5.1 Human resources

Security risk management in the aid sector is a multifaceted function that involves a broad spectrum of interactions at multiple levels, requiring a range of technical, interpersonal and analytical skills. This chapter describes the changing profiles, qualifications, competencies and roles of people who manage an organisation's security and how security can and should impact people management, from recruitment through to the end of contracts.

5.1.1 Evolutions in the security risk management function

As security risk management in the aid sector has evolved over the decades, so has the cadre of professionals now inhabiting security risk management roles. The shift from highly protective approaches based on military and law enforcement models towards more integrated approaches focused on enabling humanitarian action has given rise to a new professional field: humanitarian security. In this emerging discipline, professionals are increasingly valued for their combination of traditional security skills and understanding of humanitarian programming and principles.

Other developments that have affected the profiles and skillsets of humanitarian security staff include the challenges of higher risk appetites and risk threshold levels among some organisations, and the need for in-house skills development to enable work in multi-threat, high-risk environments and to manage crisis situations. More frequent partnering with other organisations, as well as enhanced security collaboration in response settings, requires the ability to coordinate and liaise across a wide range of entities. Additionally, humanitarian security staff are continually engaging with emerging technologies as both potential security threats and as tools for security risk management.

Finally, security risk management roles have increasingly emphasised people skills and adaptive leadership as teams become more diverse and inclusive, and as security strategies increasingly focus on person-centred security and identity-based risk factors.

► *See Chapter 1.1 for more on building a positive security culture.*

5.1.2 People in security risk management roles

The management of security risks is shaped by the organisation's broader structures and decision-making policies. A small organisation operating in just one locality might have a single security focal point. Conversely, a large international organisation may deploy multinational security teams at global, regional, national and sub-national levels. The roles and responsibilities of such professionals may vary – but most play technical and advisory roles focused on supporting leadership, with limited decision-making authority. For example:

- For international organisations, a senior security director based at the global level who advises the organisation's executive leadership and oversees the development and implementation of security policies across the organisation.
- For international organisations, a security advisor and/or team at the regional level providing operational security risk management support, technical advice and oversight to country programmes.
- A security focal point and/or team at the country level who advises the country leadership and oversees security risk management – for national organisations, this would be their head office and most senior security staff.
- Local-level security focal points in different programme locations managing security incidents and taking on day-to-day security risk management activities.

Depending on the organisation, these positions may have different titles, including security director, advisor, manager, coordinator, officer or focal point.

It is important to highlight that there is diversity in how organisations structure and implement their security risk management. In some instances, the responsibility is embedded in regular management roles and there is no separate security function. In others, decision-making authority for security sits with security functions. Other organisations may have – in addition or alternatively – security working groups, where different functions share security risk management responsibilities.

In structuring staff roles, it may be useful to refer to the 'RACI' model,[77] which identifies, for each area of activity, the person or people:

---

[77] For more detailed discussion of how the RACI model can be used in security risk management, see GISF (2024) *Security risk management (SRM) strategy and policy development: a cross-functional guide* (https://gisf.ngo/resource/srm-strategy-and-policy-guide/)

- **Responsible** – the one(s) implementing the work
- **Accountable** – the one ultimately answerable for the task or decision
- **Consulted** – those who provide input and advice
- **Informed** – those kept up to date on progress or decisions but not directly involved in the work.

This section outlines an advisory security risk management model, which is one of the most common in the aid sector. In this model, security staff are usually responsible for security risk management while accountability sits with leadership. Note: while reference is made only to 'security', in practice many of the job roles and responsibilities encompass both safety and security.

► *See Chapter 3.1 for more details on governance and security structures.*

Senior security staff

Senior security positions at the organisational leadership level are ideally held by highly qualified and experienced security risk management professionals who provide leadership and undertake several critical functions, including:

- Communicating vision, developing policies, standards and strategies related to security, and creating security risk management plans.
- Leading security staff and teams.
- Helping to develop multi-level security training programmes.
- Undertaking research and development projects on evolving trends and good practice, and integrating these into organisational processes and procedures
- Developing core security budgets.
- Developing and overseeing security compliance and effectiveness monitoring efforts.
- Representing the organisation at global interagency forums and engaging in high-level discussions on security risk management within the aid sector.
- Writing crisis management policies and participating in crisis management teams.
- Partnering with stakeholders in the organisation to integrate security within a broader organisational risk management approach.
- Reviewing and improving security activities to reflect changing operating contexts, including trends in incident data.

