

3.1 The humanitarian security risk management system

This chapter describes some of the key elements of an organisation's security risk management system – the organisational policy instruments, structures and roles and responsibilities involved in reducing risks to staff and fulfilling duty of care.

3.1.1 Security risk management framework

Security risk management involves many processes and overlaps with different areas of work and functions. To help guide planning and implementation around security risk management, it may be helpful to visualise a framework – reflecting the security risk management architecture, structures, processes and arrangements of an entire organisation, all of which are built from the foundational objective of achieving safer access and fulfilling duty of care through a person-centred approach (see Figure 4).

The different elements of this framework are discussed in more depth in various chapters of this GPR.

Figure 4 Example security risk management framework



3.1.2 Security policy

Overview

A security policy is a critical governance document that is usually endorsed by the organisation’s board or a similar authoritative body. The policy reflects the organisation’s culture and values, outlining how it will uphold duty of care while pursuing strategic objectives. A well-defined security policy not only addresses operational risks, but also promotes a culture of vigilance and responsibility. The

security policy should be crafted in alignment with the organisation's objectives and operational modalities. In the context of an organisation's governance framework, the security policy serves as a foundational document that supports its overall strategic direction and operational integrity. This policy should ideally not be developed in isolation, but connect with other governance documents to ensure a cohesive approach across the entire organisation.²⁸

Elements of a security policy

Security policy documents can encompass the following elements.

- **Statement of approach.** This outlines the organisation's general approach to security, including its governance structure. The statement can also address whether the organisation pursues a person-centred approach (see *Chapter 7.2*). It can specify the scope of the policy and who it applies to, including staff, volunteers, consultants, casual labour and organisational partners. It helps everyone within the organisation understand their role and the security expectations placed on them.
- **Roles and responsibilities.** The specific roles and responsibilities related to security risk management within the organisation. It defines the hierarchy and accountability mechanisms, ensuring that everyone from senior management to operational staff understands their part in maintaining security.
- **Minimum security requirements.** The minimum security requirements the organisation expects staff to uphold in each operational location. These can be helpful for standardising security practices and ensuring a consistent approach across the entire organisation. (See below for further information.)
- **Integration with other policies.** The security policy should link to other relevant organisational policy documents, such as those on civil–military coordination, sexual exploitation, abuse and harassment and duty of care. This integration helps ensure cohesion and can reinforce the organisation's commitment to comprehensive risk management and ethical conduct. By aligning these policies, the organisation ensures that security considerations are embedded across all areas of operation and governance.
- **Principles and culture.** The policy should outline the organisation's risk threshold, security culture and other guiding principles that shape its approach to security risk management. It can also highlight the organisation's

²⁸ While a security policy provides practical guidelines for implementing security measures, a security risk management strategy outlines the organisation's long-term goals and approach for managing security risks. For more on how to develop and implement a security risk management strategy, see GISF (2024) *Security risk management (SRM) strategy and policy development: a cross-functional guide* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

commitment to maintaining a security approach that aligns with relevant principles, values and ethical standards (see examples in Table 1). Clearly stating the organisation’s risk threshold enables staff to make decisions that align with the organisation’s risk attitude.²⁹

Table 1 Principles, values and ethical standards in security

Term	Definition
Humanitarian principles	Adherence to the core humanitarian principles of humanity, neutrality, impartiality and independence, which guide humanitarian action by emphasising the need to address human suffering, remain neutral in conflicts, provide aid based solely on need without discrimination, and maintain autonomy from political or other non-humanitarian objectives.
Do no harm	Organisations avoid exacerbating existing conflicts or creating new forms of harm through their presence and work.
Shared responsibility for security	Security is a shared responsibility between the organisation and its staff at all levels.
Primacy of life	The principle that human life and wellbeing should be given the highest priority and importance. This is closely linked to the concept of programme criticality.
Programme criticality (or proportionate risk)	Programme activities justify the level of risk that staff are asked to take. The more critical or lifesaving the programme, the more risk an organisation may be prepared to accept to sustain it.
Duty to inform	Security measures reduce but do not eliminate all risks. Staff must be informed of the level of risk that remains after mitigating measures have been put in place and given the opportunity to discuss this residual risk and make an informed choice based on their personal risk thresholds.
Right to withdraw	Staff have the right to withdraw from a location or activity due to security concerns.
No right to remain	Staff do not have a right to remain in a location if the organisation’s leadership has decided to suspend activities due to insecurity.

