the ways of interpreting the measure?
SWOT Analysis	SWOT stands for Strengths, Weaknesses, Opportunities and Threats. SWOT analysis is another efficient planning tool, in which members suggest, list and assess the strengths, weaknesses, opportunities and threats of their organisation. Conducting a SWOT analysis is a very effective tool to assess and analyse the current health of SRM within your organisation. It can be helpful to use a SWOT analysis to review your approach to SRM alongside the whole organisation strategy to see where strengths, weaknesses, opportunities and threats to aligning the SRM strategy may exist. (See Tool 4, SWOT Analysis Template).
PESTLE Analysis	This analysis is used to identify threats and weaknesses while conducting a SWOT analysis. The first step while undertaking a PESTLE analysis is to understand all the external factors that may impact the working of your organisation. In the analysis the following factors are assessed: Political, Economic, Social, Technological, Legal, Environmental.

Affinity & Interrelation Diagrams	As a result of a SWOT analysis, there are often many internal and strategic projects that may need to be undertaken. An affinity diagram is useful for narrowing down a large number of elements into more organised and similar categories to make them more easily manageable. An affinity diagram is made by getting the leadership team to write all the prospective initiatives or projects identified from the SWOT on sticky notes. The team should then categorise these notes under specific themes, before allocating the projects to a specific function(s). This helps to streamline and identify links between functions, as well as to assign action owners in a logical manner.
Portfolio Analysis	Identify the various strategies that have been used to achieve SRM goals in the past. Then classify them into 'Star' (where implementation has been highly successful), 'Foundation' (where they form the bedrock for rolling out SRM goals), 'Question Mark' (new/untried strategies) and 'Dead Ducks' (tried and failed). This can help focus on which methods need focus and which should be scrapped or reviewed.

Tool 3
SRM Planning Template

GUIDING PURPOSE	Why are we implementing SRM? What do we aim to achieve? What benefits are we hoping to see?
MOST CRITICAL ELEMENTS OF THE SRM PROCESS FOR OUR ORGANISATION	Which elements of the SRM framework are most important for our objectives?
APPROACH FOR ADAPTING SRM PRINCIPLES TO OUR ORGANISATIONAL CULTURE AND NEEDS	How can we integrate SRM into our existing processes most effectively? Will we form a new risk council or use an existing forum for risk discussion? How will we train risk owners? How will we include SRM in budgeting and strategic planning? How will we engage our Board of Directors?
PLAN FOR INCREMENTALLY INCREASING THE VALUE OF SRM TO OUR ORGANISATION	How and when will we expand SRM to increase the value it provides our organisation?

Tool 4
SWOT Analysis Template

STRENGTHS	WEAKNESSES
What do we do well within our current SRM framework/approach? What internal resources or capacities do we have/can we tap into? e.g. a good culture around SRM, experienced SRM staff, robust risk assessment tools, strong learning and development programme.	What areas of our current SRM framework need improvement? What resources or training do we lack? e.g. inadequate training on crisis management, lack of understanding and engagement with SRM, outdated technology, poor infrastructure.
OPPORTUNITIES	**THREATS**
What opportunities exist that SRM could tap into or benefit from? Are there places where SRM could help achieve whole organisation objectives/meet strategic goals? e.g. emerging technologies, new partnerships and networking opportunities.	What might threaten our effectiveness in implementing SRM across the organisation? e.g. staff retention, cybersecurity breaches, areas of operation in high-risk contexts, staff burnout.

Tool 5
Example Risk Attitude Statements

Example 1:

In the pursuit of ....’s strategic aims *[define]* ...., it is inevitable that operational activities *[include examples]* .... will expose staff to certain threats. The organisation strives to reduce the level of risk attached to these threats by means of robust security risk management.

Risks will be considered excessive where the likelihood of a critical incident is more probable than possible, taking into account the risk mitigation measures applied.

A critical incident is one which would cause the following:

- a staff member or associated personnel suffering serious physical or psychological harm; or
- the organisation’s finances or reputation suffering serious damage.