Some larger international organisations have established global security teams, led by a global security director. To distribute responsibilities across the team, these individuals may cover different regions, or may bring in specific expertise and lead activities related to that area – for example, training or information security.

Security staff and teams at regional/country level

In many organisations, while the primary responsibility for security decision-making at the country level typically remains with the most senior manager in that office (e.g. the country director or executive director), security risk management professionals play an important advisory role and undertake many management and support functions, including:

- Advising senior leaders on best security risk management practices and introducing lessons and practices from other settings.
- Managing and mentoring more junior security staff.
- Identifying security risk management goals and objectives and developing action plans aligned with the organisation's or country programme's strategic plans.
- Implementing the security policy, standards, guidelines and procedures, and ensuring review and compliance.
- Gathering and analysing information to identify trends, adapt security risk management measures and prepare for possible future scenarios.
- Establishing and overseeing systems to record, analyse and disseminate security information or incidents affecting staff and operations.
- Conducting and reviewing security risk assessments.
- Devising plans, protocols, procedures and measures to mitigate identified risks.
- Supporting crisis management teams in handling critical incidents and crisis events.
- Recommending and procuring safety and security equipment.
- Conducting security briefings and training.
- Representing the organisation in interagency security forums and coordination meetings at regional/country levels.

Some organisations have adopted an integrated security and access management approach by combining positions.

▶ *See Chapter 3.2 for a more detailed discussion of the link between security risk management and access functions.*

In some international organisations, there are additional security advisors or teams at the regional level. These roles engage in activities similar to those listed above, and focus on advising the regional leadership and supporting the security risk management efforts of country teams in the region.

Focal points at the local office level

At the local office level, high-risk security environments usually merit a full-time security staff member. In low- and moderate-risk environments, a non-dedicated security focal point may fulfil this function alongside other responsibilities (e.g. administrative, logistics or HR). This person would usually manage day-to-day security-related work. At the country and local office level, safety responsibilities also usually sit with security focal points.

The job description for a local office-level security focal point might include:

- Conducting risk analysis of the operating environment, and sending security alerts to relevant staff.
- Helping to develop security risk mitigation strategies, including standard operating procedures, guidelines and contingency plans.
- Briefing incoming staff.
- Ensuring all staff in the location are kept up to date on changing security conditions.
- Reporting safety and security incidents.
- Advising on and managing security and communications equipment and supplies.
- Overseeing adherence to procedures and plans and reporting security breaches or deviations.
- Managing security-related staff such as guards, radio operators and other security focal points.
- Training and mentoring colleagues to develop security-related competencies.
- Participating in budgeting for operational security expenditures.
- Being involved in incident response and crisis management as well as after-action reviews and evaluations.
- Liaising with and exchanging information with other aid organisations and with the authorities.

The security focal point need not have sole responsibility for security risk management. A team approach to managing security is often beneficial. This allows for a group of focal points to manage workloads, co-own security plans and procedures, and build a positive security culture within a location. In some organisations, a local security committee supports the focal point and security is a standing topic on the agenda of programmatic and operational meetings.

5.1.3 Key attributes and competencies

Profiles, skills and qualifications

Security skills can be broadly categorised as 'hard' and 'soft'. Hard skills refer to the more technical and operational aspects of security, such as handling security equipment, physical protection and tactics. These skills are often associated with a background in the military, police or intelligence services, where individuals may have developed knowledge of weapons, military tactics, police operations and counter-terrorism measures. Hard skills may also include investigative skills as well as threat and risk analysis.