29 See GISF (2024) for an example risk appetite statement.

Use of weapons/ armed assets	An organisation should have a clear organisational principle on when and how weapons and other armed assets (such as escorts) can be used by staff as part of their work.
Equitable security	Security measures are fairly applied to all staff according to their individual needs. Equitable does not always mean equal, but rather takes into account individual circumstances to adjust security measures based on needs. This is a cornerstone of the person-centred approach to security.
Person-centred approach	An approach that places individuals at the centre of security risk management activities. This particularly involves recognising the profile-specific risks that individuals face due to their intersectional identity, their role and organisation, and the context in which they work.
Equitable partnerships	An approach that aims to establish collaborative ways to jointly address security concerns faced by all partner organisations, thereby sharing risk between partners.

Adapted from Bickley, S. (2017) *Security risk management: a basic guide for smaller NGOs*. EISF (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Regular evaluation of the organisation’s governance framework is necessary to maintain its effectiveness. Continuous improvement – through feedback, monitoring, after-action reviews and lessons learned, for example – can help refine security policies over time.

Security requirements

Minimum security requirements are protocols the organisation expects all staff to follow to ensure the safety and security of assets, personnel and information. These requirements can form the foundation of a robust security system, tailored to address specific threats and vulnerabilities inherent to each location, staff member (considering personal risk profiles) and workstream. An example of a minimum security requirement might be a security plan for each office or programme location.

Security requirements are sometimes structured in tiers, based on the security levels or risk ratings assigned to different locations (e.g. high, medium and low). By considering location-specific risk and vulnerability factors, security measures can be tailored accordingly, ensuring appropriate allocation of security risk management resources and attention.

What constitutes high, medium and low risk will vary by organisation and should ideally be determined by a thorough assessment, taking into account

staff composition and individual as well as organisational vulnerabilities to specific threats.

- **High-risk locations.** These areas usually require the most stringent security measures, which may include advanced surveillance systems, extensive access control mechanisms and armed protection.
- **Medium-risk locations.** These locations usually necessitate robust but less intensive measures, including enhanced physical barriers, regular security audits and detailed incident response plans.
- **Low-risk locations.** These sites usually require basic security protocols, focusing on general awareness and preventive measures.

For many international organisations it is common practice that staff travelling to a high-risk location undergo some form of hostile environment awareness training (HEAT) course.

► See Chapter 5.2 for more on HEAT courses.

Specific baseline requirements can also be applied to other factors, including staff positions and particular projects. Personal risk profiles also play a role in determining whether a location is high-risk or not, and it is advisable for organisations to factor this in when deciding on security requirements.

Monitoring compliance and effectiveness

Security requirements can play an important role in monitoring compliance and effectiveness by:

- Establishing a baseline for security practices across all locations, ensuring consistency and comparability.
- Providing clear criteria for internal and external security audits, helping to identify gaps and areas for improvement.
- Enabling the regular review and updating of security measures based on audit findings and evolving threats.
- Ensuring adherence to relevant laws, regulations and sector good practice.
- Assigning responsibility for security measures, fostering a culture of accountability and vigilance.

► See *Chapter 3.4* for more on *monitoring compliance and security audits*.

Good practice in implementation

Implementation of the practical components of a security policy can be challenging. One of the primary issues is resource allocation, which involves ensuring sufficient funding and personnel for effective implementation. Another challenge is adaptability; security measures must be continually adjusted to address the risks and operational needs of different locations and staff. Compliance and enforcement also pose a challenge. Keeping up with evolving security technologies and integrating them into existing systems requires continuous effort and investment. Cultural and regional differences must also be handled carefully. It is essential to respect local laws, customs and business practices while maintaining consistent security expectations across different locations.

With these challenges in mind, the following can support implementation.