.... works in some of the most challenging and remote environments. When programmatic needs are high, ... may accept a higher level of risk. In such situations, an even greater emphasis on security risk management is essential.

....’s risk attitude will always take account of programme objectives, the importance of what is to be achieved and the capacity to manage threats, as well as the impact of other strategic factors (such as key relationships and donor interests). Risk owners will decide on a case-by-case basis whether the specific programme objectives and intended outcomes justify accepting the assessed level of risk.

Example 2:

.... recognises that the organisation works in environments where risk cannot be entirely eliminated. Nevertheless, all practical measures must be taken to reduce risk levels as far as possible.

The residual level of risk that remains after such measures have been taken is considered acceptable only if it is justified by the humanitarian impact of the operation.

Where unnecessary risks have been eliminated, and the activity is deemed worth pursuing, staff members must be prepared to accept the residual level of risk involved.

Examples provided by International Location Safety

Tool 6
Establishing Organisational Approach to Risk

Risk Tolerance

Risk tolerances are acceptable levels of variation in the organisation's risk attitude based on specific circumstances (see section 1.5). This falls within organisational risk threshold (i.e. the amount of risk the organisation could actually take before its capacity to deliver its mission is critically impacted).

Defining your approach to risk:

- Establishes clear parameters for teams to work within.
- Allows the systematic treatment of risk.
- Protects you from organisational collapse.

Process:

1. **Define the context:** Provide a brief explanation of how SRM risks relate to, and may impact, the overall strategy of the organisation, based on its mission, aims, objectives and operational context. Are there any external drivers that should be considered?
2. **Identify boundaries:** Specify, in clear terms, what there is zero attitude for, what there is cautious attitude for, and why in some circumstances there could be a higher level of risk attitude (for example, donor requirements, high-risk programme locations).
3. **Set indicators:** Outline the key risk indicators that will be used to assess whether the organisation is operating within, close to, or outside of risk thresholds. These indicators will also help determine a course of action regarding the management of different risks.

To make sure that your risk attitude is proportionate, use your Organisational Risk Register to inform what your key threats are. This can be done for every function of the organisation. Assess the impact and likelihood of these threats to occur. You can use established definitions or create your own. An example is shown below.

Likelihood

Score	Term	Definition
1	Very low	The threat is very unlikely to happen.
2	Low	The threat is unlikely to happen.
3	Medium	The threat is possible.
4	High	The threat is likely to occur.
5	Very high	The threat is highly likely to occur.

Impact

Score	Term	Definition
1	Very low	Insignificant injuries or health effects, insignificant financial loss (<£1,000), insignificant business interruption (no lost time workdays), no negative reputational exposure, fully reversible impacts.
2	Low	Minimal injuries or health effects, minimal financial loss (<£5,000), minimal business interruption (<1 lost time workdays), minimal negative reputational exposure, mostly reversible impacts.
3	Medium	Moderate injuries or health effects, moderate financial loss (<£10,000), moderate business interruption (1-2 lost time workdays), moderate negative reputational exposure, outside assistance required to contain risk, partly reversible impacts.
4	High	Permanent disability or multiple hospitalisations, major health effects, major financial loss (£10,000-£50,000), major business interruption (3-6 lost time workdays), major negative reputational exposure, outside assistance required to contain risk, some reversible impacts.
5	Very high	Fatalities, multiple permanent disabilities or hospitalisations, significant financial loss (>£50,000), significant business interruption (>6 lost time workdays), major negative reputational exposures, outside assistance required to contain risk, significant impacts.

Plot these on a risk matrix and continually monitor:

		Threat impact				
		Very low	Low	Medium	High	Very high
Threat likelihood	Very low	1	2	3	4	5
	Low	2	4	6	8	10
	Medium	3	6	9	12	15
	High	4	8	12	16	20
	Very high	5	10	15	20	25

Green areas are within organisational risk attitude. They can be managed within normal mechanisms.