Soft skills relate to interpersonal abilities, such as understanding social and cultural dynamics, working with a multicultural team as well as leadership, mentoring and training skills, relationship-building, communication and management. In humanitarian security risk management, they also include a good understanding of programme objectives, organisational mandates and humanitarian principles. Given the complexity of actors and stakeholders in aid settings, it is also necessary to build and sustain networks with diverse communities and be able to understand and analyse different cultural, social, geopolitical and environmental contexts, including areas affected by violent conflict.

In recent years, as the value of soft skills and appreciation of acceptance-based security approaches have gained traction, there has been a change in the profile and skills of security staff. A security risk management professional with both technical and people skills, and solid experience in the humanitarian sector, is most often the profile of choice. Still, the availability of such individuals can be limited in many locations. To address this, some organisations seek to build security capacity in-house by training existing staff for security roles. More staff are turning to training, degrees and certifications to develop their skills and knowledge and demonstrate their competencies.

▶ *For some example training resources and certifications see Chapter 5.2.*

The skills and competencies required of a security risk management professional may depend on the type and mandate of the organisation, as well as the work to be done. It may also depend on the context in which the organisation operates. For example, in an environment with active conflict and the presence of multiple military actors where more protective and deterrence measures are required, more hard skills and military-related knowledge may be beneficial. In an environment characterised by socio-economic problems and tribal dynamics, where negotiating access and building acceptance are the key security risk management approaches, a deeper knowledge of the context and strong soft skills may be called for. High-crime contexts may demand a full spectrum of skills and competencies, including expertise in sociology, criminology and crime management. In offices or locations where staff compliance with security procedures is proving particularly challenging, it may make sense to recruit an individual who is relatable to staff (in nature, background and personal characteristics) and with strong interpersonal skills, enabling them to encourage greater adherence to security protocols.

For international organisations, a key consideration is whether a security position should be held by a local or foreign national. Staff local to the area will usually have better knowledge of the social, cultural and political environment, and greater networks of contacts. However, they may also face challenges if they are perceived by certain actors to be aligned with a party to a conflict or affiliated with contesting local groups. Given their ties to local communities, they may be more vulnerable to pressure from local actors. Staff who are not from the location may have a different vantage point and perspective, and may be better placed to liaise with all stakeholders. They may also lack local knowledge, have poor cultural and contextual awareness and have ingrained biases. Recruiting a staff member from a neighbouring country may bring benefits and challenges – and even staff from other parts of the country may be seen and treated as foreigners in particular locations.

The selection of security staff should be driven by the specific context and needs of the role, rather than relying on default profiles or structures. As situations evolve and security staff from diverse backgrounds gain new skills, organisations should remain flexible and open to considering a broader range of candidates. This approach allows for a better match between the role's requirements and growing competencies within the talent pool, ensuring more inclusive, effective and adaptable staffing.

Many organisations are striving for greater diversity in their security teams, recognising that this can improve staff perceptions and engagement with security. A balanced representation of genders, ethnicities and other identity characteristics among security staff can lead to positive outcomes, such as better understanding of the lived experiences of a diverse workforce, reduced biases in risk assessments and security arrangements, and more innovative problem-solving.

Women in security

Women have rarely held security positions in aid organisations, at least until recently. The under-representation of women has been due to a number of factors, including social and cultural barriers, as well as negative perceptions of women's aptitude and skills. These perceptions largely stem from gender stereotypes and rigid views of what constitutes an effective security focal point. The number of female staff taking on a security risk management role in aid organisations has, however, increased significantly in recent years, supported by wider policies to foster improved gender balance and equal representation. This has had numerous benefits, including added credibility, fresh ideas and approaches and greater representation and understanding of the security needs of female aid workers.

Key competencies

The specific skills and competencies of people in security roles will depend on the organisation and the context, but may include those listed in Table 6.[78]

It is unlikely that any single individual will possess all the competencies listed here. Therefore, many organisations form security teams made up of individuals with diverse expertise in various areas.

---

[78] INSSA has developed a list of core competencies for security staff: https://inssa.org/certification.