- **Leadership and accountability.** Ensuring senior leadership commitment, embedding security into the organisation's overall governance structure.
- **Resourcing.** Ensuring adequate resourcing in terms of money and people to implement the security policy.
- **Cross-functional integration.** Aiming to integrate security across all functions, such as human resources, finance, information technology (IT) and programmes.
- **Contextual adaptation.** Ensuring that the policy has sufficient flexibility in its application to allow for adaptation to local contexts or other circumstances, considering, for example, identity, cultural, linguistic, technological and environmental factors.
- **Continuous monitoring.** Regularly monitoring, reviewing and adapting the organisation's approach through feedback and incident reporting.
- **Dissemination.** Ensuring that the policy is shared in an accessible and relevant format with all staff.

3.1.3 Governance and accountability

As employers and legal entities, organisations have a formal responsibility towards all their staff, in line with their duty of care obligations. An organisation's duty of care towards its staff should ideally be defined in its security policy as well as documents such as employment contracts. While security is a shared responsibility between the organisation and its staff, organisations are responsible

for establishing effective governance structures and ensuring that staff are aware of and understand their roles and responsibilities within this structure.

► See Chapter 1.1 for a more detailed discussion of duty of care.

Roles and responsibilities

Properly positioning security risk management within the organisation's governance structure means being clear about who is responsible for what. Adopting a RACI matrix can be beneficial.³⁰

► See Chapter 5.1 for more on the RACI matrix.

Executive leadership

Ultimate accountability for security usually lies with the organisation's executive director (or equivalent), or in some cases the governing board. In most organisations, executive leadership sets the tone for risk tolerance, ensures compliance with legal obligations (like duty of care) and allocates resources to implement security measures. This accountability often includes oversight of policies, crisis management and the integration of security within business continuity planning. The governing board may also have a key role in strategic oversight and risk governance. This ensures that security is not just a technical or operational concern but a fundamental aspect of organisational governance and resilience.

The operational management of security is linked to organisation-wide management and decision-making practices, and most organisations decentralise security decisions to the closest relevant level of authority. Decisions about whether to initiate operations in a new location, and what type of programme to undertake, are usually the responsibility of senior leadership. The organisation may also require that senior staff contribute towards, or advise on, major security decisions (for example, whether to relocate or evacuate staff). Issues around media, communications and fundraising, and human resource issues such as the establishment of insurance policies, are typically decided and managed at the head-office level. Specific decisions may also need formal approval from senior leadership, including whether:

- to raise or lower the risk rating of a location;
- to re-enter an area from which staff have been relocated/evacuated because of security risks;

³⁰ For a detailed example of a RACI matrix in relation to security responsibilities, see GISF (2024).

Humanitarian security risk management

- to adopt a ‘low-visibility’ approach and remove logos and flags from offices and vehicles;³¹
- to use armed protection; and
- to use a private security provider.

Security staff

Many organisations employ security staff to provide expertise and advisory support to managers (who are usually ultimately responsible for security-related decisions). These security focal points are often tasked with undertaking security-related actions, such as developing security plans and sharing insight and expertise with non-security colleagues. Most organisations have either fully dedicated or multi-hatting security focal points across different levels, from head office to local project officers, with the highest-risk locations often receiving the most investment in staffing. In some organisations security is managed across teams, or by committees or working groups, where security risk management tasks and decisions are shared by a number of key staff. In other organisations, security risk management is integrated into line management, and no separate security function exists (see below for a more detailed discussion of these types of governance structures).

► See *Chapter 5.1* for more details on security roles.

Country-level leadership (for international organisations)

In-country, it is usually the responsibility of the senior representative (i.e. the country director or head of mission) to ensure that organisational policies and procedures are implemented and adhered to, with most security risk management tasks delegated to a security focal point.

Managers

Managers at every level within an organisation will have a responsibility towards their staff, which includes ensuring they are safe. What this means in practice will vary across organisations, but can include ensuring staff attend security briefings and training, providing support to security focal points, and inputting into risk assessments and security planning.

³¹ Government donors may impose contractual obligations regarding the visibility (‘branding’) of assistance they fund, in which case the organisation may have to seek their formal approval to forgo this requirement.