Amber areas are at the high-end of organisational risk attitude but within risk tolerance. These should be reported for awareness and review/contingency plans may be required.

Red areas are outside organisational risk thresholds. These should be reported, with immediate action required to improve controls.

Source: International Location Safety

Tool 7
Example Terms of Reference for Risk Management Committee

Meeting purpose

The Risk Management Committee (RMC) works to ensure that an NGO proactively identifies and manages the risk to its people. It ensures that the NGO continuously works to maintain and improve the organisation's security stance, where necessary remediating identified issues and risks.

The group's responsibilities and duties include:

- Ownership of the Security Risk Management Framework and strategies.
- Approve all high and very high threat level trip requests.
- Conduct post-incident and crisis reviews.
- Manage compliance to the Security Risk Management Framework.
- Agree security risk management activities and priorities.
- Ensure appropriate security risk management and crisis funding.
- Agree security communications and messaging to staff.

The group provides all functions with the opportunity to flag issues from within their teams. It ensures that solutions to identified risks encapsulate the needs of the organisation.

Attendees

Role	Committee Role
	Chair / Committee Member
	Deputy Chair / Committee Member
	Committee Member
	Committee Member
	Committee Member

Scheduling

a. The RMC Meeting will be scheduled as a monthly meeting.

b. The Chair or any committee member may arrange an emergency meeting should circumstances require such a meeting.

c. The meeting location will be confirmed by the Chair on a per event basis.

d. The meeting duration is set at 90 minutes.

Agenda

Item	Paper reference	Presented by	Actions
Agenda		Chair	
Incidents since last RMC	Incident reports / lessons identified report	Chair / Committee member	Update Global Incident Database and/ or risk register if necessary
Update on actions from the last SRMG	Meeting minutes	Chair / Committee Member	
Key security risk management achievements, issues or risks		Chair / Committee Member	
Review very high-risk Trip Forms (if necessary)		Committee Member	
Next meeting		Chair	
Any other business		Chair	

Terms

a. The Chair reports to the CEO / Board when necessary.

b. Each Committee Member carries a vote.

c. At least three Committee Members need to be in attendance for the meeting to be quorate.

d. Attendance in person is not mandatory but is preferred. Attendance via video or audio conference is acceptable.

e. In the event of absence of Committee Members, authorised deputies may attend.

f. Attendees will be authorised to make recommendations within the context and confines of their areas of knowledge.

g. In the absence of both the Chair and Deputy Chair, the Meeting should be rescheduled.

h. Decisions will be made by consensus of Committee Members and will be recorded.

i. Invited parties may present to the Committee if such a decision is carried at a previous meeting.

Responsibilities and authorities

a. Providing a confidential forum to identify issues/risks to the organisation or departmental actions which may affect the organisation's security.

b. Ensure that the working group is a working group and demonstrates continuous improvement in safety and security.

c. Own the organisation's Security Risk Management Framework and strategies, including signing off protocols and tools.

d. Approve all high and very high threat level trip requests.

e. Conduct post incident and crisis reviews.

f. Manage compliance to the Security Risk Management Framework.

g. Agree security risk management activities and priorities.

h. Ensure appropriate security risk management and crisis funding.

i. Agree security communications and messaging to staff.

j. When digital and legal risks may exacerbate the threat to staff or those under the organisation's instruction, factor this into risk management strategies and risk reduction measures.

k. Review and agree changes to the terms of reference for the Security Risk Management Framework.

Example provided by International Location Safety

OCHA/Joel Opulencia

Switzerland

A Risk Management Committee should aim to meet once per month.

Tool 8
Learning and Development Plan Template

Organisational objective	Knowledge and skills required	Who will participate?	Learning and development activities/methods	How will this be evaluated?	Cost	Date

Adapted from NCVO, Skills 3rd Sector; Training Needs Analysis

Tool 9
Strategic Training Matrix Example

This tool can be adapted or expanded at the operational level to reflect specific employees needs/date completed/skill level in each area.