Table 6 Key competencies of security staff

Competency	Description
Problem-solving, analytical, critical and adaptive thinking	The ability to analyse complex situations, foresee potential risks and develop effective solutions to make informed decisions in dynamic environments. Linked to this are skills in managing change to adapt security approaches and plans to evolving threats and organisational changes, ensuring continuous adaptation and risk mitigation.
Risk assessment and mitigation	The ability to identify and analyse security risks and develop risk mitigation strategies.
Security planning	The ability to develop security plans, including contingency planning.
Incident response and crisis management	Proficiency in handling incidents and crises.
Security measures	Knowledge of – and ability to implement – security measures for specific threats or threat environments. This will be context-dependent but can include measures related to site security, combat-related threats and abduction risks, for example. In some cases, knowledge of first aid and trauma response, digital security or skills in detecting and mitigating hostile surveillance may be relevant.
Negotiation and conflict resolution skills	Skills in transactional negotiation and conflict resolution with colleagues and external stakeholders.
Effective communication and persuasion skills	Clear and persuasive communication for conveying security policies, coordinating with teams and liaising with senior leadership and external authorities and stakeholders.
Teamwork and collaboration	Ability to work well in teams and collaboratively across different organisational departments.
Finance and budget management	Skills in managing budgets to ensure resources are allocated efficiently to mitigate risks.
Presentation skills	The ability to present information clearly and effectively to various audiences, including staff, stakeholders and donors.

Competency	Description
Project cycle management	Understanding the phases of project management, from planning to evaluation, in order to implement security measures that align with project goals and timelines.
Legal and regulatory knowledge	Awareness of relevant laws and regulations to ensure compliance and to help colleagues navigate legal challenges in different jurisdictions.
Cultural awareness	The ability to understand and respect local customs and norms, and adapt security efforts as appropriate.
Information and communication technologies (ICT)	Proficiency in using technology tools for secure communication, data management and incident reporting.
Data literacy/data analytics	The ability to collect, analyse and visualise data using software tools and technologies, which can aid in, for example, extracting information from data sets to identify trends and make evidence-based decisions.
Enterprise risk management	Comprehensive knowledge of organisation-wide risk management frameworks and practices.
Training skills	The ability to build competencies and educate staff on security protocols, emergency procedures, the use of protective equipment and other relevant subjects.

Internal communications good practices

Effective communication is a crucial soft skill needed for successful security risk management in organisations. Yet security professionals often struggle to effectively communicate their message to others in the organisation and instigate change. Technical jargon, complex explanations of risks and formulas and differing priorities can create barriers to understanding and buy-in from non-security staff. A lack of empathy for and understanding of the perspective, motivations and challenges faced by internal stakeholders can also be a barrier to effective collaboration. Organisational leaders and non-security staff will likely engage more with security staff who listen attentively and communicate solutions tailored to their requirements in a way they understand.

Security staff can address communication challenges by:

- **Simplifying technical language** – avoiding jargon and complex explanations, making information easier to understand.
- **Tailoring messaging to the audience** – customising communication based on the audience's level of understanding and specific concerns.
- **Providing context through examples and stories** – using relatable examples or personal stories to help staff understand why security matters to them personally and to their work.
- **Offering training and raising awareness** – organising training sessions or awareness initiatives that clarify the vision and goals of security risk management within the organisation.
- **Maintaining regular, varied communication** – using different communication methods and sharing consistent updates, highlighting successes to boost morale.
- **Being empathetic** – beginning conversations by showing empathy, building trust through open dialogue and active listening.
- **Encouraging two-way communication** – inviting feedback from colleagues and stakeholders to ensure they feel heard and adapt strategies based on their input.
- **Using non-verbal communication –** being mindful of body language, tone and facial expressions as these can enhance or hinder the message being conveyed.

▶ *For more information on security communication within an organisation, see Chapter 5.3.*

Values, principles and people skills

In addition to the above competencies, staff in security roles can build on values and attributes such as:

- **Continuous learning** – actively upgrading knowledge and skills to remain current and relevant.