Staff

All staff, from senior programme managers to interns, have a responsibility for their own security – and for the security of the team as a whole, as well as the organisation. All staff should ideally be involved in regular security-related discussions and activities, including training.

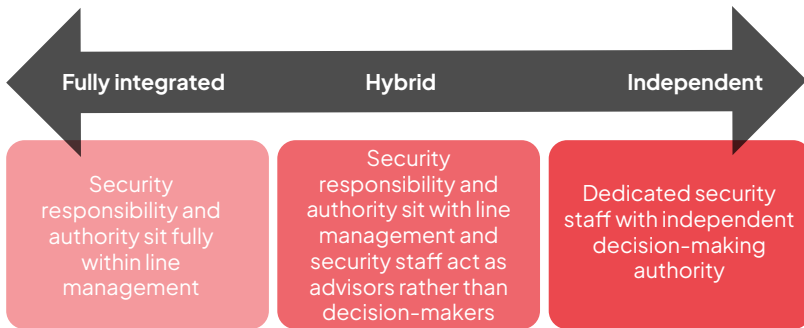
Types of security governance structures

Security governance structures may vary depending on the organisation's overall approach. This can be conceived as a continuum with fully integrated security risk management at one end, and a heavily resourced and independent security structure at the other (see Figure 5).

- **Fully integrated.** Security responsibility and authority sit fully within line management. There are usually no dedicated security staff.
- **Hybrid.** Security responsibility and authority sit with line management but security tasks, such as undertaking risk assessments and creating plans, sit with dedicated security staff. Any security staff in these organisations usually act as advisors but are not decision-makers.
- **Independent.** Organisations that adopt this structure have dedicated security staff at multiple levels with the authority to take security risk management decisions independently of other management functions. This structure is more common in corporate environments and is sometimes described as a 'corporate security' model.

Most organisations typically sit somewhere along this continuum depending on their security risk management approach, resources and preferences. For example, an organisation may employ a large number of professional security staff but still keep all security decision-making authority within management. Some organisations may also employ different structures in different locations, such as more dedicated advisory security positions in high-risk contexts and a more integrated approach in low-risk settings. What is important is consistency and clear communication on who has ultimate responsibility for security decisions at different levels within the organisation.

Figure 5 Types of security governance structures



All of these structures have their strengths and weaknesses.

In the integrated approach, managers are fully responsible for staff security, which can help ensure that security is viewed as part of the operational decision-making process, making it more likely that security will be aligned with programme goals. However, managers tasked with security responsibilities may lack expertise in this area as well as the time to properly undertake security tasks in addition to their other responsibilities. Reliance on outsourced security services may be greater in these circumstances (though not necessarily).

The hybrid structure allows organisations to benefit from dedicated security expertise while still maintaining decision-making within line management. This offers a balanced approach, with security advice integrated into the planning process without undermining programme goals. The flexibility of this structure makes it adaptable to different organisational needs. However, the advisory role of security staff can limit their ability to enforce security measures. This dependence on line management for final decisions may lead to delayed actions or inconsistent implementation of security measures, especially if programme managers do not prioritise security concerns.

The independent security function structure provides the most resources and authority to security staff. Security staff can take direct action, which can improve risk mitigation, staff training and compliance. However, this structure may lead to the siloing of security from other functions. Security may be

perceived as a blocker to programme activities, especially if decisions made by security staff conflict with programme goals. This can hinder the flexibility and responsiveness needed in certain operational contexts and undermine staff buy-in to security measures.

In summary, fully integrated structures can offer better alignment with programmes but may lack expertise; hybrid approaches can offer a balance but may struggle with consistency and implementation; and independent structures may provide robust security but can be seen as restrictive. Much can depend on how security staff engage with their colleagues. For example in an independent structure, even though security staff have the authority to enforce strict measures, they might choose to reserve this for extreme cases, preferring to collaborate with other teams to reach balanced decisions. Ultimately, while governance models can shape the organisation's overall approach to security, the attitudes and approaches of individuals can also play a significant role in how security is managed and perceived.