Description	Name of provider (internal/external)	Strategic leaders	Regional directors	Country managers	Security focal points	All staff
Security framework		🟠	🟠	🟠	🟠	🟠
Creating procedures (e.g. country S&S plans, country risk, registers, incident management plans)		🟢	🟠	🟠	🟠	🟢
Risk assessment		🟢	🟡	🟡	🟡	🟢
Personal field security training / security awareness		🟡	🟠	🟠	🟠	🟡
Travel safety and security training		🟡	🟡	🟡	🟡	🟡
Crisis management workshop		🟠	🟢	🟢	🟢	🟢
First aid		🟢	🟢	🟡	🟡	🟢
Resilience and stress management		🟡	🟡	🟡	🟡	🟡
Security risk management training		🟢	🟢	🟢	🟠	🟢
The importance of duty of care		🟠	🟠	🟡	🟡	🟢
Reporting security incidents		🟡	🟡	🟡	🟡	🟡
Cybersecurity		🟡	🟡	🟡	🟡	🟡
Integrity and anti-corruption training		🟡	🟠	🟠	🟠	🟢
Anti-bribery and corruption training		🟢	🟡	🟡	🟡	🟢
Surveillance		🟢	🟡	🟡	🟡	🟢

- 🟠 Priority
- 🟡 Within 12 months
- 🟢 Not required

Example provided by International Location Safety

Tool 10
Theory of Change Template

Situation: What is the context or reason for this change?

Aims: What will 'success' look like?

Inputs and activities	Outputs	Change mechanism	Outcomes	Impacts
Inputs What financial outlay, staffing and other resources will be required?	What tangible results, products, lessons, inspections or improvements will be produced?	What actions will be needed to achieve the change(s)? Are you removing frictions, changing behaviour etc.?	**Short term** What will be the benefits and wider outcomes, both leading and lagging?	What are the impacts and how do they fit with departmental and governmental priorities?
Activities What will be delivered, such as training or guidance?			**Long term** What will be the sustainable and lasting changes, and what metrics will be used to measure these?	

Evidence assessment: What is the strength of the existing evidence base for this change?

Assumptions: What is being assumed as part of the plan?

Possible unintended consequences: Are there any other outcomes that might result from this project?

Adapted from an example provided by the UK Foreign, Commonwealth and Development Office (FCDO)

Tool 11
Logframe Template

	PROJECT SUMMARY	INDICATOR How is it calculated?	DATA SOURCE How will it be measured?	RISKS/ ASSUMPTIONS
Goal				
Outcomes				
Output				
Activity				