- **Professionalism** – an appreciation of, and desire for, mastery in a professional domain and adhering to standards in competence, diligence and ethics.
- **Emotional intelligence** – the ability to identify and manage one's emotions, empathise with others, communicate effectively, recognise different perspectives and defuse conflict.
- **Building relationships** – interacting effectively with colleagues and a wide range of external networks, including the UN, other aid organisations, private companies, local authorities and the business community, as sources of information and expertise.
- **Personal resilience** – the physical, mental and emotional capacity to endure problems and hardships and to prevail under stressful situations in changing environments.

▶ *See Chapter 5.4 for more on resilience and stress management.*

Note on humanitarian principles

Belief in, and adherence to, humanitarian principles and values is increasingly viewed as an important characteristic of an effective security risk management professional. Understanding and engaging with these principles and values allows security focal points to communicate more effectively with programme staff and align security risk management measures to an aid organisation's overall strategic objectives. It is, therefore, advisable to ensure that newly recruited security staff, particularly those new to the humanitarian sector, understand, buy into and can apply and effectively communicate these values and principles.

Management skills and adaptive leadership

The knowledge, experience, interpersonal and social skills of a manager are pivotal in shaping a team's collective experience and influencing the team's success. This holds true for security staff as well. A security focal point who seeks to make changes or achieve security objectives in a 'bulldozer' fashion, rather than adapting and collaborating, can create more problems than solutions. It is advisable for security staff to adopt collaborative approaches to gain buy-in and build a positive security culture, ensuring that the overall objective is to enable colleagues to carry out their work in the safest way possible.

The adaptive leadership model has gained attention in recent years and may prove particularly useful to security risk management positions. This approach uses problem diagnosis, interruption and innovation to handle issues and obstacles as they arise, which is directly relevant to managing risks in ever-changing internal and external environments. If one technique or process is not yielding the desired results, an adaptive leader finds new strategies that can work. Adaptive change requires leaders to effectively communicate to people on what stays the same (continuity) and what needs to change. Adaptive leadership involves strategies such as:

- Diagnosing and interpreting problems from a broad perspective.
- Acknowledging and collectively mourning losses.
- Monitoring stress levels to prevent harm to teamwork and individuals' mental health.
- Depersonalising conflicts to understand different perspectives.
- Actively determining what to retain or discard within organisational systems.
- Encouraging experimentation and smart risk-taking.
- Conducting disciplined assessments to refine systems and processes.

5.1.4 Security and managing people

Managing people is a critical part of an organisation's security risk management. Contented and motivated employees are more likely to be engaged, committed and productive. Conversely, poorly motivated and disgruntled employees not only underperform in the workplace, but are also likely to become a source of risk to the organisation. One of the many ways to establish a well-functioning and healthy team is to ensure leadership and clarity in organisational identity, roles, communication, decision-making, conflict management and team-building, and to create a conducive working environment where team members feel comfortable and valued. This starts with clarity in employee handbooks and contracts and continues through each phase of a staff member's employment – recruitment, onboarding, performance, development and end of contract.[79]

---

[79] For more details on how security can feed into these different phases, see Davis, J. et al. (2020) 'Module 13, People management' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/)

Transparency and clarity on contractual arrangements (e.g. early termination of contracts) can reduce concerns and grievances among staff. It is also an important mechanism through which the organisation can clarify each staff member's role in following security rules and guidance. Through the HR process, staff can be informed of the organisation's security-related policies, strategy and structure, where security responsibilities sit and who to turn to for support. Clarity and transparency around disciplinary procedures such as warnings and termination are paramount in the event of non-compliance with security rules and expectations.

Recruiting the right individuals is especially important for aid organisations. Inadequate skills or poor judgement may not only impact operational effectiveness, but also increase vulnerability to external risks. It is also important for personal risk profiles to be proactively considered in recruitment decisions in order to safeguard staff, without being unduly discriminatory. Job advertisements should be written in a non-discriminatory manner, considering identity-based issues and inclusivity. Where certain personal profiles may be at higher risk than others due to the context and other circumstances, this can be discussed during the recruitment process.