► *This is discussed in more detail in Part 5 – People in security risk management.*

External service providers

Some organisations hire external security advisors, either as the only providers of security expertise and resources or to support internal functions lacking the necessary capacity, skills or time. While external providers offer broad experience, unbiased perspectives and knowledge of good practice, they may lack deep understanding of or investment in the organisation's culture and internal relationships. Over-reliance on them can weaken in-house capacity and institutional knowledge.

► *See Chapter 2.1 for more on private security providers.*

Integrating security with other organisational functions

Within an organisation, security risk management interfaces with many areas of work. The security risk management function in an organisation can be located under an overall 'risk management' umbrella, in operations or in another

functional area, depending on the structure of the organisation. Regardless of where security sits, collaboration across the whole organisation and other relevant risk management measures is key, and often the biggest challenge.

Security staff can improve collaboration by understanding the organisation's internal ecosystem and the security function's role within it. This includes understanding internal organisational dynamics and external environments, and anticipating and responding to risk trends, seizing opportunities to develop and improve ways of working and fostering relationships that benefit the organisation as a whole. This holistic approach promotes resilience and organisational adaptability.

Security risk management staff can benefit from the following:

- **Promoting a comprehensive view of the organisation's internal dynamics, external influences and cross-functional interactions.** This approach helps security practitioners and leaders identify security risks across all departments, processes and systems, rather than dealing with them in isolation. This also aligns with the principles of enterprise risk management (see below).
- **Active interdisciplinary collaboration.** The complexity of an organisation often necessitates collaboration with other departments and areas of expertise. Integrating security risk management into existing work areas brings diverse perspectives, experiences and knowledge together to address the multifaceted nature of risks.
- **Incorporating systems thinking.** This allows organisations to better identify, understand and mitigate risks through the analysis of dynamic interactions and feedback loops within the whole organisation. Systems thinking for effective security risk management means understanding the interdependencies between various organisational functions and external factors, fostering cross-functional collaboration for comprehensive risk assessments, and developing adaptive and dynamic management strategies.

Understanding how security interfaces with other organisational functions

Questions for security staff:

- How does security risk management integrate into other organisational functions, influencing its overall resilience and adaptability?
- Does your organisation's security risk management strategy enable everyone to achieve their objectives and goals effectively, fostering a culture of success and collaboration?
- Is the security team's vision and purpose fit to support resilience?
- To support greater collaboration, are there key individuals or teams in other organisational functions who should be prioritised for outreach?

Some larger international organisations have adopted an 'enterprise risk management' approach, which involves identifying, assessing and managing all risks across an organisation. Security is one risk type that organisations manage on a day-to-day basis. Others include strategic, fiduciary and financial, cyber, safety, legal, information, reputational and operational risks. These risk types often overlap and can impact, and be impacted by, security. Organisations that adopt an enterprise risk management approach aim to integrate risk management practices into overall strategy and decision-making processes to ensure a coordinated and systematic approach. By situating security risks within the overall risk management framework of an organisation, decision-makers can balance security considerations with other risks, such as financial or reputational risks, ensuring that security measures do not inadvertently hinder the organisation's operations or strategic objectives.

Good practices for enterprise risk management include defining clear risk attitudes, tolerances and thresholds, which help guide decision-making across departments. It is advisable to link enterprise risk management efforts to business continuity and crisis management, ensuring that security risk management supports broader organisational resilience. Implementing an enterprise risk management approach involves senior leadership engagement, cross-functional collaboration and regular monitoring and evaluation to adapt

the strategy to emerging risks. Cross-functional integration is particularly important. Security risk management should not be siloed or viewed as a separate workstream; instead, it should connect with other departments. Cross-functional teams can work collaboratively to manage risks and ensure smooth information flow. Regular communication, shared objectives and a collective responsibility across functions drive better risk management practices. This integration can address diverse risks – be they related to accessing communities, protecting data or ensuring business continuity – and promote a positive security culture across the organisation.³²

Further information

Guidance

Bickley, S. (2017) *Security risk management: A basic guide for smaller NGOs*. EISF (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

GISF (2024) *Security risk management (SRM) strategy and policy development: A cross-functional guide* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

³² For more practical recommendations on cross-functional integration, see GISF (2024).