Source: Tools4Dev

Tool 12
MEAL Planning Template

Indicator	Specific MEAL activity	Who's involved	Who's responsible	Key milestones	Expected duration	Cost
Organisational culture regarding engagement with and understanding of SRM	Online perception survey sent to all staff	IT, HR, SRM, Communications	SRM and Communications	**Q1:** Question design completed, online system developed **Q2:** Survey out for completion **Q3:** Survey results analysed and present	**Q1-Q3**	**Staff time:** Five days to develop survey and IT system and conduct quality assurance 30 minutes per staff member to complete the survey Three days to analyse and present findings **Financial cost:** £250 e-survey system membership
Engagement with reporting SRM mechanism	Incident/near-miss/concern log (access via mobile app) with linked actions and owners	HR, SRM, IT, Finance, Legal, Programmes	SRM and IT	**Q1:** Logging system set up and rolled out **Q2:** Capacity training to all staff **Q3:** System live **Q4:** Results and first analysis and actions	**Q1-Q2: Develop and set-up** Ongoing: Quarterly review and reflect	**Staff time:** 30 days to develop and implement one-hour training for all staff **Financial cost:** £3,000-£5,000 for app-based system £1,000 for external training
Engagement with and communication of SRM issues/concern	Online log set-up of all meetings, agendas and minutes relating to SRM	IT, SRM	SRM	**Q1:** Internal systems set-up **Q2:** Capacity training, agendas confirmed **Q3:** Ongoing collation, reflection and review	**Q1-Q2: Develop and set-up** Ongoing: Quarterly review and reflect	**Staff time:** Two days to set up One-hour capacity training for key SRM staff **Financial cost:** £0
Physical check of SRM resources, equipment and measures in place	Internal audit structure designed and rolled out	SRM, IT, Legal, Programmes	SRM and Programmes	**Q1:** Internal audit system and process set-up **Q2:** Capacity training for all audit leads and whole staff roll-out **Q3:** Ongoing collation, reflection and review	**Q1-Q2: Develop and set-up** Ongoing: Quarterly review and reflect	**Staff time:** 15 days set-up Three-hour training per audit lead, one-hour training for all staff **Financial cost:** £1,000 IT system amendments and development
Engagement with and communication of SRM issues/concern	Amend programme report templates to include SRM feedback section linked to incident/near-miss/concern log	SRM, IT, Programmes	Programmes and SRM	**Q1:** Amendments made **Q2:** Capacity building with programme leads **Q3:** Roll-out **Q4:** Ongoing collation, reflection and review	**Q1-Q2: Develop and set-up** Ongoing: Quarterly review and reflect	**Staff time:** 10 days to develop and review Three-hour training per programme lead **Financial cost:** £0
Capacity building with regards to SRM	Training matrix and log developed, populated and integrated	HR, SRM, IT, Finance	HR and SRM	**Q1:** Training needs analysis completed. Matrix developed and log set-up **Q2:** Training programme commences **Q3:** System live **Q4:** Results and first analysis and actions	**Q1-Q2: Develop and set-up** Ongoing: Quarterly review and reflect	**Staff time:** Eight days to develop and implement Ongoing training needs dependent on training needs analysis **Financial cost:** Dependent on training providers

Example provided by International Location Safety

Bibliography

General

Breckenridge, M.-J., Czwarno, M., Duque-Díez, M., Fairbanks, A., Harvey, P., and Stoddard, A. (2023). Aid worker security report 2023. Security training in the humanitarian sector: Issues of equity and effectiveness. Humanitarian Outcomes. https://www.humanitarianoutcomes.org/AWSR_2023

Hermann, E., & Oberholzer, S. (2020). 'Security Risk Management and Risk Aversion in the Humanitarian Sector. Assessing Decision-Making Processes in Local and International Humanitarian NGOs'. Geneva: ICVA. https://www.icvanetwork.org/uploads/2021/07/Security_Risk_Management_May2020-1.pdf

Humanitarian Practice Network (HPN). (2010). Good Practice Review: Operational Security Management in Violent Environments. Number 8 (new edition). Overseas Development Institute. https://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

Chapter 1

Chapple, M, (2023): 'Risk appetite vs risk tolerance; How are they different', Tech Target. https://www.techtarget.com/searchcio/feature/Risk-appetite-vs-risk-tolerance-How-are-they-different

Datminr, (2022), 'Understand and plan for the corporate risk landscape'. https://www.dataminr.com/resources/ebook/understand-and-plan-for-the-corporate-risk-landscape

Donovan, L (2022), 'What is risk appetite and how do you implement it?', Risk Leadership Network. https://www.riskleadershipnetwork.com/insights/what-is-risk-appetite-and-how-do-you-implement-it

Draper, R (2014), 'How to write a strategic security risk management plan', LinkedIn https://www.linkedin.com/pulse/how-write-strategic-security-rick-draper/

Khushi, S, (2017), 'Strategic planning for NGOs: A guide to understanding the basics of strategic planning', LinkedIn. https://www.linkedin.com/pulse/strategic-planning-ngos-guide-understand-basics-samina-khushi/

Simpson, K. & Randall, I (2020). 'Systemcraft: A primer', Wasafiri. https://u05.88f.myftpupload.com/wp-content/uploads/2020/10/Wasafiri-SystemCraft-2020-Small.pdf

UN Programme Criticality Steering Group (2016), United Nations System Programme Criticality Framework, CEB/2016/HLCM/23. https://programmecriticality.org/Static/index.html