▶ *See Chapter 1.2 for more discussion about how personal risk profiles can be considered during recruitment.*

Pre-employment screening is crucial. At a minimum, criteria should aim to include a criminal record check, online presence/history, verification of declared qualifications, past employment history and investigation of employment gaps of more than one month. Many international donors require that staff members' names be checked against a list of sanctioned individuals and entities, with proof of this vetting saved on file.

Onboarding processes can prepare new employees for the security environment they are entering. A good onboarding process considers multi-level orientations on HR policies, security, operations, programmes, organisational structure, mandate, mission and risk appetite/acceptance level, as well as personal behaviour and how it relates to security. This can include the potential security implications of personal activities, including use of social media. In high-risk contexts, intensive briefings and security orientations are advisable. Onboarding is an ideal point at which an organisation can meet its duty to inform staff of the risks they may face, and ensure that staff feel comfortable accepting these risks.

▶ *See Chapter 1.1 for more on the duty to inform, and on individual risk thresholds.*

When employees leave an organisation, particularly in cases of sudden withdrawal, termination or office closure due to insecurity or funding issues, there are significant security implications. Preparing for these kinds of scenarios is essential, not just to treat staff fairly, but also to ensure that security information is passed on in the best way possible to incoming new recruits. Failures in planning, as seen during evacuations in Afghanistan in 2021 and Sudan in 2023, can leave local staff particularly vulnerable to security risks, highlighting potentially major ethical and security failures. Early discussions about end of contracts and conducting exit interviews can help organisations retain valuable knowledge, and offering support to departing employees can mitigate potential future issues.

Finally, some security incidents have resulted from a lack of internal grievance redress mechanisms, and many organisations still overlook the need to manage internal security risks. Establishing complaint procedures or mechanisms for staff provides a formal and safe channel for reporting misconduct – including mismanagement, corruption, bullying and abuse – without fear of retribution. This can help identify and address issues early, and fosters a culture of accountability and trust. It is also a fundamental element in managing incidents of sexual violence affecting staff within an organisation.

This is closely linked to safeguarding, which has received significant attention in recent years within the aid sector. Safeguarding refers to the broader measures taken by organisations to protect people both inside and outside the organisation from harm, abuse, neglect and exploitation (see the box below).

Key safeguarding elements

Policies and procedures

- Robust safeguarding policies that outline the organisation's commitment to preventing sexual exploitation, abuse, harassment and other misconduct by staff and associated personnel.
- Clear, confidential and safe reporting mechanisms and investigation procedures for safeguarding concerns or incidents.
- Safeguarding integrated into codes of conduct, human resources practices, security risk management and programme design.

Prevention

- Thorough screening and vetting during recruitment processes.
- Mandatory safeguarding training for all staff, partners and volunteers.
- Raising awareness among affected communities on their rights and how to report concerns.
- Assessing and mitigating safeguarding risks in programme areas.

Response

- Survivor-centred approaches that prioritise the rights, needs and wishes of the survivor.
- Confidential reporting channels and whistleblower protection measures.
- Fair and timely investigations into allegations, conducted by trained investigators.
- Transparent accountability measures and disciplinary action for substantiated cases of misconduct.

Further information

Research and discussion

EISF (2018) *Managing the security of aid workers with diverse profiles* (https://gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/).

GISF and Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Heifetz, R.A., Linsky, M. and Grashow, A. (2009) *The practice of adaptive leadership*. Harvard Business Review Press (www.hks.harvard.edu/publications/practice-adaptive-leadership-tools-and-tactics-changing-your-organization-and-world).

USAID Partner Liaison Security Operations (PLSO) (2022) *Women in security. A study of barriers and enablers to entering and progressing within the security field in South Sudan* (https://gisf.ngo/resource/women-in-security-a-study-of-barriers-and-enablers-to-entering-and-progressing-within-the-security-field-in-south-sudan/).

Guidance and tools

Davis, J. et al. (2020) ‘Module 13, People management’ in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/).

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

INSSA (n.d.) Certification (https://inssa.org/certification).

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