USAID (2022). 'USAID Risk Appetite Statement: A Mandatory Reference for ADS Chapter 596'. https://www.usaid.gov/sites/default/files/2022-12/596mad.pdf

Chapter 2

Mind Tools Article, 'The RACI Matrix: Structuring accountabilities for maximum efficiency and results'. https://www.mindtools.com/agn584l/the-raci-matrix

Von Moltke, N, (2024), 'RACI Template and Ultimate 2024 Guide to the RACI Matrix', Academy to Innovate. https://www.aihr.com/blog/raci-template/

Chapter 3

IEC 31010:2019: Risk Management: Risk Assessment Techniques. https://www.iso.org/standard/72140.html

Swiss Centre of Competence for International Cooperation (CINFO) and GISF, Duty of Care Self-Assessment Tool. https://dutyofcare.cinfo.ch/index.html

3.2 Programme/Operations

Frontline Defenders, Workbook on Security. https://www.frontlinedefenders.org/en/workbook-security

GISF Security Toolbox, 2. Acceptance Analysis. https://www.gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/

GISF. (2021) Achieving Safe Operations through Acceptance: challenges and opportunities for security risk management. Global Interagency Security Forum (GISF). https://www.gisf.ngo/wp-content/uploads/2021/12/Achieving_Safe_Operations_through_Acceptance_challenges_and_opportunities_for_security_risk_management.pdf

Larissa Fast, L., Finucane C., Freeman F., O'Neill M., Rowley E., (2011) The Acceptance Toolkit, Save the Children. https://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf

Morrow, E. (2023) Humanitarian Access & Security Management: considerations for staff security, GISF blog. https://www.gisf.ngo/blogs/humanitarian-access-security-management-considerations-for-security-staff/

Stoddard, A., Czwarno, M., and Hamsik, L. (2019). NGOs & risk: Managing uncertainty in local-international partnerships (global report). Humanitarian Outcomes. https://www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships

3.3 Finance

Global Interagency Security Forum (GISF). (2013). The cost of security risk management for NGOs. https://www.gisf.ngo/resource/the-cost-of-srm-for-ngos/

Sweeney, A, (2019), 'Securing aid worker safety through effective budgeting', Crisis Response, October 2019 | Vol: 14 | issue 4 https://www.gisf.ngo/wp-content/uploads/2019/11/Securing-Aid-Worker-Safety-Through-Effective-Budgeting.pdf

3.4 Communications

Foulkes, I, (2022), Misinformation campaign against the International Committee of the Red Cross in Ukraine, BBC News. https://www.bbc.com/news/world-europe-60921567

GISF and Cornerstone OnDemand Foundation, (2019), Security Risk Management Toolkit: Strategies. https://gisf.ngo/wp-content/uploads/2020/03/Planning-security-risk-management-strategies-and-systems.pdf

Internews, (2019), Managing Misinformation in a Humanitarian Context. https://internews.org/wp-content/uploads/2021/02/Rumor_Tracking_Mods_3_How-to-Guide.pdf

Leyland, J., Tiller, S., and Bhattacharya, B. (2023). Misinformation in humanitarian programmes: Lessons from the MSF Listen experience. Journal of Humanitarian Affairs, 5(2).

Oh, S., Adkins, T. (2018), Disinformation Toolkit, InterAction. https://www.interaction.org/wp-content/uploads/2019/02/InterAction_DisinformationToolkit.pdf

3.5 IT

Dugan, S. (2022), 'Cyberattacks; a real threat to NGOs and not-for-profits', Reliefweb. https://reliefweb.int/report/world/cyberattacks-real-threat-ngos-and-nonprofits

GISF, (2020), Security to Go: Module 4 Digital Security. https://gisf.ngo/wp-content/uploads/2020/11/GISF_Security-to-Go_Module-4_Oct20.pdf

ICRC, (2024), Cyberattack on ICRC: What we know. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

Kumar M. (2017), Digital Security of LGBTQ+ Aid Workers: Awareness and Response. https://www.gisf.ngo/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/

Stine K., Quinn S., Witte G., Gardner R.K., (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM), National Institute of Standards. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

3.6 HR

Arthur, T and Moutard, L, (2022). Toward inclusive security risk management: the impact of 'race', ethnicity and nationality on aid workers' security. Global Interagency Security Forum (GISF). https://gisf.ngo/wp-content/uploads/2022/05/Towards-Inclusive-Security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security.pdf

GISF Inclusive Security Podcast Series E1: Introducing a person-centred approach. https://gisf.ngo/resource/inclusive-security-e1-introducing-a-person-centered-approach/

GISF, (2018), Managing the Security of Aid Workers with Diverse Profiles. https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/

GISF (2017), Security-to-Go Toolbox: Module 12 People Management, C Williamson. https://gisf.ngo/resource/people-management-security-to-go-module/

Goldhill, O (2019), Palestine's head of mental health services says PTSD is a western concept, Quartz Journals. https://qz.com/1521806/palestines-head-of-mental-health-services-says-ptsd-is-a-western-concept

Goozee, H (2020), Decolonizing Trauma with Franzt Fanon, Oxford University Press. https://academic.oup.com/ips/article-abstract/15/1/102/5868933?redirectedFrom=fulltext

McKinsey & Company. (2023). What Is Psychological Safety? McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-psychological-safety

Persaud, C. (2014a). Gender and security: Guidelines for mainstreaming gender in security risk management. GISF. https://www.gisf.ngo/resource/ gender-and-security/

3.7 Legal

GISF, (2012), International agencies working with local partners, GISF Briefing Paper. https://gisf.ngo/resource/international-agencies-working-with-local-partners/

ISOS Global Duty of Care Benchmarking Report, 2015. https://www.internationalsos.co.id/duty-of-care

Merkelbach, M. and Kemp, E. (2011). Can you get sued? Legal liability of international humanitarian aid organisations towards their staff. Security Management Initiative. https://www.gisf.ngo/resource/ can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

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

3.8 Safeguarding

GISF Webinar | Intersection of Security and Safeguarding | Recording. https://gisf.ngo/resource/gisf-webinar-intersection-of-security-and-safeguarding-recording/

Mullin K., (2021), Launching the community-based safeguarding visual toolkit. https://www.interaction.org/blog/launching-the-safeguarding-community-visual-toolkit/

Safeguarding Resource and Support Hub (RSH). https:/ safeguardingsupporthub.org/

How-to note on implementing the safeguarding cycle. https://www.gisf.ngo/resource/how-to-note-on-implementing-the-safeguarding-cycle/

Essentials. https://safeguardingsupporthub.org/essentials

PSEA Glossary. https://safeguardingsupporthub.org/psea-glossary-clear-global

Introduction to safeguarding – RSH South Sudan. https://safeguardingsupporthub.org/sites/default/files/essentials/Essentials_What%20is%20safeguarding/Essentials_Introduction%20to%20safeguarding%20South%20Sudan.pdf

3.9 Travel

ISO 31030: Travel Risk Management. https://www.iso.org/standard/54204.html

Chapter 4

GISF (2022), NGO Security Collaboration Guide, Global Interagency Security Forum (GISF). https://www.gisf.ngo/long-read/ngo-security-collaboration-guide/

GISF. (2021) Partnerships and Security Risk Management: a joint action guide for local and international aid organisations. Global Interagency Security Forum (GISF). https://www.gisf.ngo/wp-content/uploads/2021/06/GISF_Partner-Joint-Action-Guide_EN_download_Aug211.pdf

GISF. (2020) Partnerships and Security Risk Management: from the local partner's perspective. Global Interagency Security Forum (GISF). https://www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/

ISO 31000:2018 Risk Management. https://www.iso.org/standard/65694.html

UN Department for Safety and Security (UNDSS). (2015). Saving lives together. A framework for improving security arrangements among international non-governmental organisations/international organisations and the United Nations. https://www.gisf.ngo/wp-content/uploads/2020/02/2225-UNDSS-2015-Saving-Lives-Together-Framework.pdf

Williams C., (2020), Collaborative Security Risk Management: A case for local development, GISF Article. https://www.gisf.ngo/collaborative-security-risk-management-a-case-for-local-development/

Chapter 5

Buth P., (2010), Crisis Management of Critical Incidents, GISF. https://www.gisf.ngo/resource/crisis-management-of-critical-incidents/

GISF and OSAC. (2023) NGO Crisis Management Exercise Manual: a guide to developing and facilitating effective exercises. Global Interagency Security Forum (GISF) and Overseas Security Advisory Council (OSAC). https://www.gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/

Kunal K., Eder P., LinkedIn Community, (2023), How do you foster a culture of risk awareness and accountability across different functions and levels? https://www.linkedin.com/advice/0/how-do-you-foster-culture-risk-awareness

Lucidchart, (2023), Top strategies for managing cross-functional teams. https://www.lucidchart.com/blog/managing-cross-functional-teams

Miller, R., (2018), Cross-functional teams impacting information security efforts, LinkedIn. https://www.linkedin.com/pulse/cross-functional-teams-impacting-information-security-richard-miller/?trk=public_profile_article_view

Nagele-Piazza L., (2018), Create a cross-functional team to combat data security issues, Society for Human Resource Management (SHRM) https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/cross-functional-team-to-combat-data-security-issues.aspx

White J., Gouveia B, Singer J, Josias M., Emerging trends and early lessons on crisis management and business resilience, S-RM Intelligence and Risk Consulting. http://www.s-rminform.com/srm-insights/crisis-management-business-resilience

Chapter 6

Benjamin M., (2023), The benefits of real-time monitoring and evaluation, LinkedIn. https://www.linkedin.com/pulse/benefits-real-time-monitoring-evaluation-migolo-benjamin/

Data for Development, (2021), Ways you can integrate technology in monitoring and evaluation. https://datafordev.com/ways-you-can-integrate-technology-in-monitoring-and-evaluation/

International Rescue Committee (2021), Result Chain, Logframe and Theory of Change Terminology. https://rescue.app.box.com/s/e8sj6rep7hghs8j2yern8crxauavs6o8/file/775591027183

Gadkari M., (2023), What is Monitoring, Evaluation and Learning (MEL)?, Resonance Global. https://www.resonanceglobal.com/blog/what-is-monitoring-evaluation-and-learning-mel

Pasanen T., Barnett I, (2019), Supporting adaptive management, Overseas Development Institute. https://cdn.odi.org/media/documents/odi-ml-adaptivemanagement-wp569-jan20.pdf

Scotland's International Development Alliance, (2023), Monitoring, Evaluation and Learning (MEL) Guide. https://intdevalliance.scot/wp-content/uploads/2023/08/MEL_Support_Package_4th_June.pdf

The World Bank, (2004), Monitoring and Evaluation; Some Tools, Methods and Approaches. https://cnxus.org/wp-content/uploads/2022/04/WB_ME20ENG.pdf

The Monitoring and Evaluation Toolkit: An introductory toolkit for beginners, Article: 'What is M&E'. https://thetoolkit.me/what-is-me/

Turnbull M., Turvill E., (2012) Participatory Capacity and Vulnerability Analysis: A practitioner's guide, Oxfam GB. https://policy-practice.oxfam.org/resources/participatory-capacity-and-vulnerability-analysis-a-practitioners-guide-232411/

Wilsdon, N. Institute of Voluntary Action Research, 'Taking a strategic learning approach to evaluation'. https://www.ivar.org.uk/blog/taking-a-strategic-learning-approach-to-evaluation/

OCHA/Yasmina Guerda

Nigeria
A volunteer with Médecins Sans Frontières assists at a clinic supporting people who have been displaced from their homes.

gisf

Global Interagency Security Forum

GISF Research and Programmes
T: +44 (0)20 7274 5032
E: research@gisf.ngo

www.gisf.ngo